Formation NTFS - Windows 10-11- Server - SR 10-11- SR 22 - Cours

Michel Cabaré / www.cabare.net / michel@cabare.net

NTFS File System Windows 10 Windows 11 Windows Server - SR 10-11 – SR 22 - Cours V3-0 - Janvier 2022

ICPF
Certification PRO
Formateur Expert

https://WWW.CABARE.NET ©

CABARÉ FORMATION

Microsoft Partner

TABLE DES MATIÈRES

ACCES AUX PERMISSIONS NTFS 4

PERMISSIONS DE SECURITE – AUTORISATIONS DE PARTAGE : 4

SECURITE NTFS 5

ACL ET ACE : 5
PERMISSIONS NTFS SUR DOSSIERS - FICHIERS : 5
PERMISSIONS STANDARD ET SPECIALES : 6
COMBINAISON FICHIER – DOSSIER EN NTFS: 8
Exemple 1 : (fichier contre dossier) *8*
Exemple 2 : (combinaison sur dossier) *8*
Exemple 3 : (combinaison dossier - fichier) *8*
PERMISSION NTFS ET D'AUTORISATIONS DE PARTAGE (RESEAU): 9
Exemple 1 : *9*
Exemple 2 : *9*

HERITAGE NTFS 10

NOTION D'HERITAGE 10
CASSER UN HERITAGE – INTERFACE WINDOWS 10 12
Convertir… = repartir de l'existant *13*
Supprimer… = repartir de zéro *14*
RECREER UN HERITAGE – INTERFACE WINDOWS 10 15
RECREER UN OU PLUSIEURS HERITAGES – WINDOWS 10 15
CASSER UN HERITAGE – INTERFACE 7 17
RECREER UN HERITAGE INTERFACE 7 19
RECREER UN OU PLUSIEURS HERITAGES – INTERFACE 7 20

PROPRIETE NTFS 22

NOTION DE PROPRIETE 22
PRENDRE POSSESSION DES DOSSIERS ET FICHIERS 23
DONNER L'AUTORISATION D'APPROPRIATION 24
DONNER LA POSSESSION DES DOSSIERS ET FICHIERS 26
REGLES "D'AFFECTATION" DES PERMISSIONS NTFS: 27

VOIR LES AUTORISATIONS EFFECTIVES 28

AUTORISATIONS EFFECTIVES - 10 : 28
AUTORISATIONS EFFECTIVES - 7 : 30
UTILITAIRE ACCESENUM 31
UTILITAIRE ACCESSCHK 33

COPIER-DEPLACER EN NTFS 36

CREER – COPIER- - DEPLACER 36
SENSIBILISATION AUX FINESSES DE L'INTERFACE 36
XCOPY 37
SAUVEGARDE DE FICHIERS 39
ROBOCOPY INVITE DE COMMANDE 41
Ajout d'interface graphique *42*

LIENS SYMBOLIQUES 43

LIENS SYMBOLIQUES - RACCOURCIS: 43
LIENS SYMBOLIQUES – MKLINK : 43
COPIE DE LIENS SYMBOLIQUES: 45
JONCTIONS DE REPERTOIRE – JONCTION: 46
LIENS SYMBOLIQUES - REELS SUR FICHIERS : 47

TP DROITS NTFS 1° 48

OBJECTIF : 48
PERMISSIONS DE PARTAGE : 48
PERMISSIONS DE SECURITE : 48
NOTION DE CREATEUR PROPRIETAIRE : 50

TP DROITS NTFS 2° 51

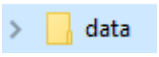
OBJECTIF : 51
GROUPES ET COMPTES : 51
PARTAGES : 52
PERMISSIONS NTFS : 52
CREATEUR PROPRIETAIRE : 54

TP APPROPRIATION DE FICHIER 55

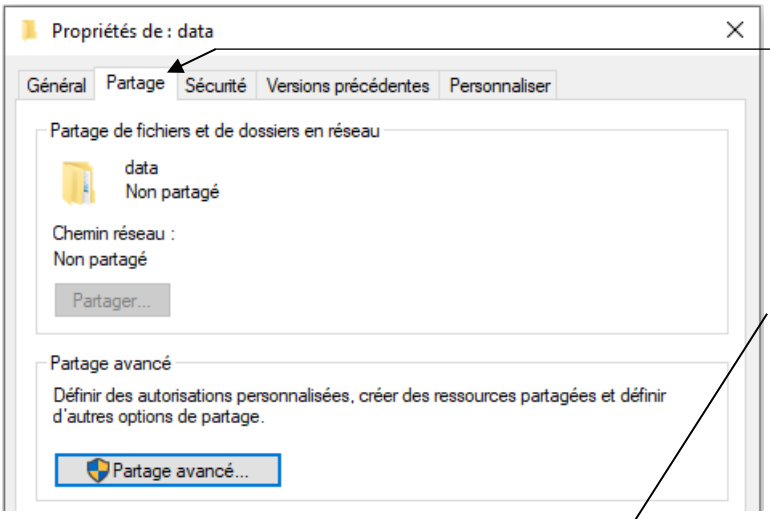
DESCRIPTIF DU PROBLEME : 55
RAISONNEMENT : 56

ACCES AUX PERMISSIONS NTFS

Permissions de Sécurité – Autorisations de Partage :

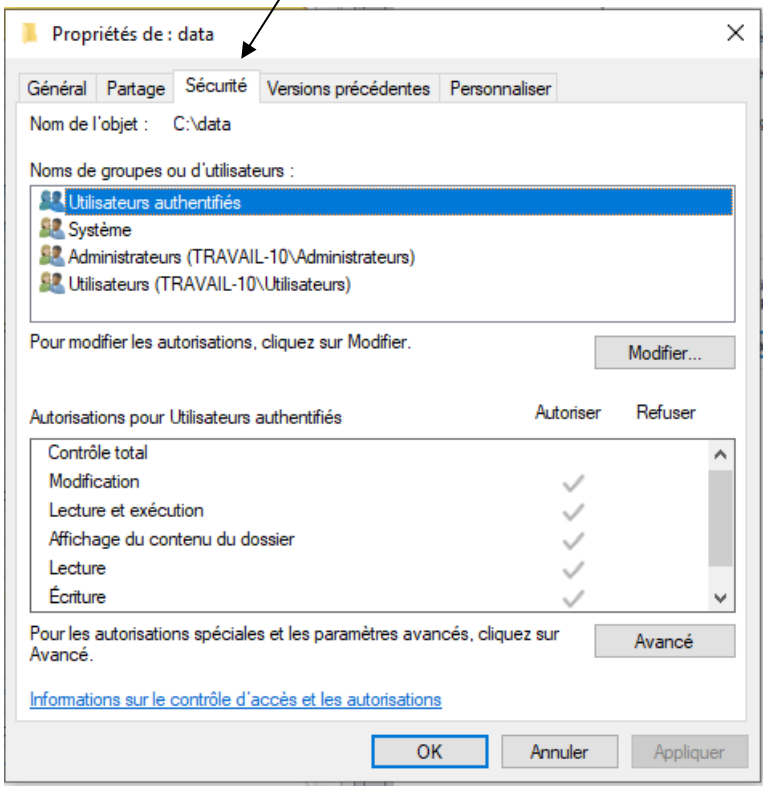
A partir du moment où l'on se trouve sur un lecteur en NTFS en cliquant sur un dossier quelconque 

via les **propriétés** ...



On a bien accès à l'onglet "**Partage**" (pour des autorisations

mais aussi à un onglet "**Sécurité** pour défnir des **permissions**



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 inclues dans les fichiers, dossiers, au niveau du disque lui-même…

Pour gérer les demandes d'accès depuis le réseau on pourrait continuer à travailler avec l'onglet **Partage** et demander **Autorisation**, mais comme ce sont les droits les plus restrictifs qui prédominent… c'est inutile

Donc au niveau "**Partage**" on laissera le **Contrôle Total** à **Tout le monde** et on travaillera essentiellement au niveau de l'onglet **Sécurité** qui permettra de définir des **permissions**

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** (**Access Control List**) 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.

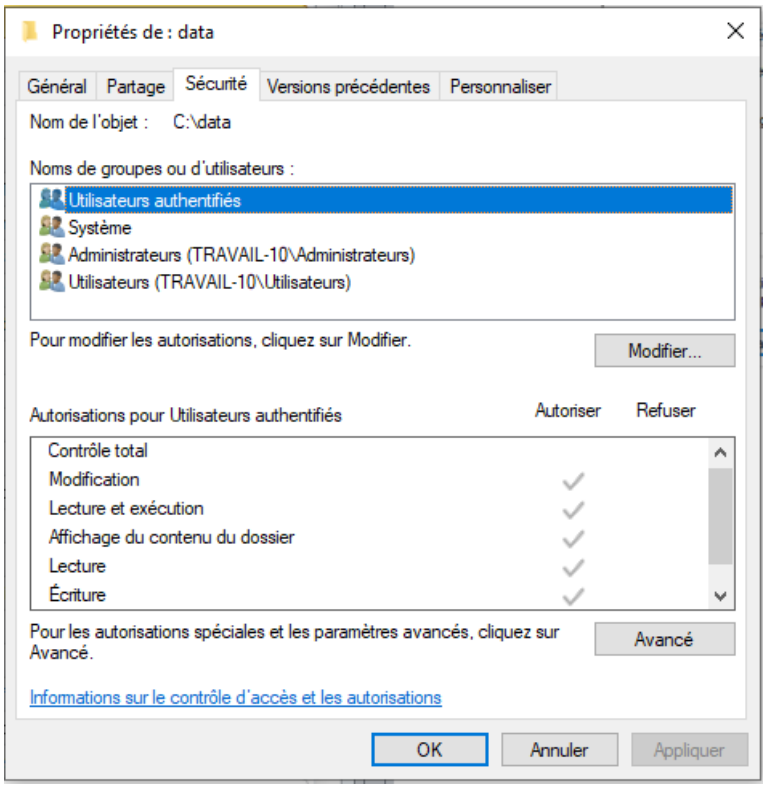
Pour qu'un utilisateur puisse accéder à un fichier ou à un dossier, la liste **ACL** de ce fichier dossier doit contenir une entrée, appelée **ACE** (**Access Control Entry**) auquel l'utilisateur est associé.

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

Permissions NTFS sur Dossiers - Fichiers :

Dossier = 6 autorisations, Fichier = 5 autorisations

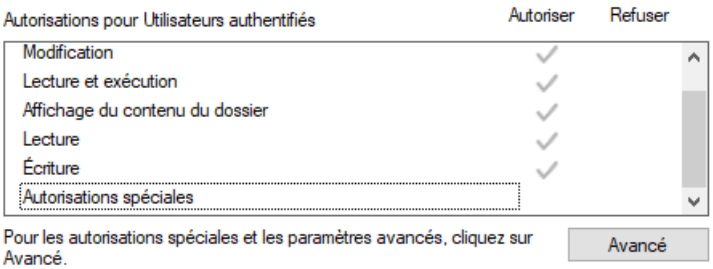
Sur un **dossier** on peut définir 6 sortes de **permissions**, via l'onglet **Sécurité**



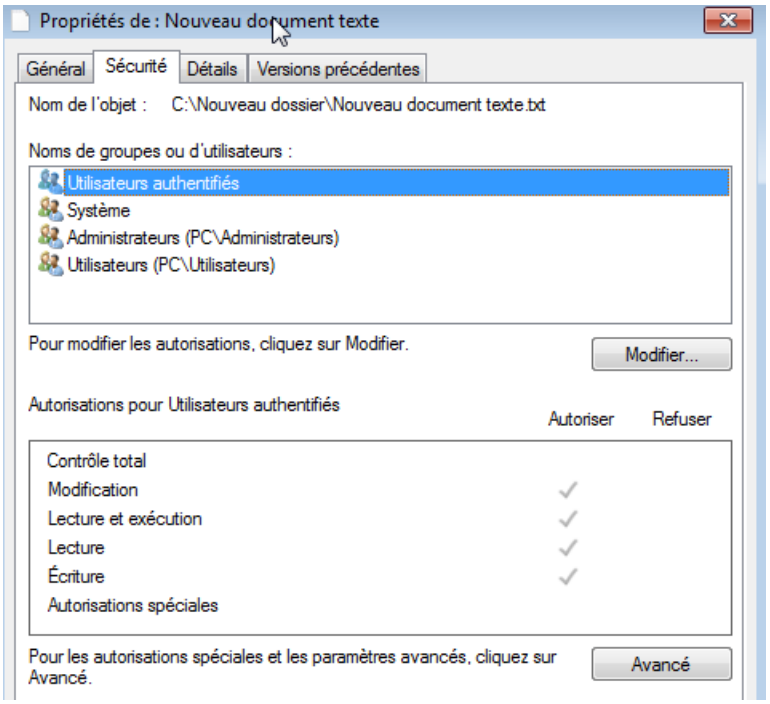
Ces 6 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

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

Les **Autorisations Spéciales,** affichées après les 6 premières, 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	×	×	×	×		
Liste du dossier / Lecture de données	×	×	×	×	×	
Attributs de lecture	×	×	×	×	×	
Lire les attributs étendus	×	×	×	×	×	
Création de fichiers / Écriture de données	×	×				×
Création de dossiers / Ajout de données	×	×				×
Attributs d'écriture	×	×				×
Écriture d'attributs étendus	×	×				×
Suppression de sous-dossiers et de fichiers	×					
Supprimer	×	×				
Autorisations de lecture	×	×	×	×	×	×
Modifier les autorisations	×					
Appropriation	×					
Synchroniser	×	×	×	×	×	×

N.B: Une différence importante entre **Modifier** et **Contrôle Total**, c'est la possibilité de supprimer ou non les sous-dossier … et surtout **Modifier les permissions** et devenir le **propriétaire** (cf chap **Propriété NTFS**)

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,** on dit qu'il a la **« somme des droits »**
3. si la permission "aucun accès" est donnée, cette dernière **prime sur les autres permissions**, et la permission effective est "aucun accès" on dit que **« un refus explicite est opposable a tout»**

Donc, en résumé, si l'utilisateur est membre de plusieurs groupes, la permission résultante 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

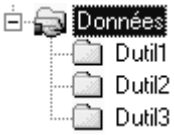
Q: Quelle est la permission effective de **Util1** lorsqu'il accède au fichier **A** à travers **une session locale** sur la machine ?

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 créé avec à l'intérieur 3 sous-dossiers nommés **Dutil1**, **DuitI2** 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

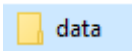
Q : Quelle est la permission effective de **Util2** pour le dossier **Dutil1**

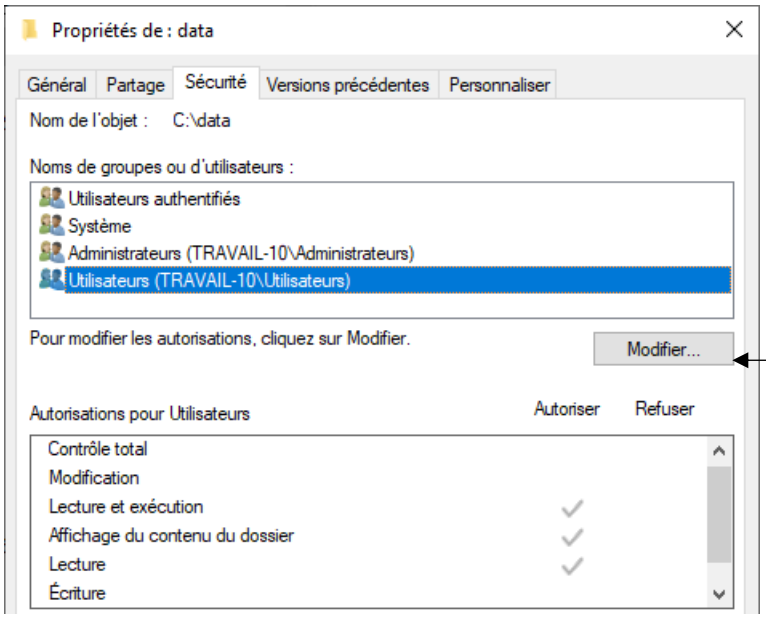
R : Util2 ne bénéficie pas de l'accès au dossier Dutil1 car la permission NTFS contrôle total sur ce dossier a été attribuée uniquement à Utils1

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, voire de la racine du disque ! Visuellement cela se traduit par le fait que les propriétés sont grisées, et semblent donc non modifiables.

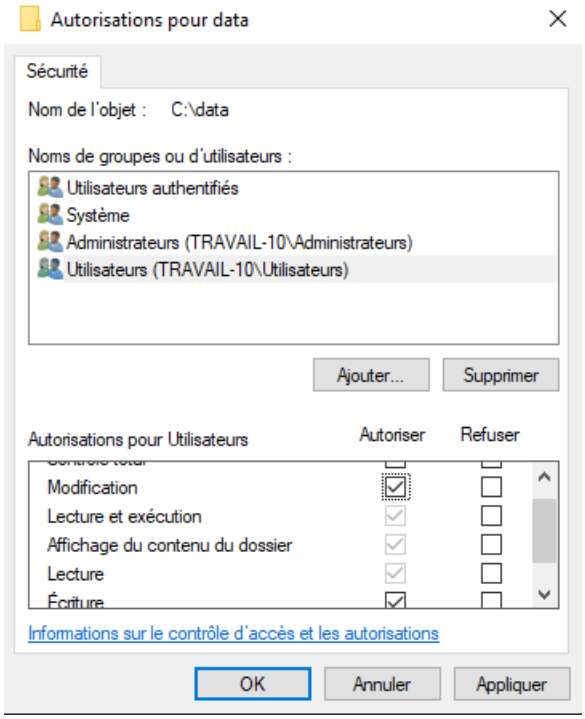
Notre dossier ***data*** 



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

On ne peut pas modifier les permissions « existantes, » qui apparaissent grisées…

Mais si on en a les droits, on peut toujours venir « ajouter » des autorisations à coté de celles héritées… par exemple, via **Modifier…**

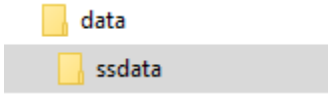


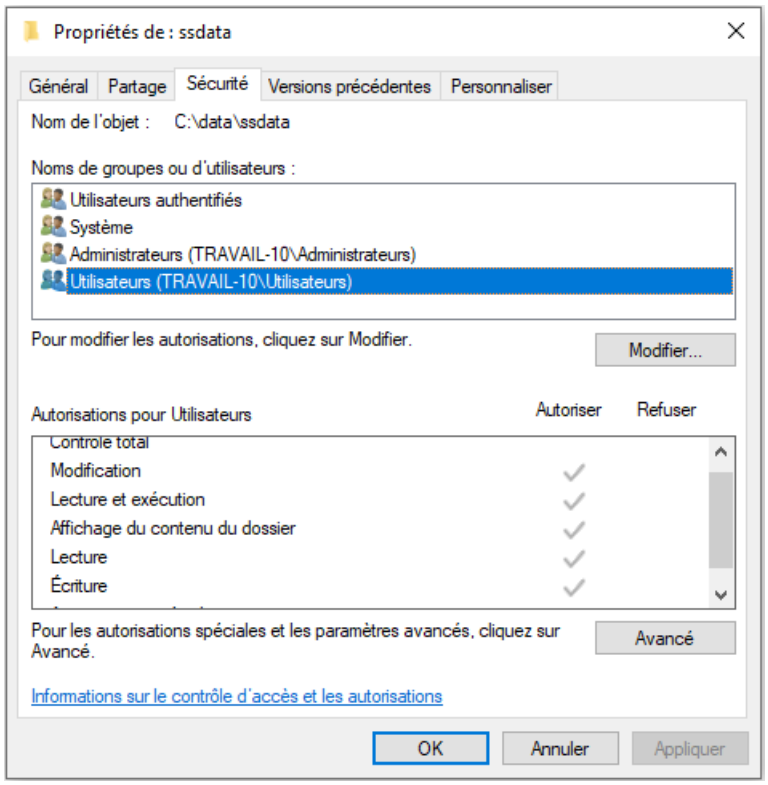
pour le groupe des **Utilisateurs** on demande **Ajouter** …

et on coche **Modification** (Ecriture se coche automatiquement)

Si on modifie les permissions des **parents**, ont concernés alors ensuite dans l'arborescence ceux qui ont accepté l'héritage. (par défaut tous)

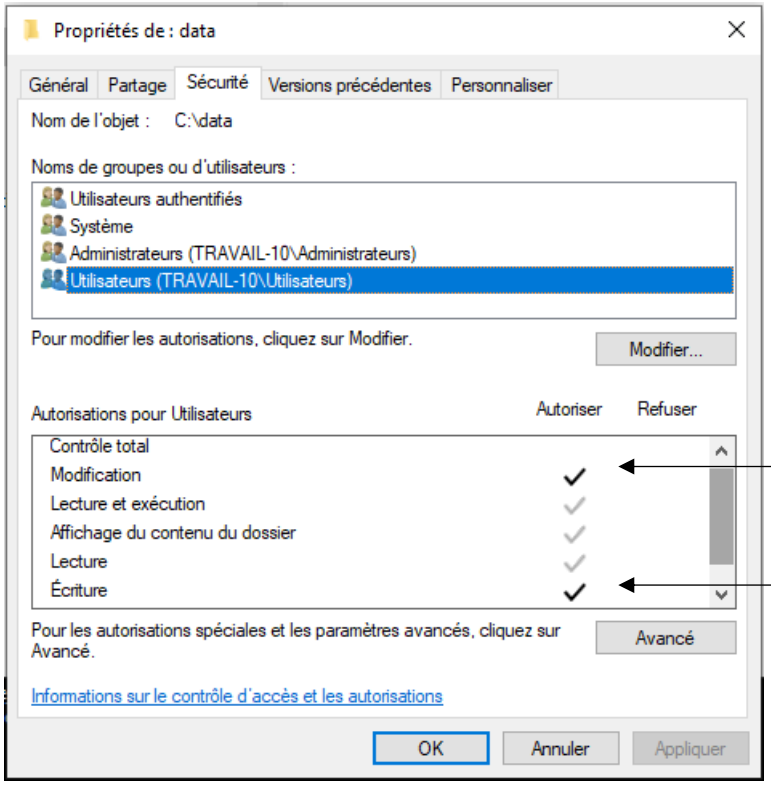
Si on se crée un sous dossier ***ssdata***





alors le groupe des **Utilisateurs** est en "***lecture seule***", par héritage…

Et le lien **d'héritage** est permanent, c'est-à-dire que si on revient sur le dossier ***data*** et que l'on décoche **Modification / Ecriture** (qui sont accessibles), et bien la modification se propagera sur le dossier ***ssdata***



Si via **Modifier**, on décoche pour les **Utilisateurs** les permissions **modifications / lecture**, cela s'appliquera au dossier ***ssdata***

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

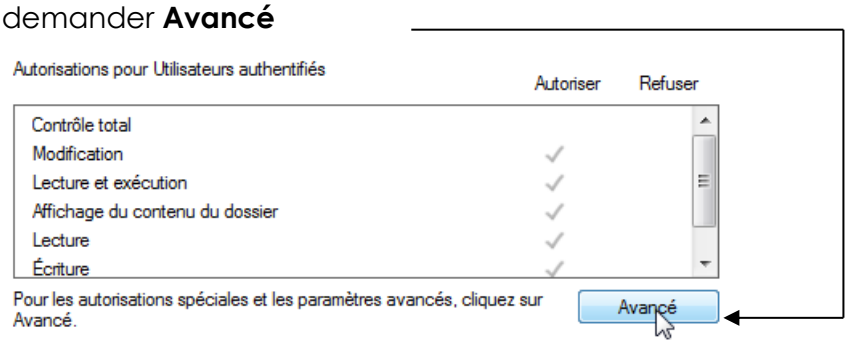
- Exécutez les modifications sur l'objet parent ; l'objet héritera alors de ces autorisations.
- Sélectionnez l'autorisation opposée (**Autoriser** ou **Refuser**) pour contrer l'autorisation héritée.
  PEU CONSEILLE !
- Casse l'héritage en désactivant la case à cocher
  Permettre aux autorisations pouvant 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 jamais de l'objet parent…

Casser un héritage – interface windows 10

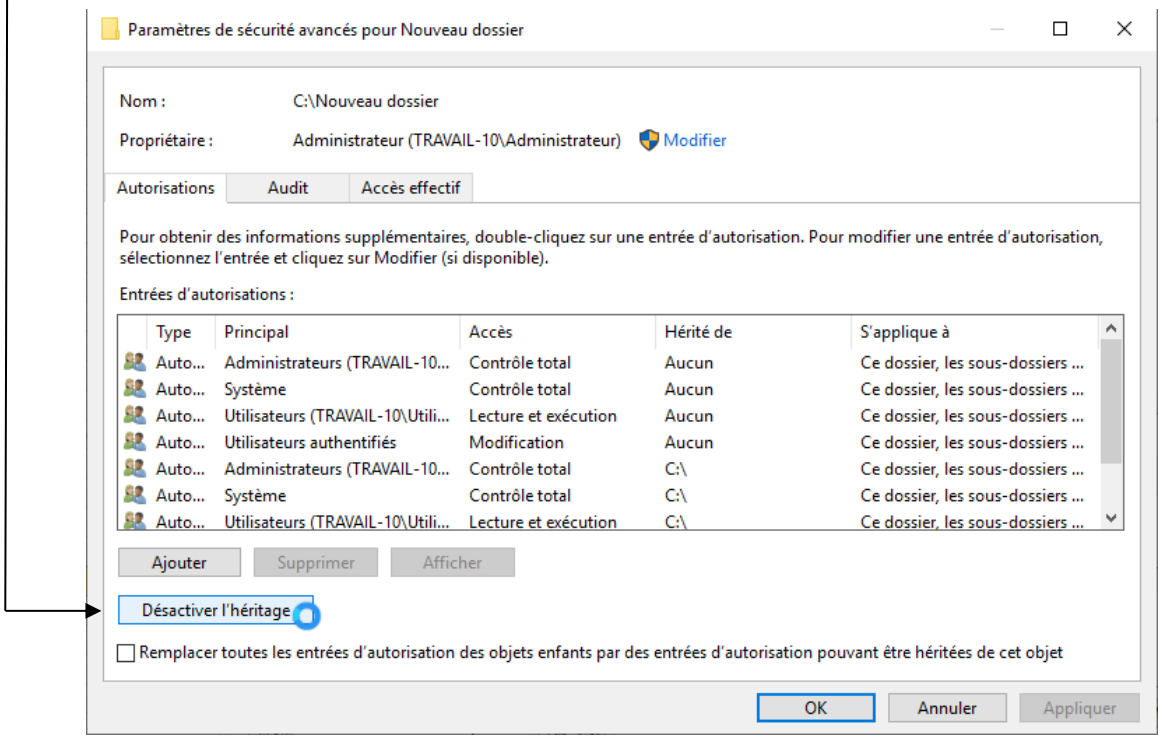
N.B : si on veut pouvoir **modifier directement les permissions**, il est nécessaire d'abords de casser **l'héritage (ex : seven** désactiver la case à cocher **« Inclure les autorisations pouvant être héritées du parent… »)**

Par exemple pour le **Groupe utilisateur authentifiés** d'un **Nouveau Dossier**

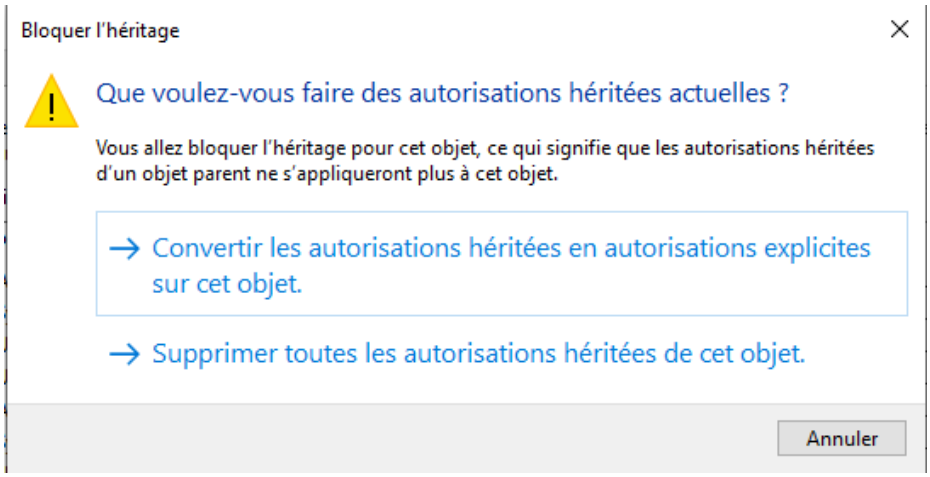
Il faut demander **Avancé**



Désactiver l'héritage

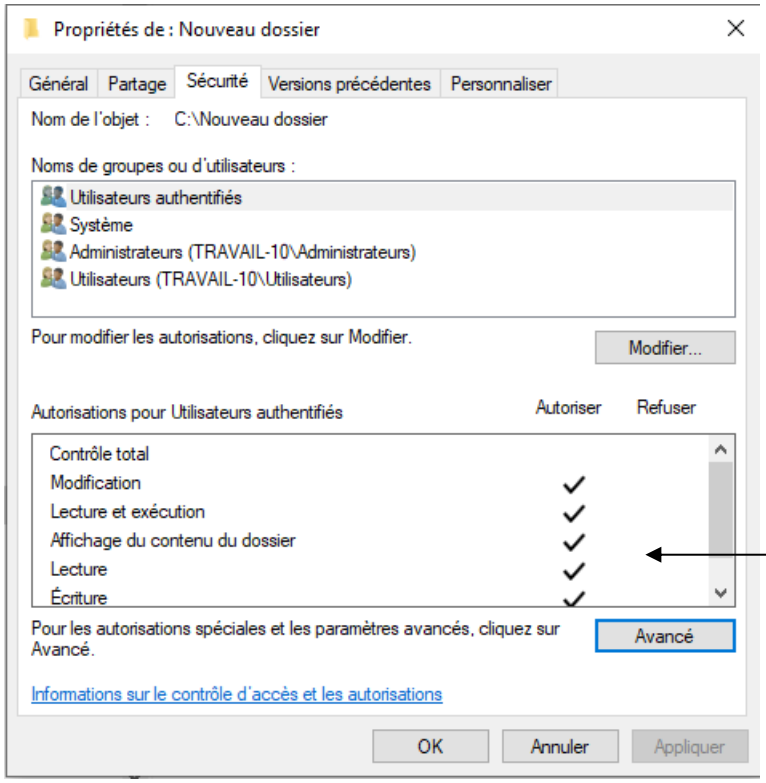


Dans ce cas, on peut choisir si on veut les **supprimer** complètement ou les **convertir (ajouter)** à notre arborescence (et pouvoir ensuite les modifier…)



Convertir… = repartir de l'existant

Si on demande **Convertir les autorisations…** suivit de **Ok (appliquer)**



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

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

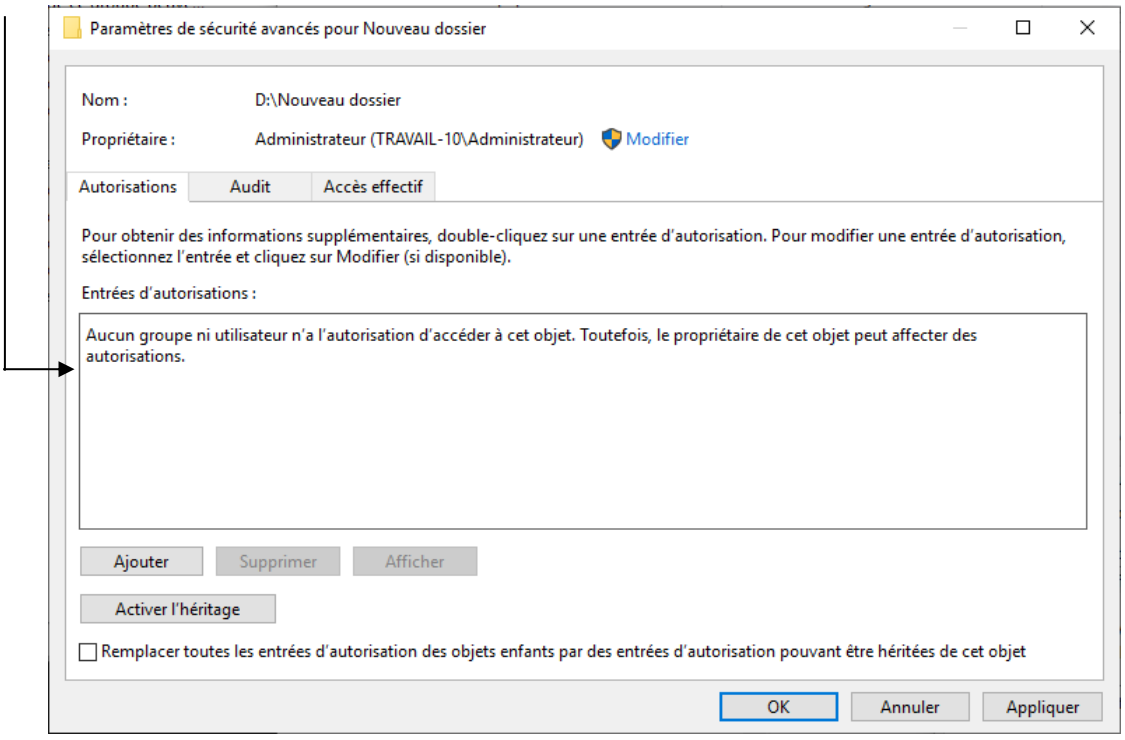
On peut ici à partir de l'existant,

- Modifier ce que l'on veut,
- Ajouter ce que l'on veut

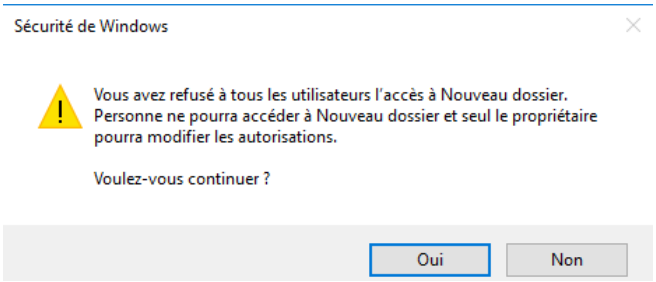
N.B :c'est la technique conseillée lorsque l'on doit intervenir dans une zone, notamment système, pour effectuer des modifications !

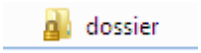
Supprimer… = repartir de zéro

Si on demande **Supprimer** Windows 10-11 nous informe…que l'on se retrouve si on reste ainsi, sans aucune **permissions** de posée sur le dossier !



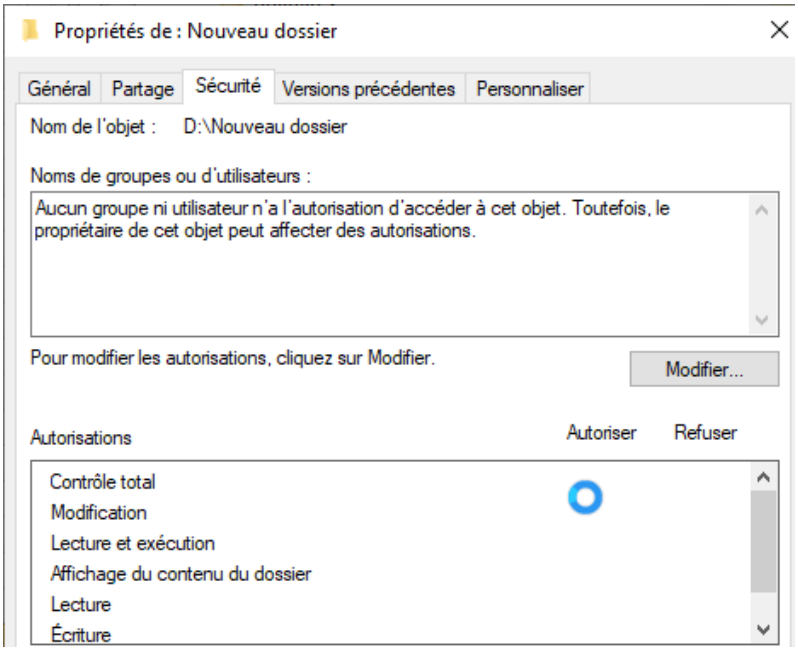
Si on valide Appliquer quand même, une 2° mise en garde apparaît… mais bon… Si on répond NON, l'opération est annulée





Seul le propriétaire pourra modifier ce dossier désormais…

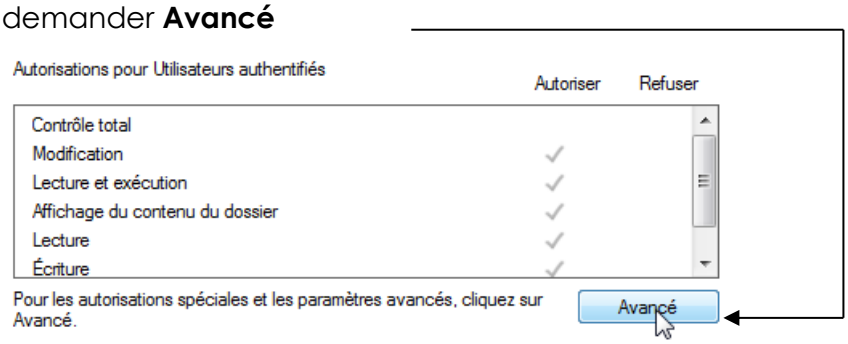
Si on répond OUI, c'est le moment d'indiquer qui peut avoir accès via **Modifier**



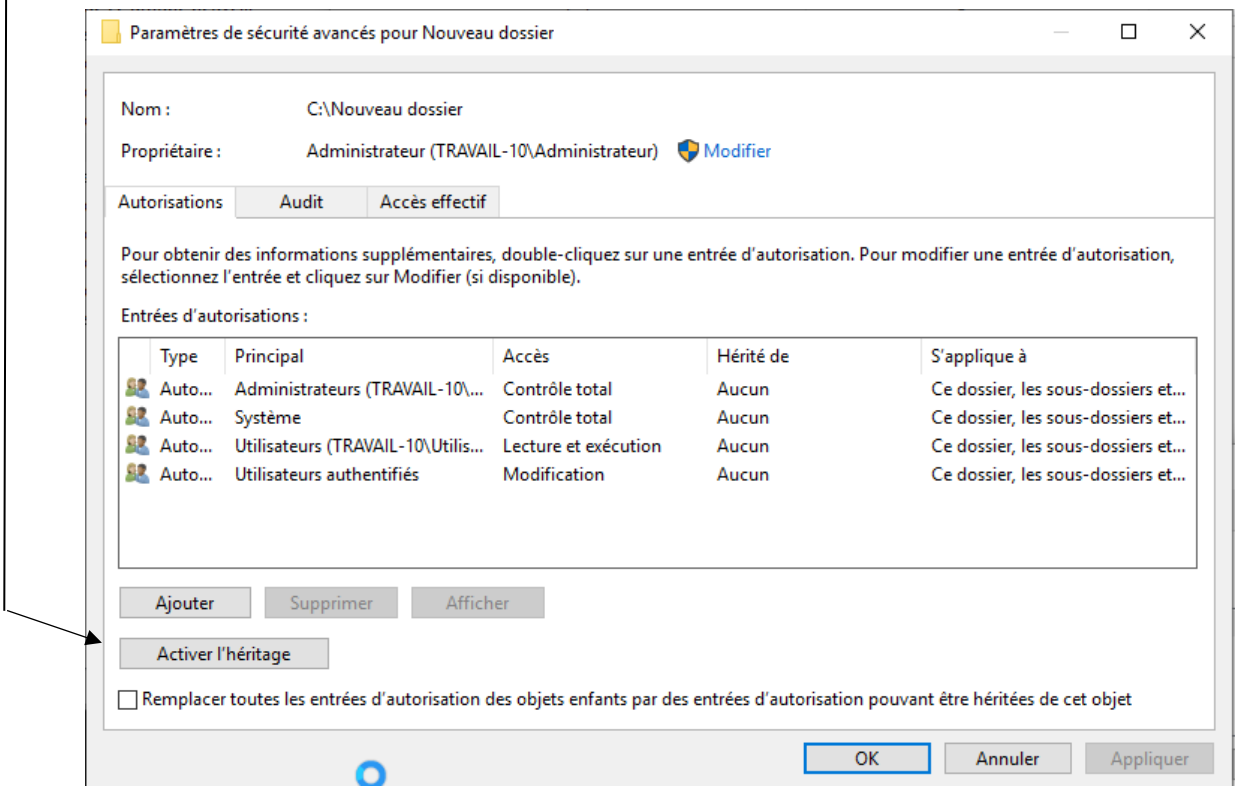
Recréer un héritage – interface windows 10

N.B : lorsque l'on recrée un **héritage**, on n'efface pas les éventuelles modifications qui auraient été apportées !!!! ELLES RESTENT VALABLES !

Il faut demander **Avancé**



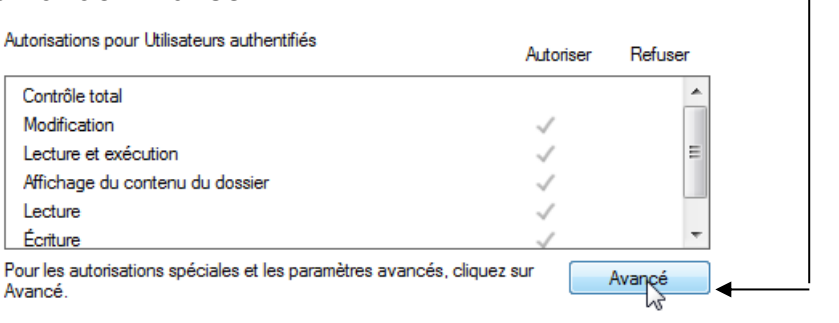
Activer l'héritage



Recréer un ou plusieurs héritages – Windows 10

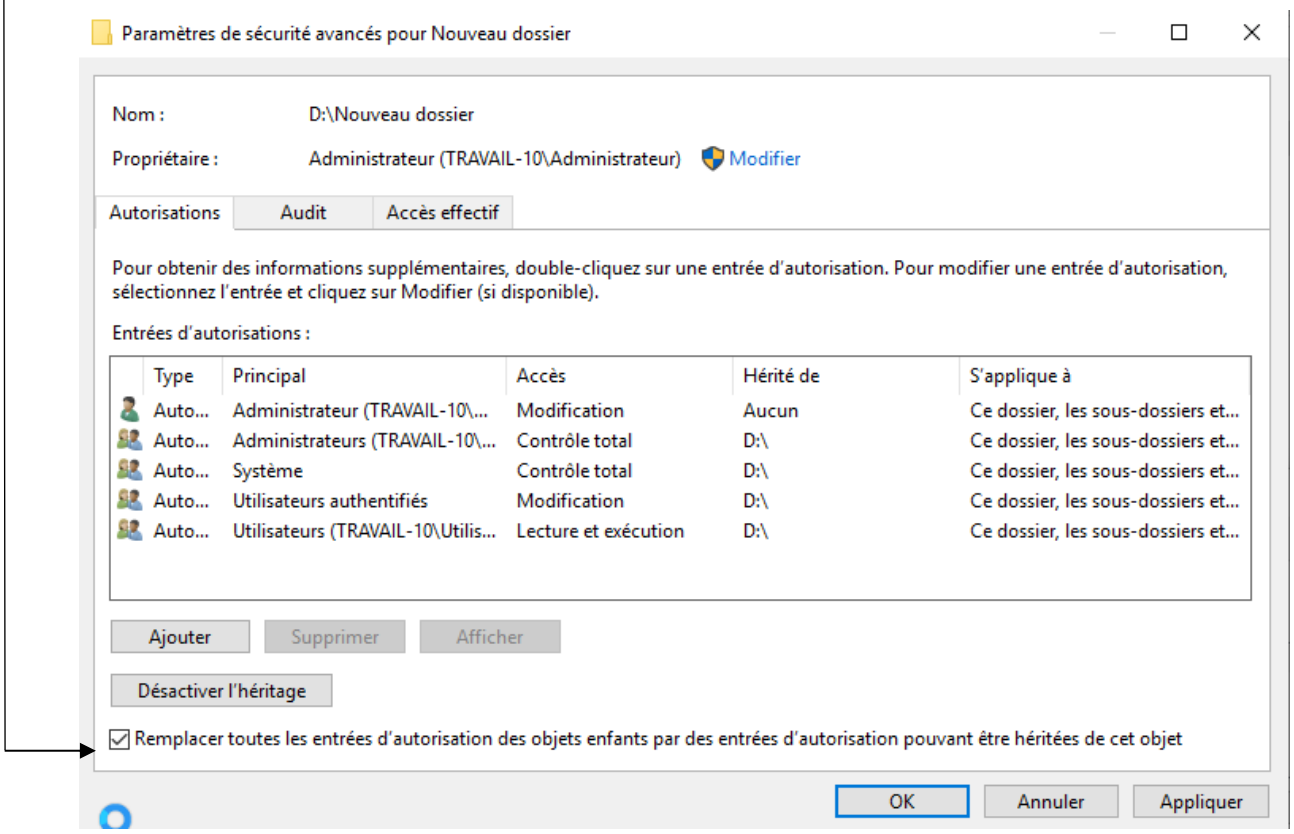
On ne souhaite pas récupérer un héritage du niveau de dessus, mais on souhaite propager vers le bas nos réglages…

Il faut se placer sur le dossier dont on veut propager vers le bas la sécurité, puis demander **Avancé**

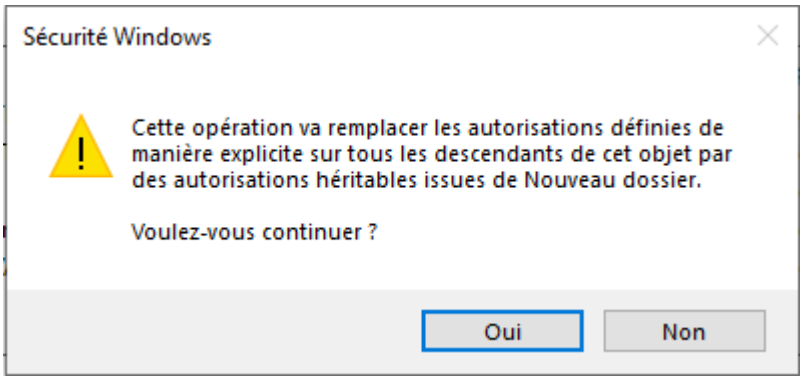


Et là on coche la case

Remplacer toutes les entrées d'autorisation des objets enfants….



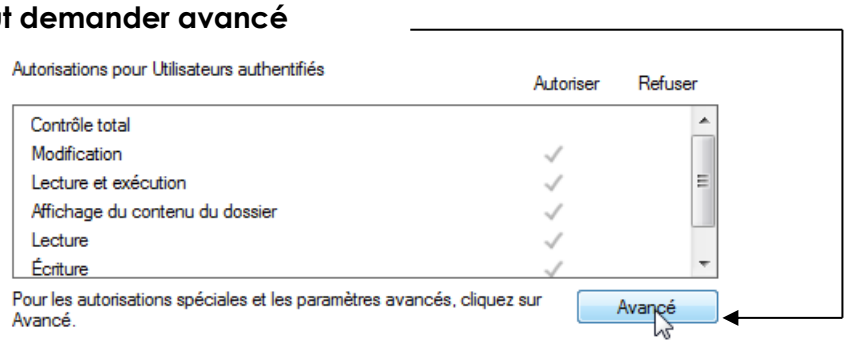
Et on confirme



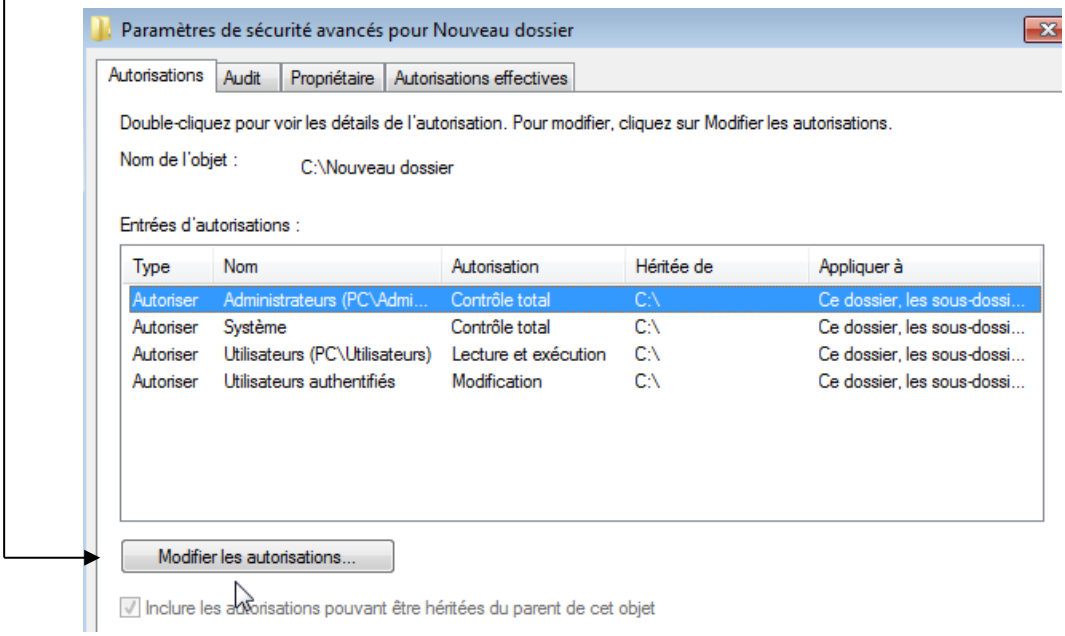
Casser un héritage – interface 7

N.B : si on veut pouvoir **modifier directement les permissions,** il est nécessaire d'abords de casser **l'héritage** Par exemple pour le **Groupe utilisateur authentifiés** d'un **Nouveau Dossier**

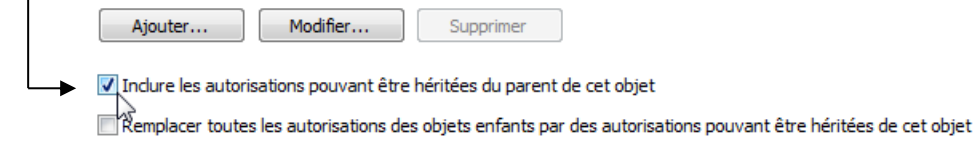
Il faut demander avancé



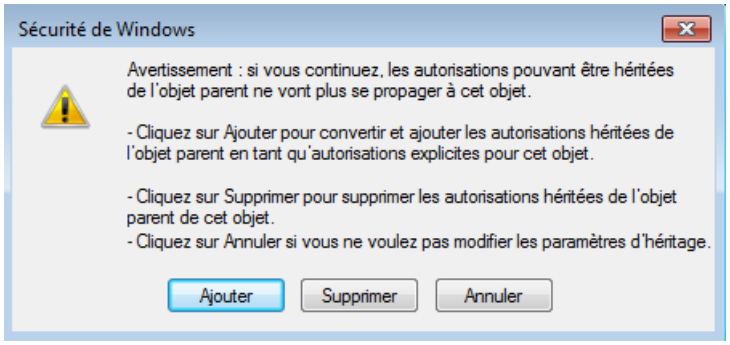
Modifier les autorisations



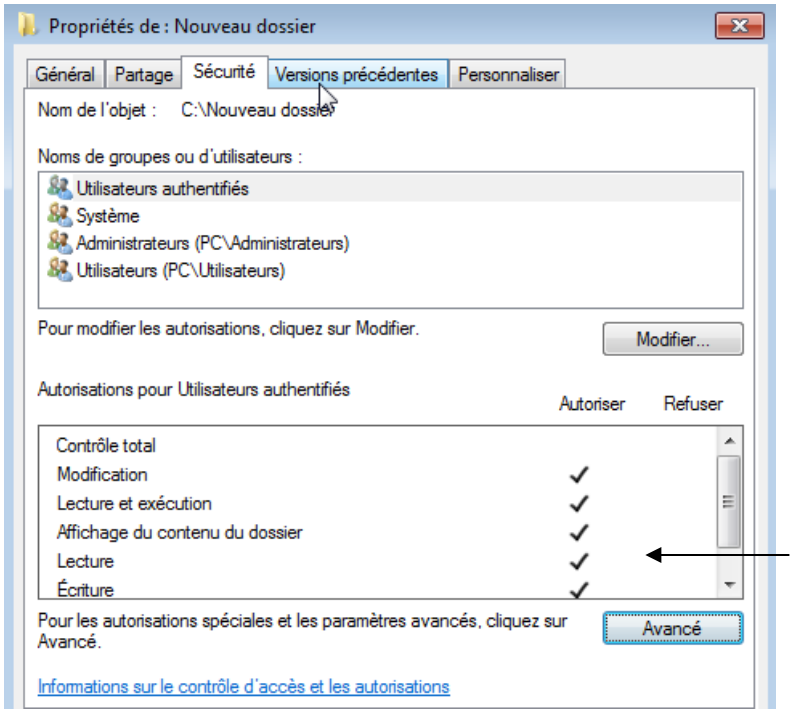
Décocher



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



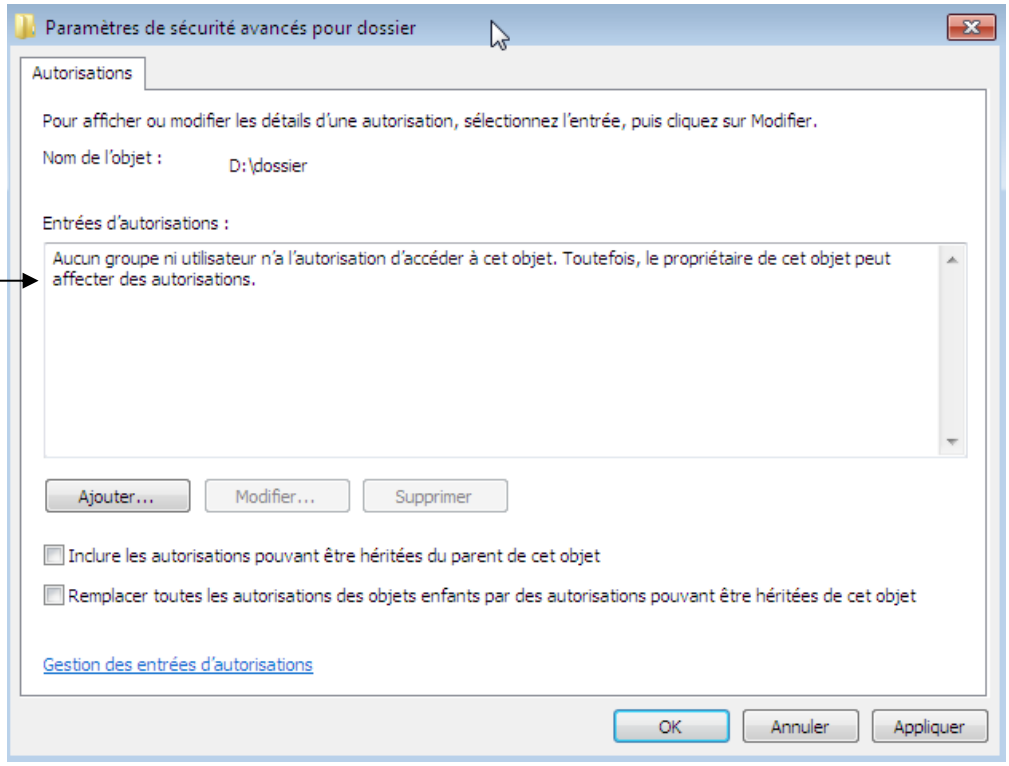
Si on demande **Ajouter** suivit de **Ok / Ok**



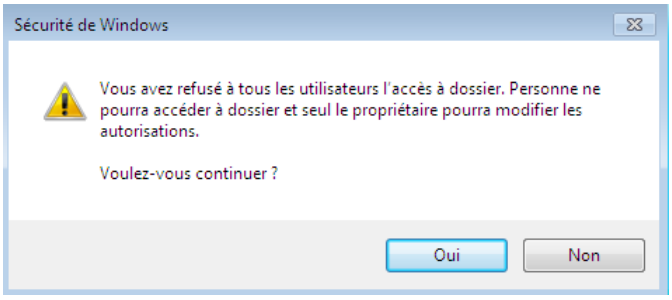
Ces 5 combinaisons standard, ne sont plus **héritées** (dans ce cas elles sont noires)

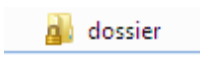
Et ont deux valeurs possibles **Autoriser**, ou **Refuser**

Si on demande **Supprimer** Windows seven nous informe…



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





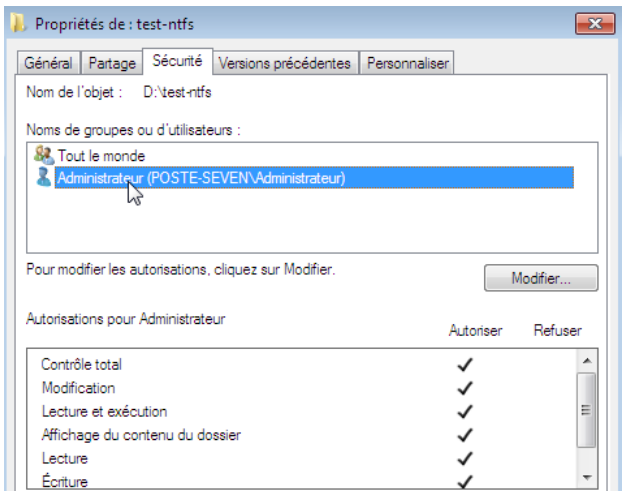
Seul le propriétaire pourra modifier ce dossier désormais…

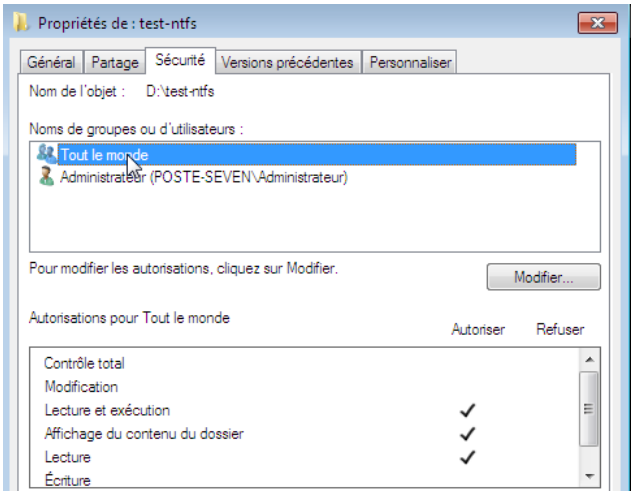
Recréer un héritage interface 7

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

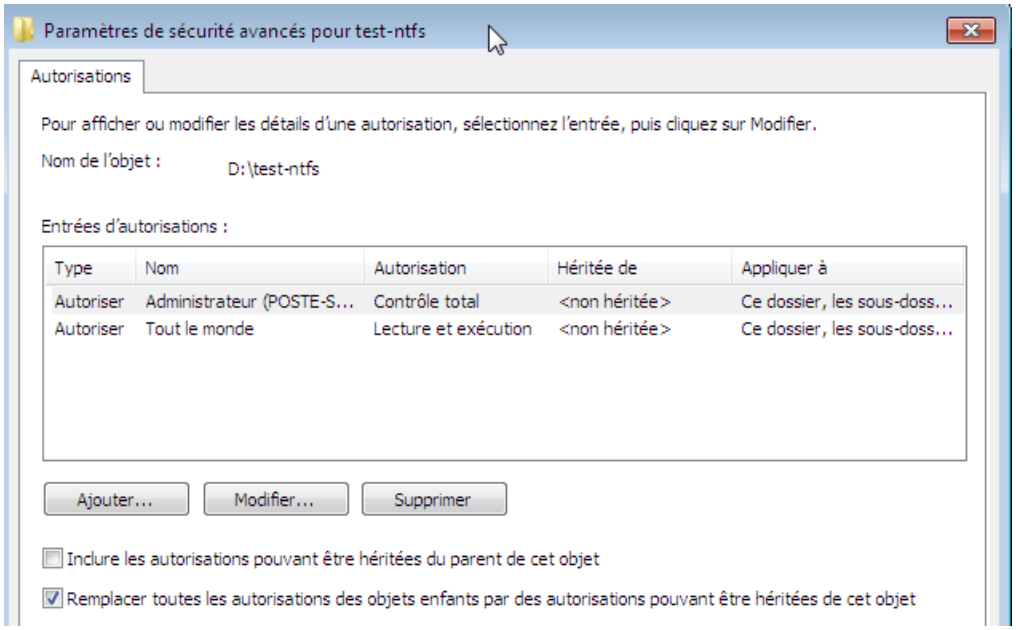
Groupe Tout le Monde Lecture Seule



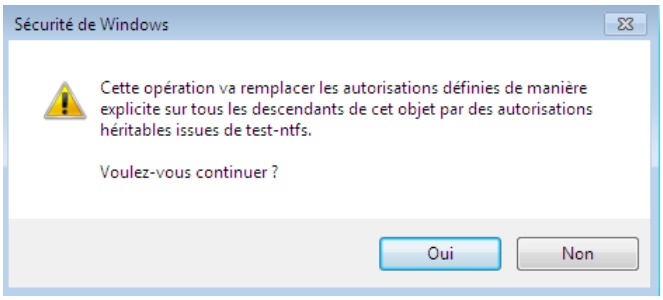


On crée un sous dossier **sous-test**. Vérifier de quoi ce sous dossier hérite…

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 – interface 7

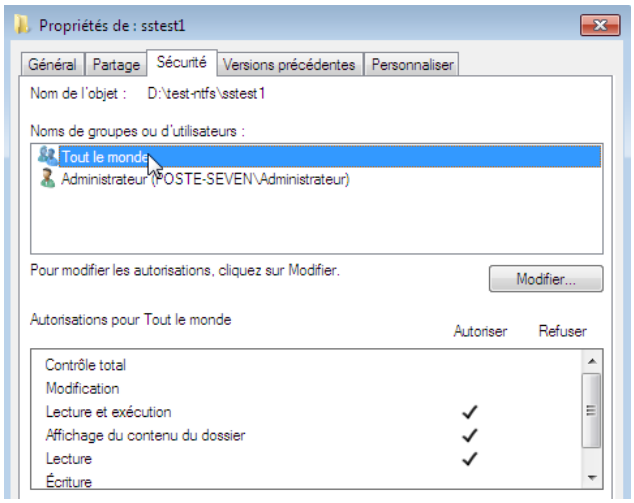
Soit un dossier **test-ntfs**, sur lequel, après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

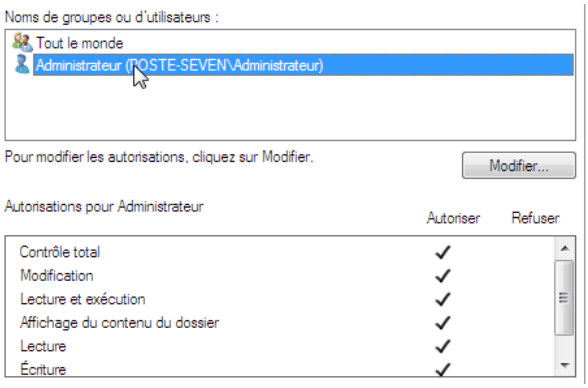
Compte **Administrateur** **Contrôle Total**

Groupe **Tout le Monde** **Lecture Seule**

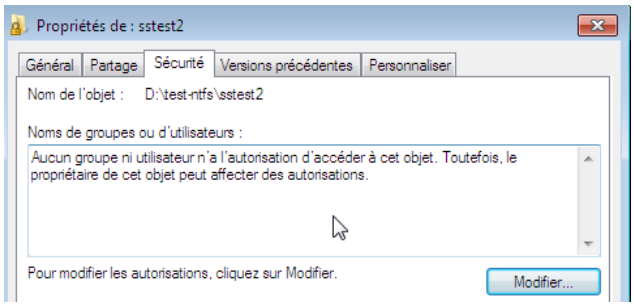
On construit trois sous-dossiers, respectivement **sstest1**, **sstest2**, **sstest3**, qui héritent donc a priori de la sécurité du dossier parent.

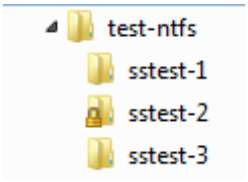
pour **sstest1** on, casse l'héritage en copiant les permissions…



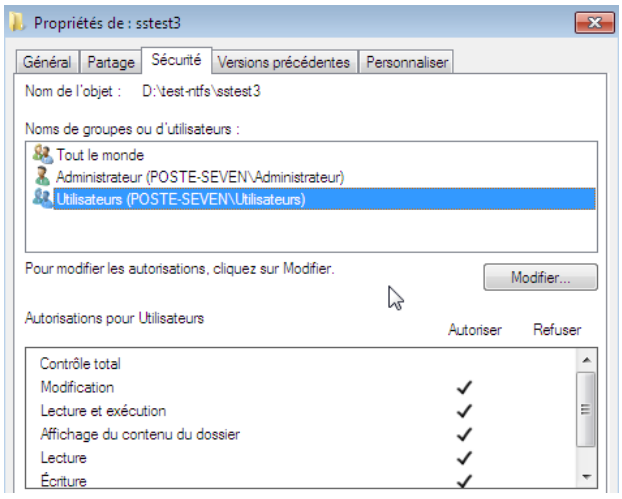


pour **sstest2** on, casse l'héritage en supprimant les permissions…





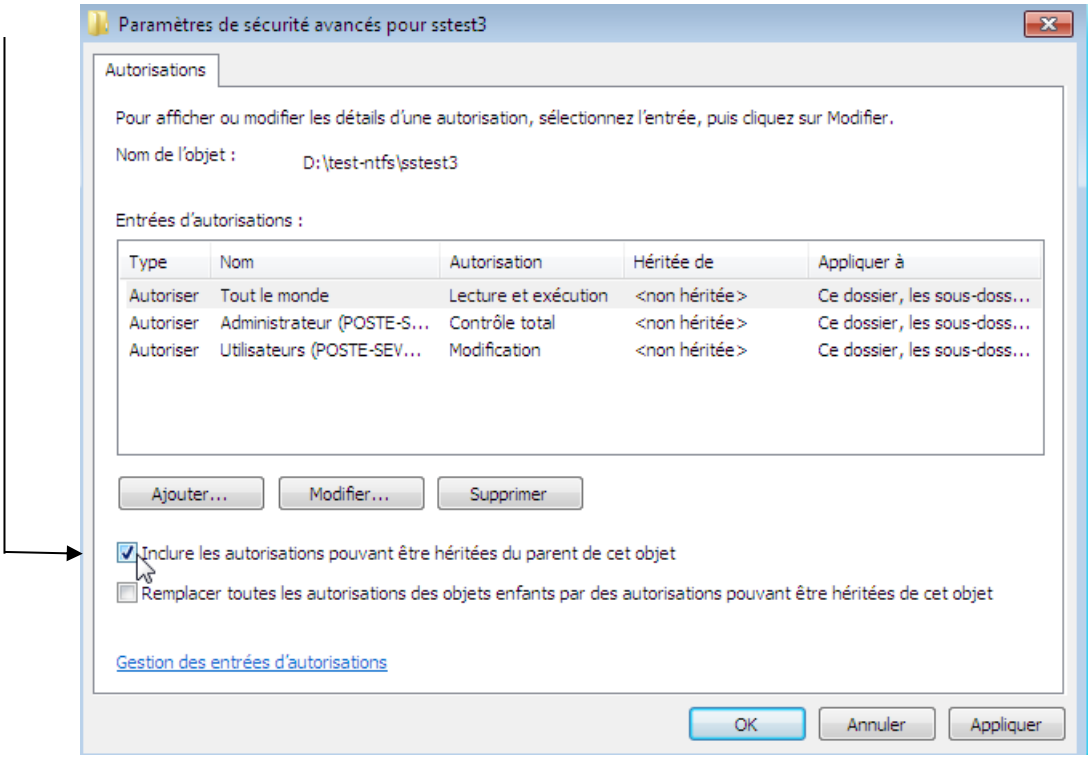
pour **sstest3** on, casse l'héritage en copiant les permissions et ajout du groupe des **Utilisateurs**- en **Modifier**…



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

  Il faut depuis le dossier **sstest3**,

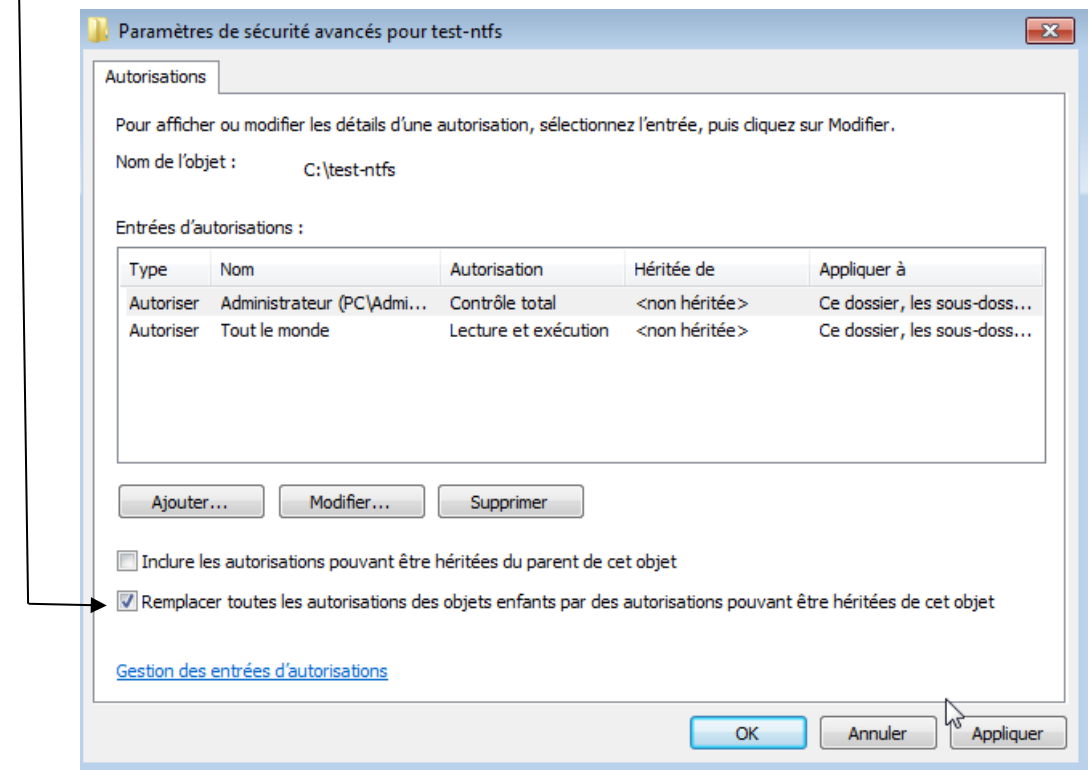
  1. Demander d'effacer toute la sécurité
  2. Demander la case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet (ou activer l'héritage)**



- 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

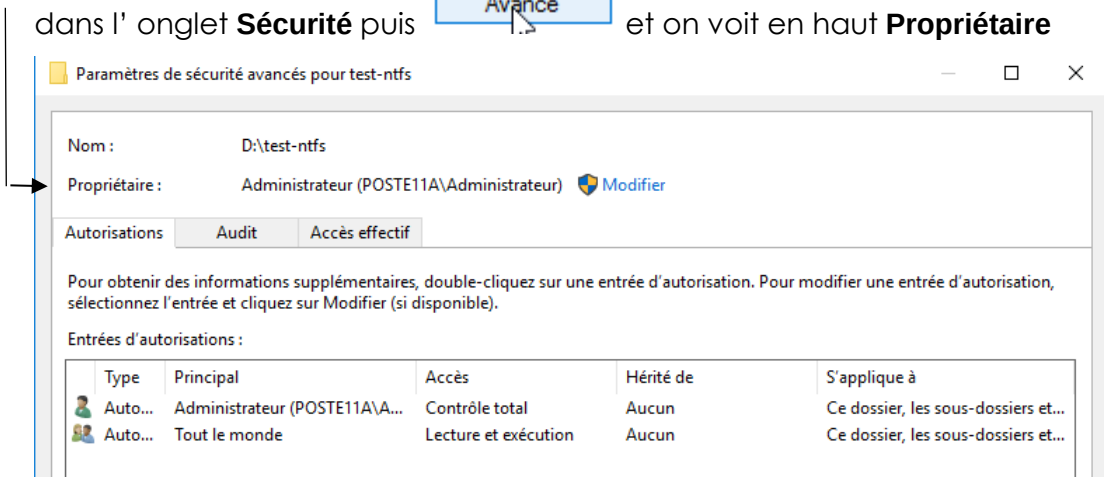
Notion de Propriété

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

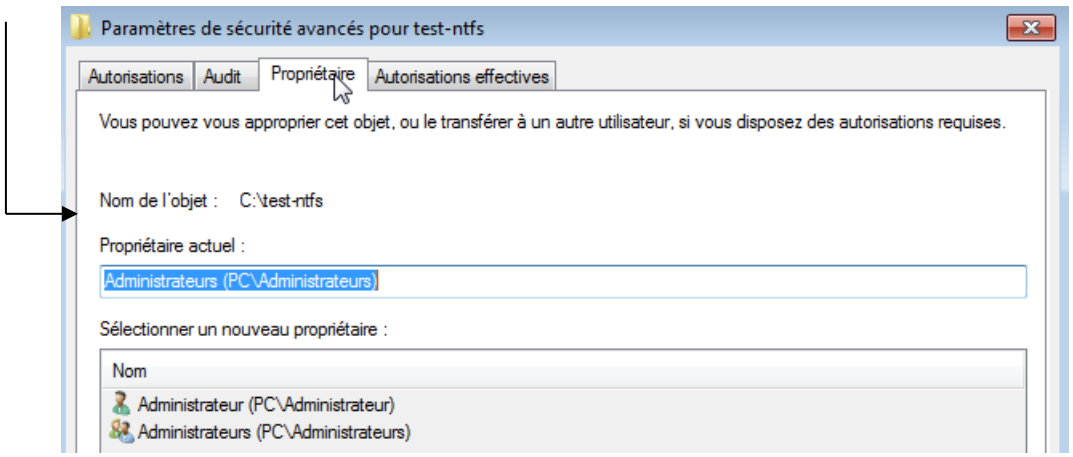
C'est la raison du groupe prédéfini **Créateur Propriétaire**, qui est géré automatiquement par Windows (on ne peut spécifier qui fait partie de ce groupe, ni savoir qui en fait partie… cela dépends de l'objet que l'on pointe !)

N.B : En tant que "**propriétaire**" on peut toujours redéfinir les permissions de son dossier ou de son fichier. Indépendamment du fait que l'on soit explicitement mentionné dans les droits d'accès !

Sous **Windows 10** Pour connaître qui est propriétaire d'un objet, on demande dans l' onglet **Sécurité** puis Avancé et on voit en haut **Propriétaire**



Sous **Windows 7** Pour connaître qui est propriétaire d'un objet, on demande dans l' onglet **Sécurité**, puis Paramètres avancés onglet **Propriétaire**



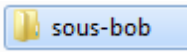
Prendre possession des dossiers et fichiers

On peut s'approprier un objet :

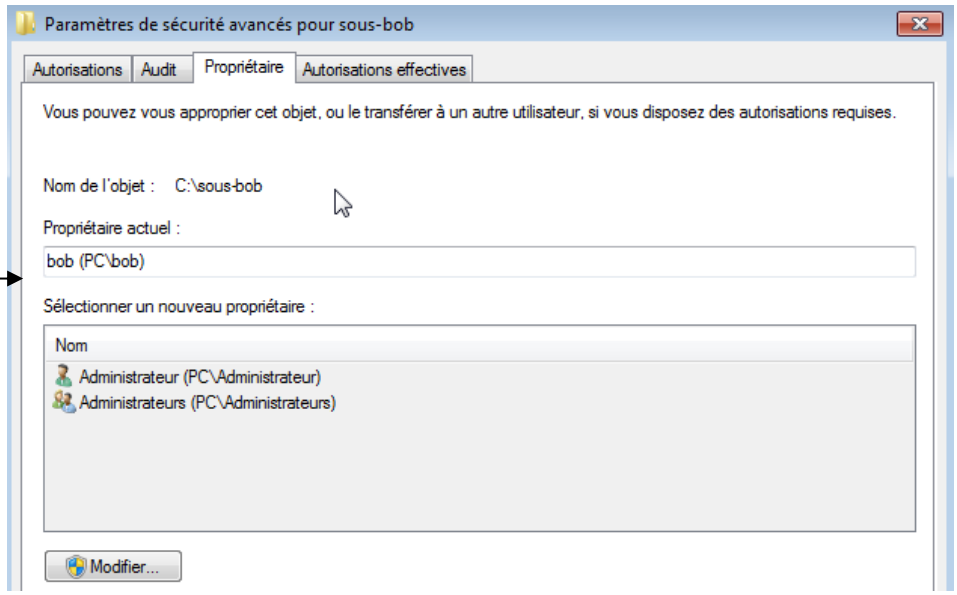
- si l'on est administrateur
- si on en a "les droits" (explicitement donnés)

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

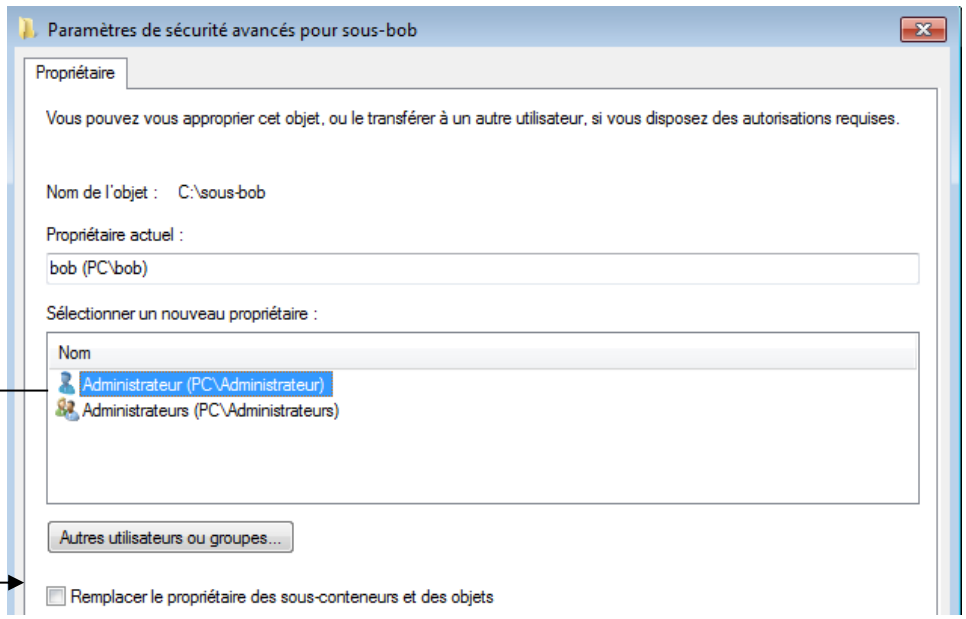
Imaginons que cela soit bob qui ait crée le dossier **sous-bob**



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

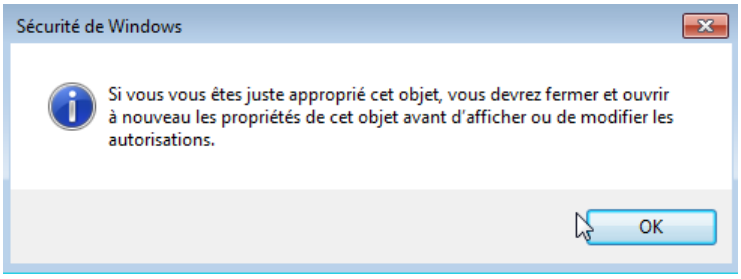


Mais on peut s'approprier l'objet

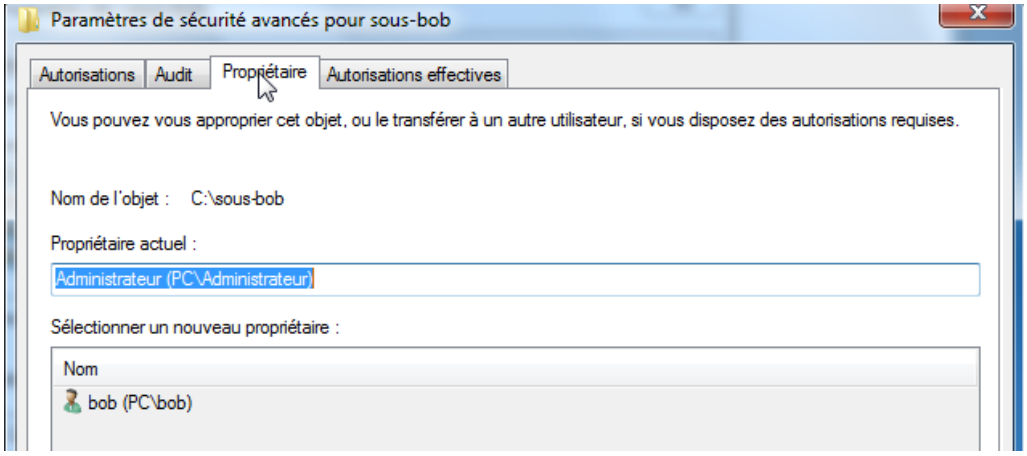


Et éventuellement tout le contenu de l'arborescence…

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

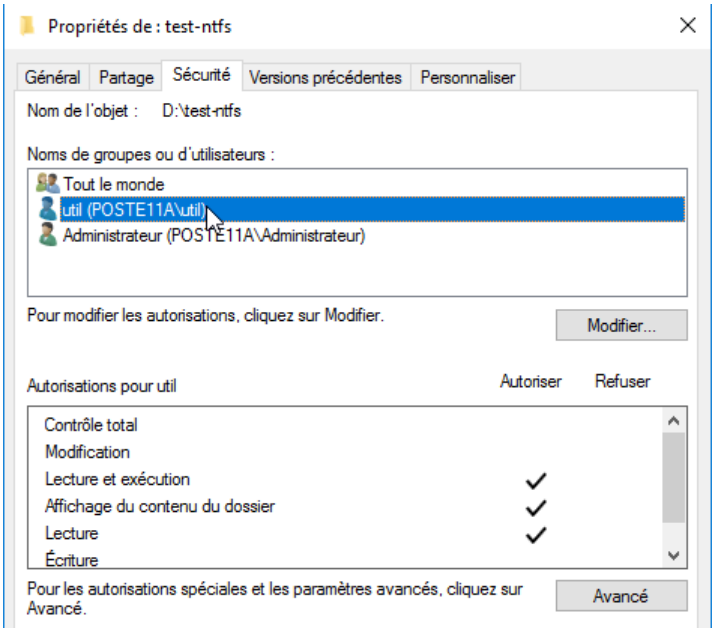


Donner l'autorisation d'appropriation

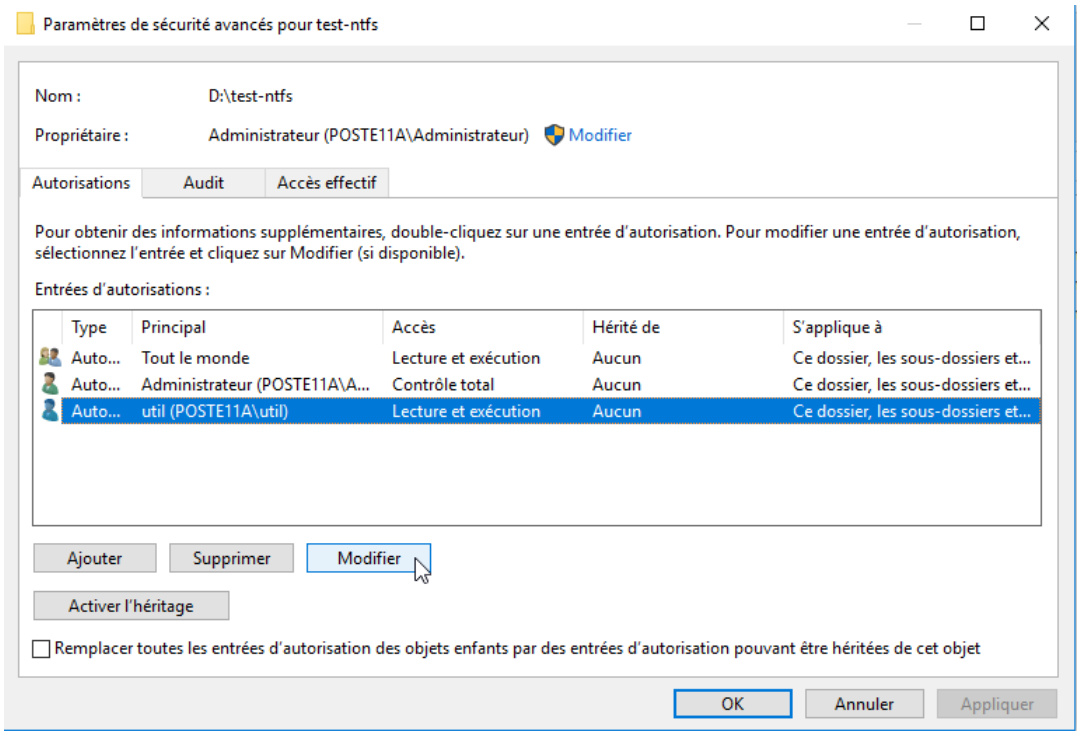
Il est donc possible de donner attribuer la permission "**Appropriation**" aux autres utilisateurs ou groupe en passant par les autorisations avancées…

Imaginons vouloir donner à un utilisateur ***util*** le droit de s'approprier un dossier ***test-ntfs.***

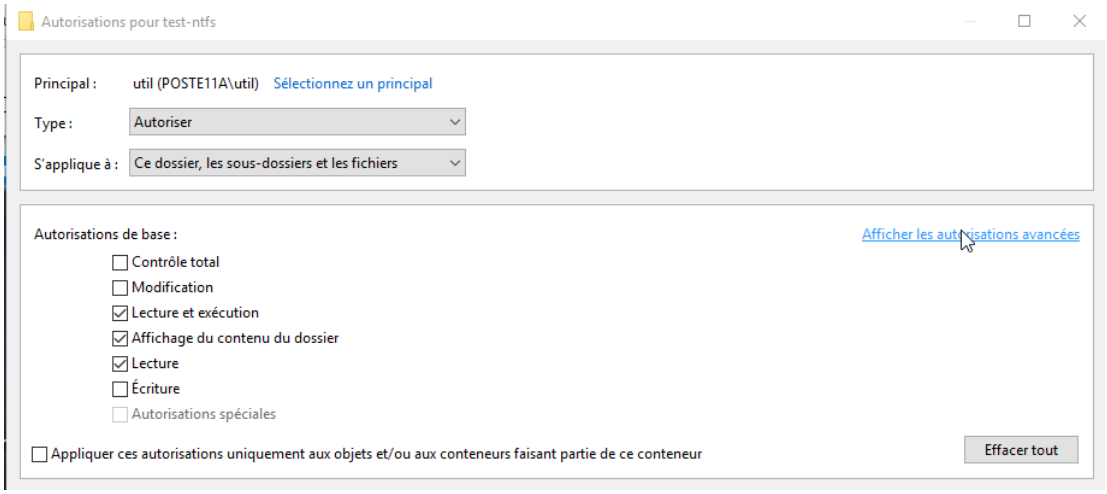
On se place sur le dossier ***test-ntfs***, on demande **Propriétés**, Onglet **Sécurité**, on se place sur l'utilisateur à qui l'on veut donner les droits d'appropriation et on demande **Avancé**



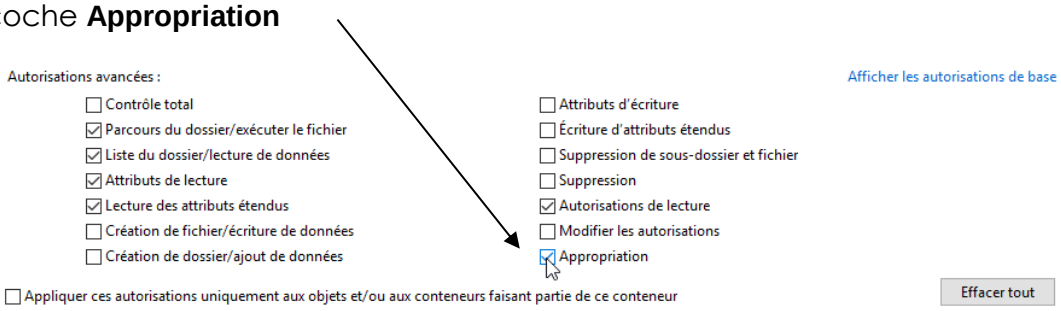
On sélectionne l'utilisateur et on demande Modifier



Puis on demande **Afficher les autorisations avancées**

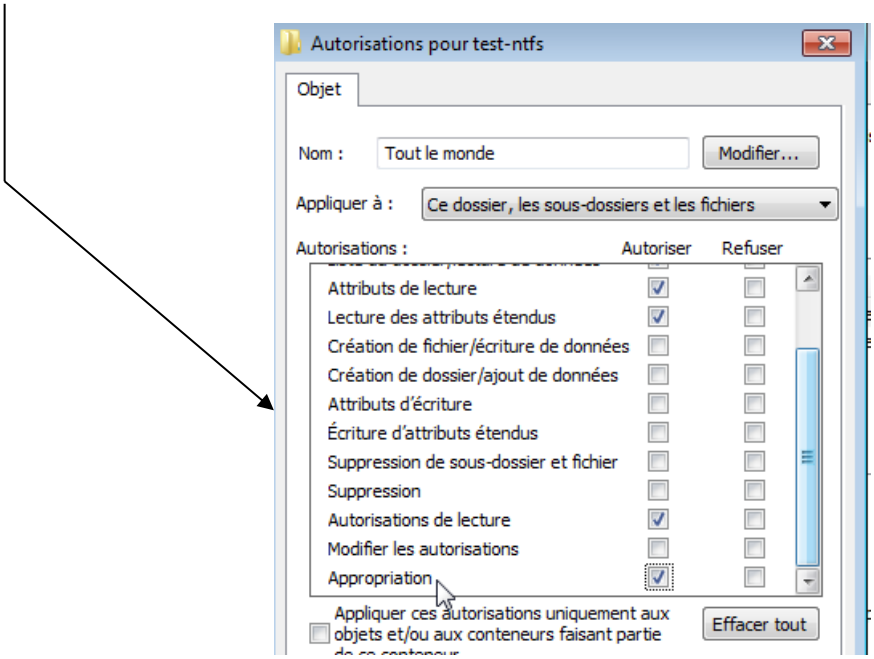


Et on coche **Appropriation**



Suivit de OK, Appliquer, OK

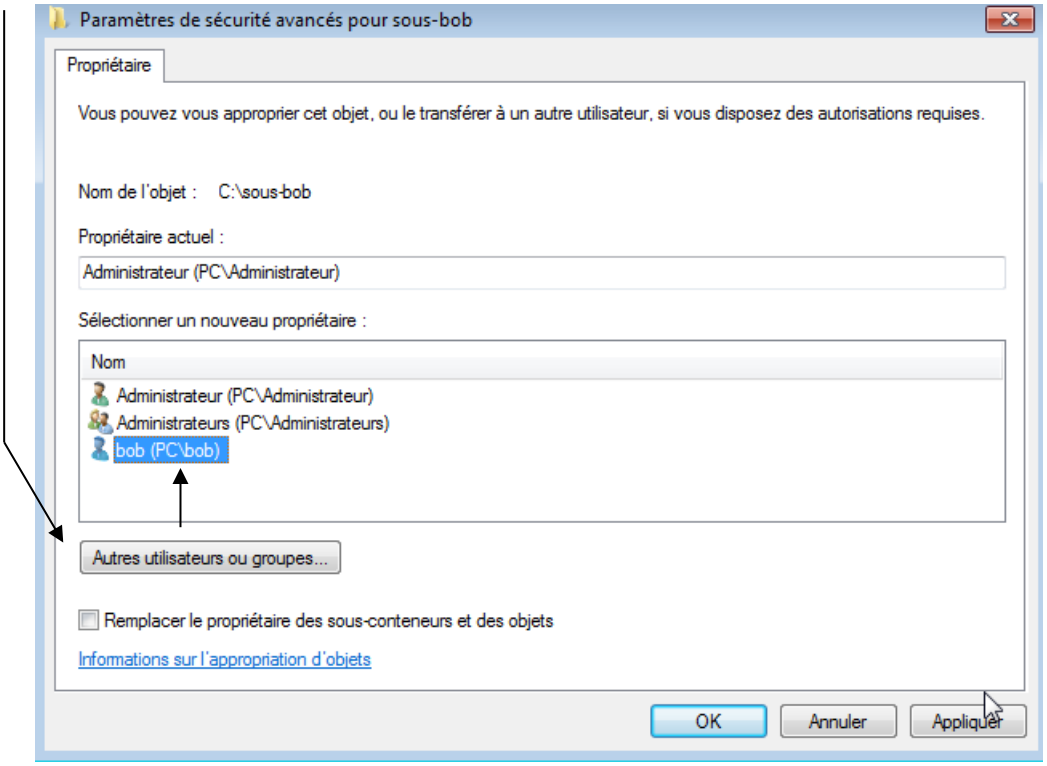
Sous **Windows Seven**, les autorisations spéciales apparaissent sous la forme



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 cas de figure existent

Pour les dossiers existants ou contenant des programmes

1. Ne pas toucher la sécurité, Ne pas casser l'héritage, ou du moins documenter
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

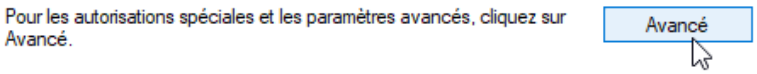
Pour les dossiers contenant des données

1. Enlever la permission par défaut "Modifier" attribuée à Utilisateurs Authentifiés, et la donner uniquement selon les besoins
2. On peut casser l'héritage
3. Pour les utilisateurs plusieurs possibilités, selon les besoins :
    - 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
    - donner des accès selon les groupes d'appatenance
4. Pour les administrateurs, ils n'ont pas forcément accès aux données

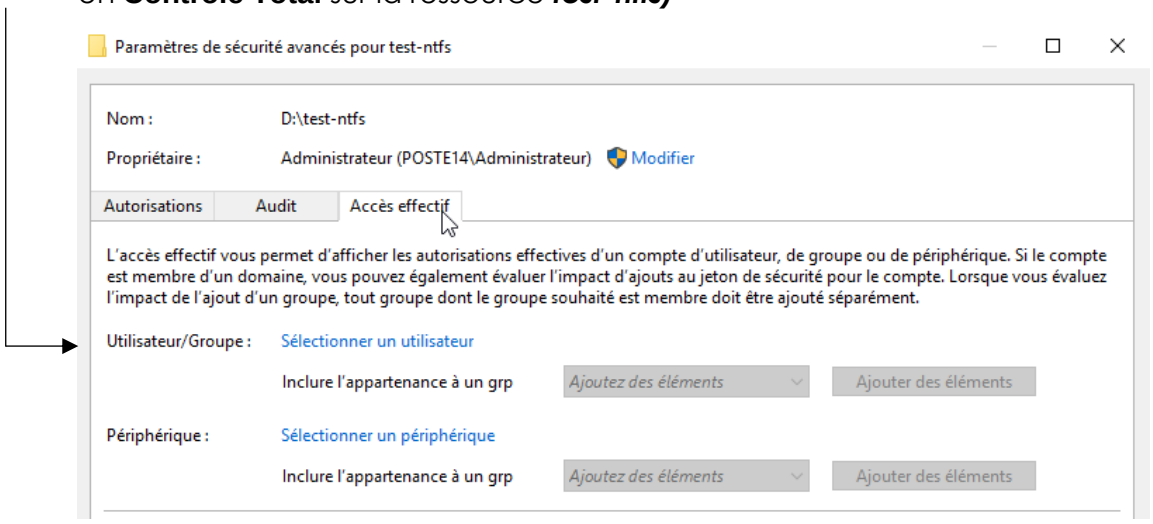
VOIR LES AUTORISATIONS EFFECTIVES

Autorisations effectives - 10 :

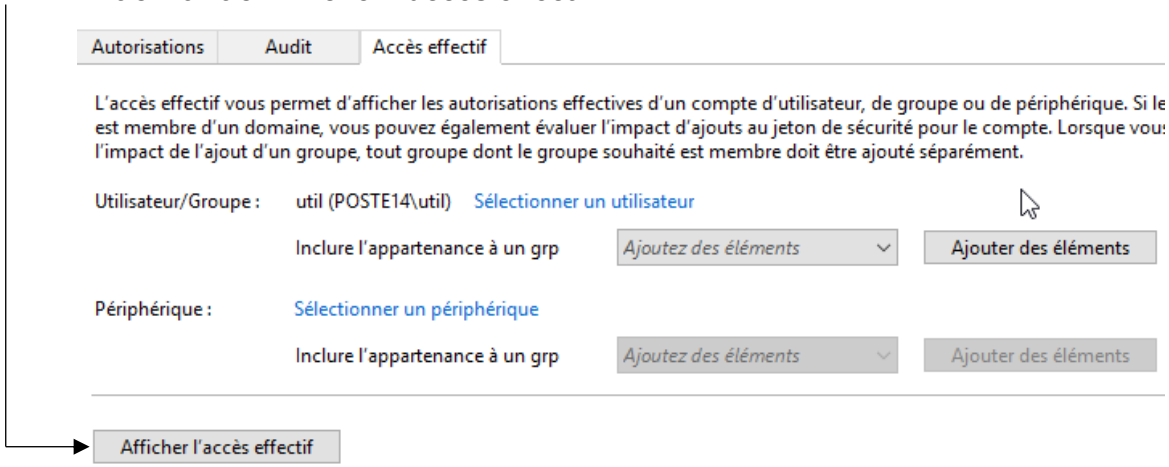
On peut connaître les autorisations qu'un utilisateur ou un groupe possède sur un objet à l'aide des **Autorisations effectives**. On demande pour un dossier **Avancé**



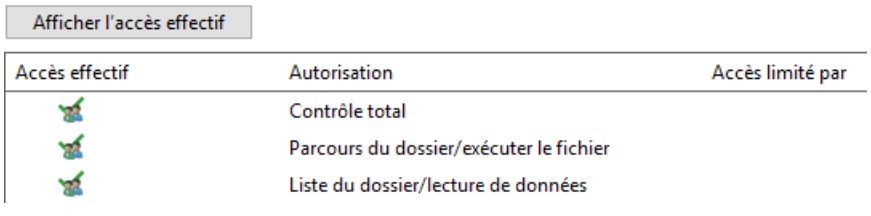
Puis dans l'onglet **Accès effectif** on peut alors ajouter un utilisateur par **Sélectionner un utilisateur (**dans l'exemple le compte ***Util*** est **Administrateur** avec des droits en **Contrôle Total** sur la ressource ***test-ntfs)***



Et demander **Afficher l'accès effectif**



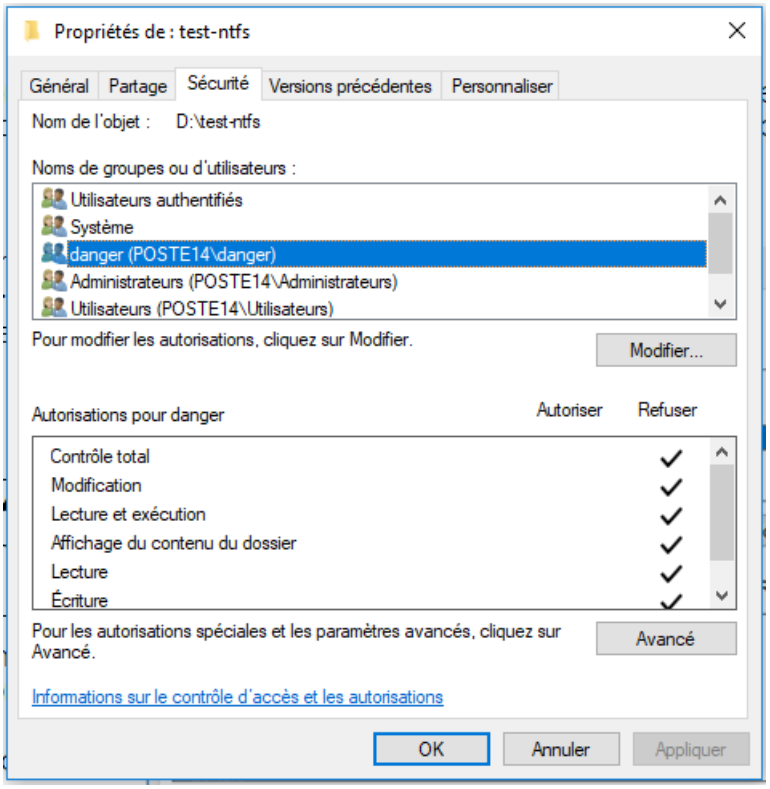
Pour obtenir le résultat



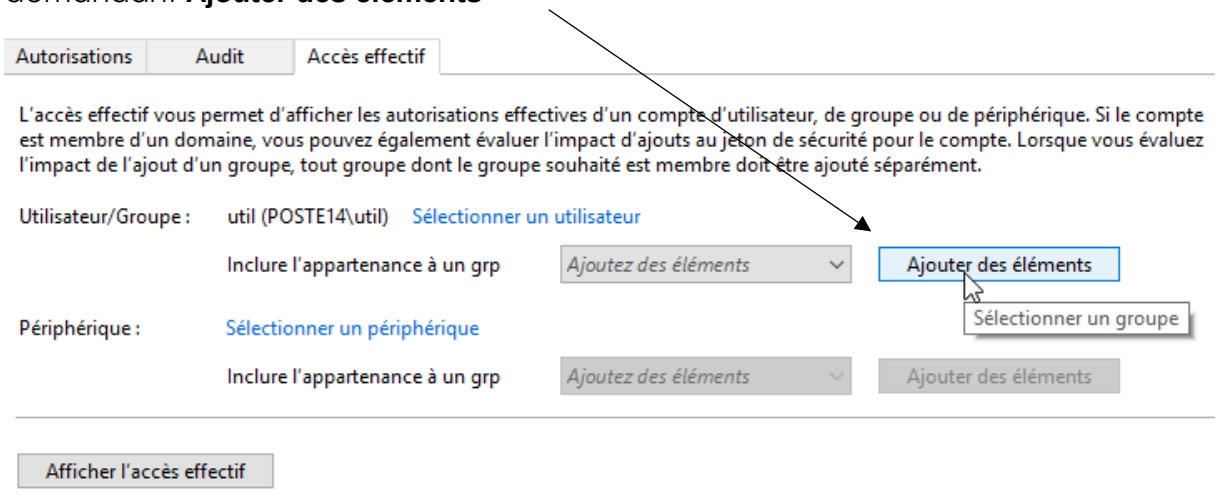
N.B : Il est désormais possible de simuler/tester « en direct » l'appartenance à un groupe, sans avoir besoin de modifier réellement l'appartenance de l'utilisateur à ce groupe

Soit par exemple un groupe ***danger*** posé en refus sur le dossier,

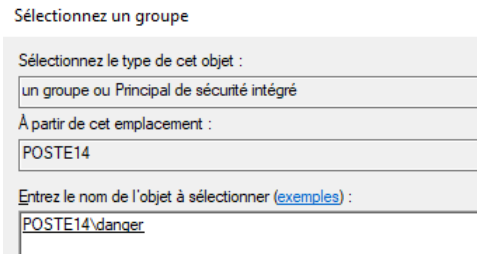
Ce groupe ***danger*** ne contient pas le compte ***util*** (pour l'instant)

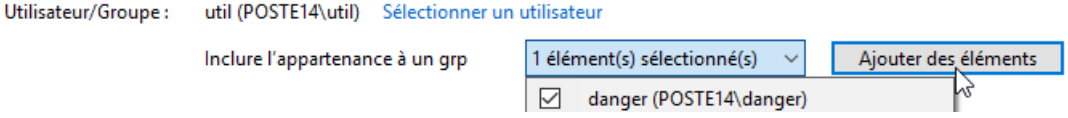


On voudrait tester les conséquences de l'appartenance du compte ***util*** dans le groupe ***danger*** : Par rapport à l'exemple précédent, une fois sélectionné le compte ***Util***, on va simuler son appartenance au groupe danger en demandant **Ajouter des éléments**

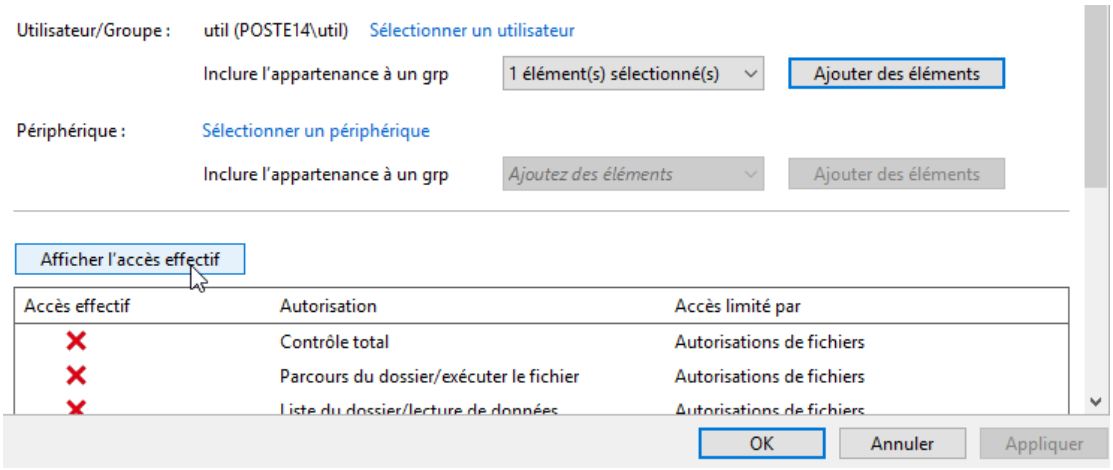


et en incluant le groupe ***danger***





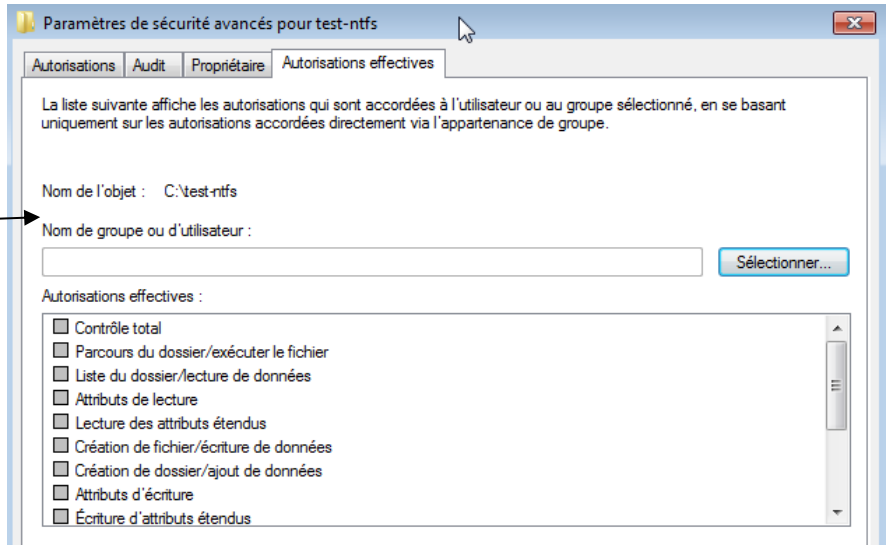
et l'on demande d'afficher les résultats toujours via **Afficher l'accès effectif**



Autorisations effectives - 7 :

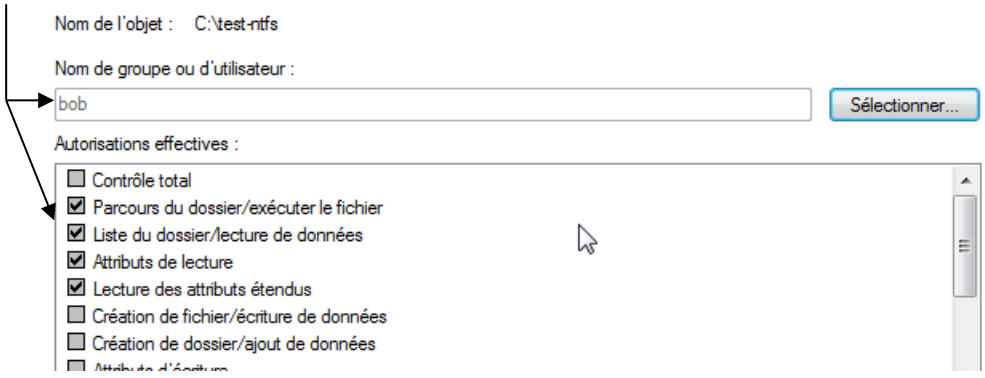
On peut connaître les autorisations qu'un utilisateur ou un groupe possède sur un objet à l'aide des **Autorisations effectives**. On demande pour un dossier

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

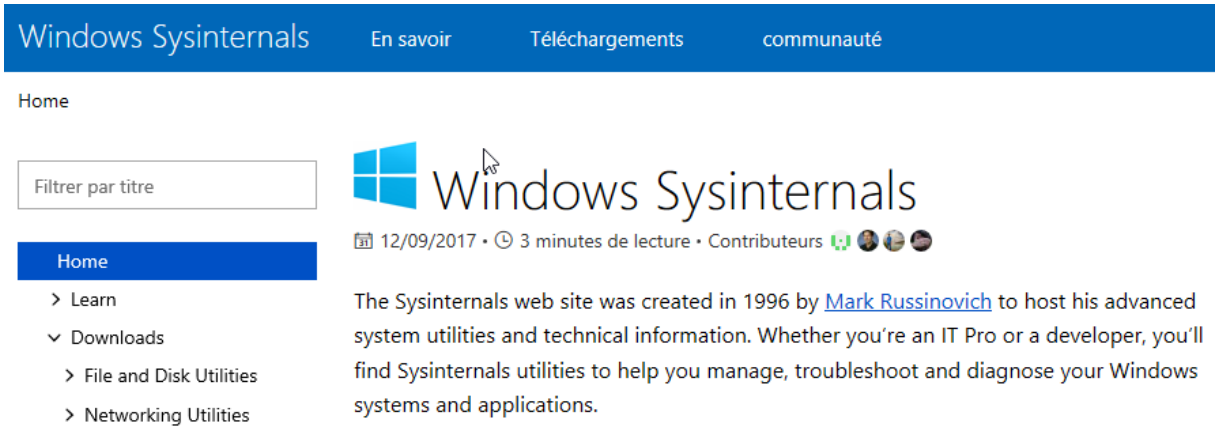


Le calcul ne tient pas compte des identificateurs de sécurité suivants :

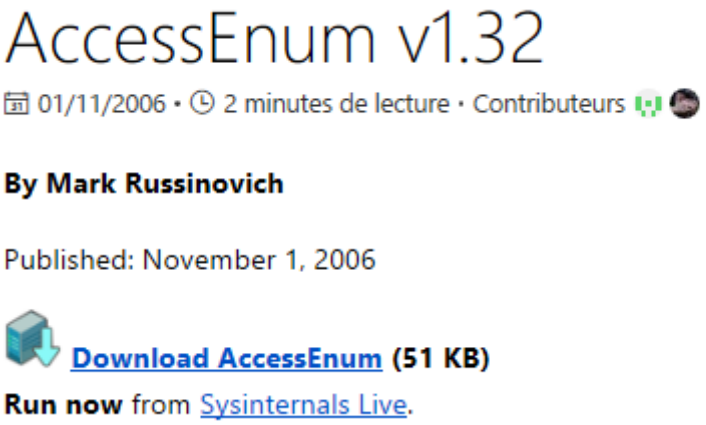
- Ouverture de session anonyme - Utilisateurs authentifiés - Créateur propriétaire.

Utilitaire AccesEnum

AccessEnum est un utilitaire en interface graphique, que l'on télécharge depuis le site **sysinternals**

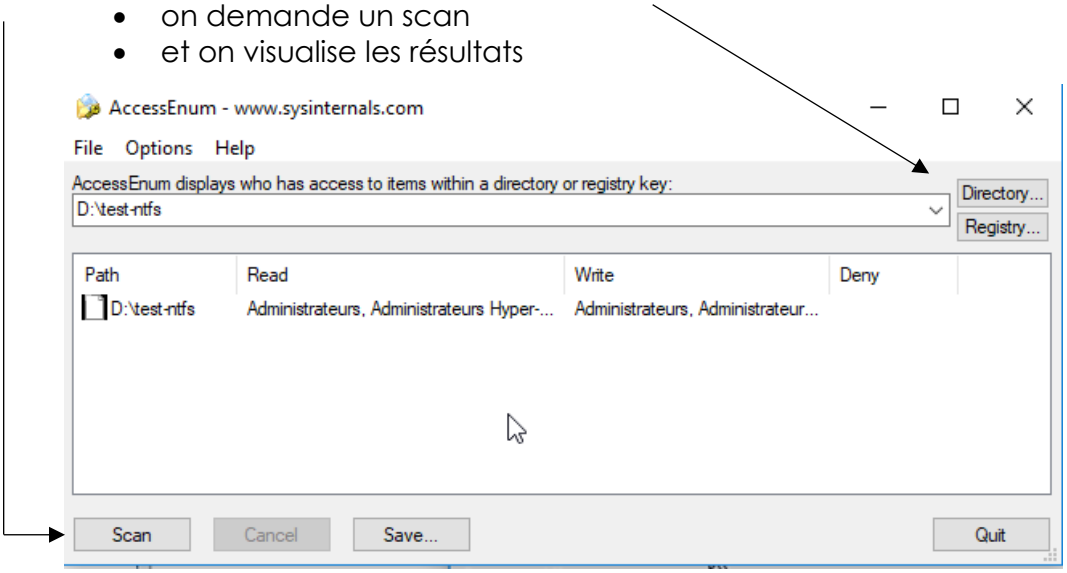


et s'exécute facilement.



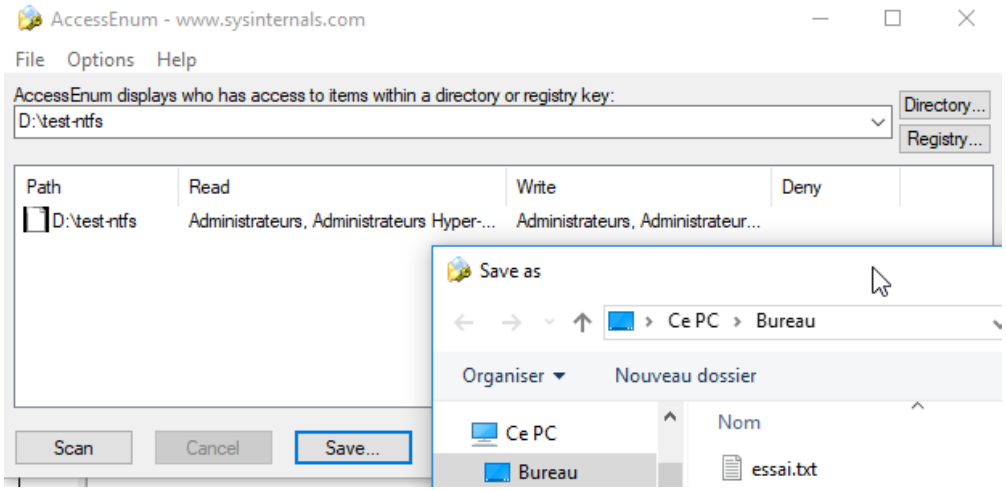
Il n'y a pas d'installation nécessaire, il est autoexecutable. L'utilisation de base est évidente,

- on indique le dossier à analyser,
- on demande un scan
- et on visualise les résultats

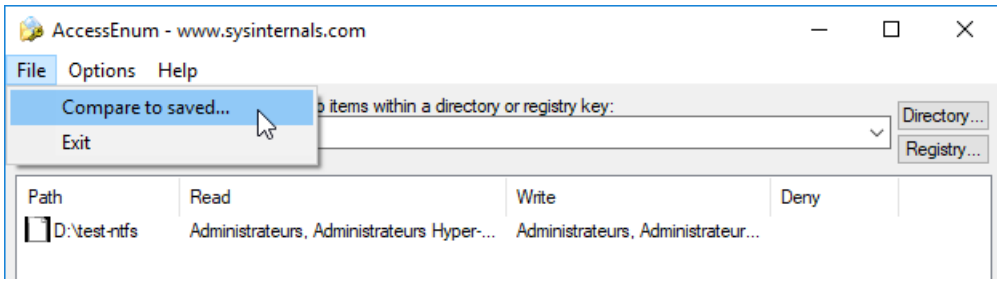


Comparaison dans le temps

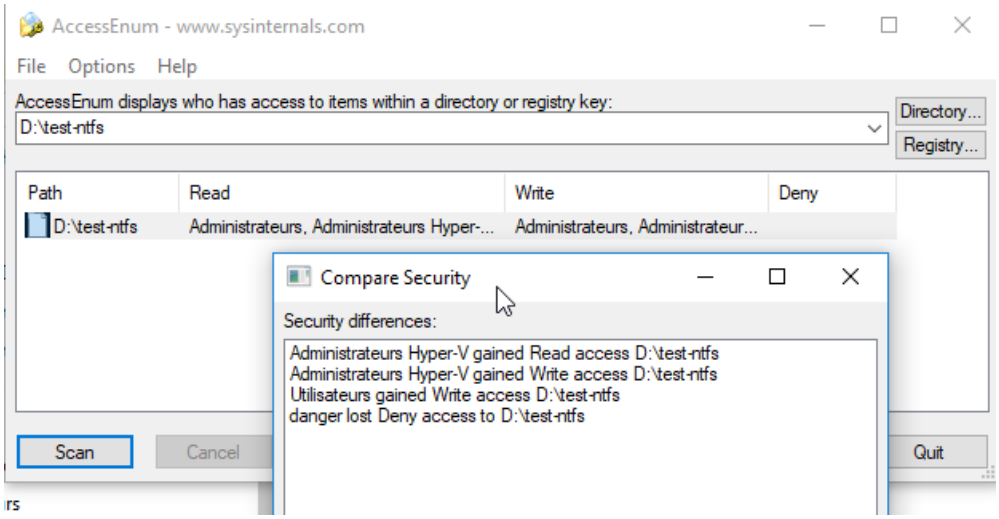
On peut mémoriser dans un fichier la situation des droits d'un dossier (ou d'une arborescence) en demandant **Save** (ou stocke un fichier texte)



Lorsque l'on reviendra effectuer un scan plus tard, une fois la situation présente analysée, il faut demander **File / Compare to saved** et indiquer le chemin du fichier texte généré lors de la situation d'origine



Et l'on obtient le différentiel



Utilitaire Accesschk

Accesschk est un utilitaire en ligne de commande, que l'on télécharge depuis le site **sysinternals**

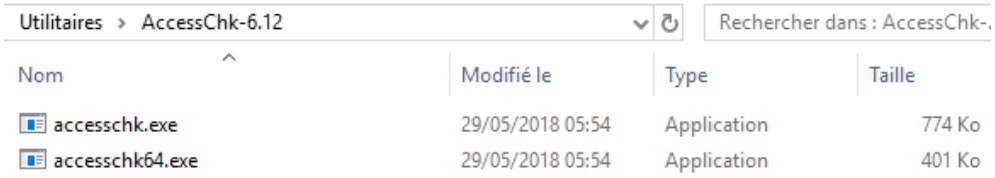
AccessChk v6.12

17/02/2017 • 2 minutes de lecture • Contributeurs

By Mark Russinovich

Published: November 19, 2017

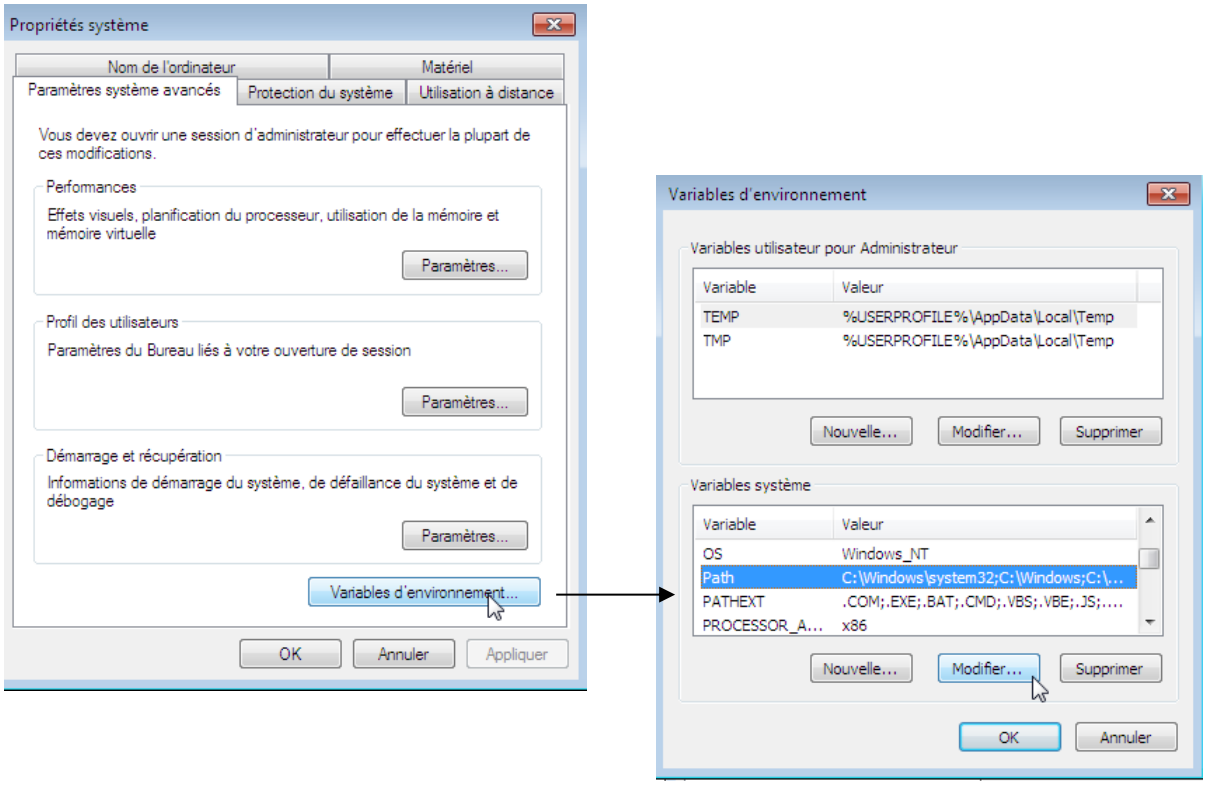
L'utilitaire téléchargé est petit



On peut renommer le fichier, et le copier dans **Windows\system32**, pour plus de rapidité.

```
C:\Windows\system32>tst-ntfs

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com
```

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:\Windows\system32>tst-ntfs util d:\*.*

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW d:\$RECYCLE.BIN
RW d:\System Volume Information
RW d:\test-ntfs
```

Les options pour les dossiers/fichiers intéressantes (et cumulables) :

- n

pas d'accès

- r

accès en lecture

-w

accès en ecriture

-d

uniquement les dossiers

Donc quel accès a le compte ***Util*** sur le dossier ***d:\test-ntfs***

```
C:\Windows\system32>tst-ntfs util d:\test-ntfs\ -d

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW d:\test-ntfs
```

Donc quel accès le groupe des ***administrateurs*** sur le dossier ***windows***

```
C:\Windows\system32>tst-ntfs administrateurs c:\windows\ -d

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW c:\Windows
```

Quel accès a 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
```

Quel accès a le groupe des « ***système*** » sur l'arborescence à partir du dossier ***windows***

```
C:\Windows\system32>tst-ntfs "système" c:\windows\

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW c:\windows\addins
RW c:\windows\appcompat
RW c:\windows\apppatch
RW c:\windows\AppReadiness
RW c:\windows\assembly
RW c:\windows\AutoKMS
RW c:\windows\bcastdvr
R  c:\windows\bfsvc.exe
RW c:\windows\BitLockerDiscoveryVolumeContents
R  c:\windows\Boot
RW c:\windows\bootstat.dat
```

Variante pour les Autorisations de Service

On peut demander la situation de qui a les droits pour utiliser un service, en ajoutant l'option **–c** suivit au choix de

- **scmanager :** pour le gestionnaire de services
- ***** **:** pour tous les services
- **Nomsvc** **;** pour le service nommé nomsvc

Par exemple qui a accès au gestionnaire de service **scmanager**

```
C:\Windows\system32>tst-ntfs -c scmanager

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

ScManager
     AUTORITE NT\Utilisateurs authentifiÚs
  R  AUTORITE NT\INTERACTIF
  R  AUTORITE NT\SERVICE
  RW AUTORITE NT\SystÞme
  RW BUILTIN\Administrateurs
     AUTORITÉ DE PACKAGE D?APPLICATION\TOUS LES PACKAGES D?APPLICATION
```

Qui a accès au service **netlogon**

```
C:\Windows\system32>tst-ntfs -c netlogon

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

netlogon
  RW AUTORITE NT\SystÞme
  RW BUILTIN\Administrateurs
  R  AUTORITE NT\INTERACTIF
  R  AUTORITE NT\SERVICE
```

Liste de tous ceux qui ont un accès en modification pour tous les services

```
C:\Windows\system32>tst-ntfs -cw *
```

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 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]] [/V] [/W]
                           [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]
                           [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z] [/B] [/J]
                           [/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: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.
/V          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

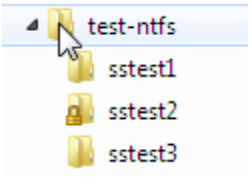
Genre **xcopy c:*.* d:*.* /s/e/c/o > info.txt**

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

N.B: Depuis 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,



Avec:

- héritage cassé pour ***sstest1*** et ***sstest2***
- la sécurité suivante

```
C:\Windows\system32>tst-ntfs d:\test-ntfs

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

d:\test-ntfs\sstest1
  RW AUTORITE NT\SystPme
  RW BUILTIN\Administrateurs
  RW POSTE14\Administrateur
d:\test-ntfs\sstest2
  RW POSTE14\util
  RW BUILTIN\Utilisateurs
  RW BUILTIN\Administrateurs
  RW AUTORITE NT\SystPme
  RW AUTORITE NT\Utilisateurs authentifiÚs
  RW POSTE14\Administrateur
d:\test-ntfs\sstest3
  RW POSTE14\util
```

N.B : On peut poser des fichier/dossier dans le dossier réservé à ***util***, avec **Runas**

```
C:\Windows\system32>runas /user:util "c:\windows\system32\cmd.exe"
Entrez le mot de passe de util :
Tentative de lancement de c:\windows\system32\cmd.exe en tant qu'utilisateur "POSTE14\util" ...

C:\Windows\system32>
```

```
c:\windows\system32\cmd.exe (en tant qu'utilisateur POSTE14\util)
Microsoft Windows [version 10.0.17134.1]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>
```

On voudrait sauvegarder tout cela sous ***D:\backup***, réservé à l'administrateur…

```
C:\Windows\system32>tst-ntfs c:\backup -d

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\backup
  RW AUTORITE NT\SystPme
  RW BUILTIN\Administrateurs
  RW POSTE14\Administrateur
```

Il faut faire un **xcopy…/0 /S** ou mieux ***/S/E/C/O*** voire

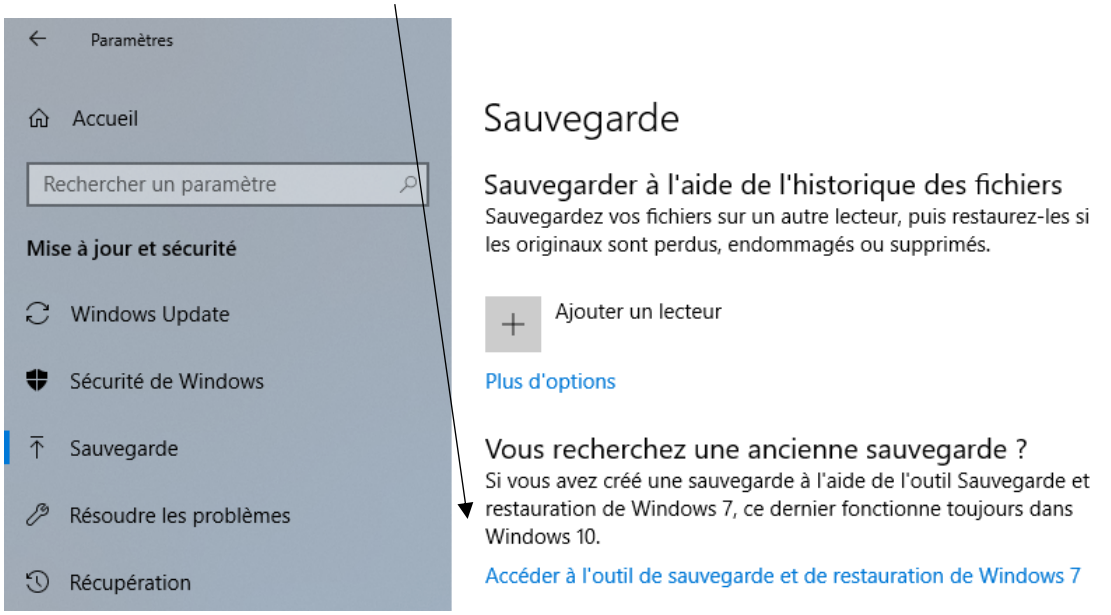
```
C:\Windows\system32>xcopy d:\test-ntfs\*.* c:\backup\*.* /s/e/c/o
D:\test-ntfs\sstest1\Nouveau document texte.txt
D:\test-ntfs\sstest2\Nouveau document texte.txt
2 fichier(s) copié(s)
```

Pour obtenir le respect des droits

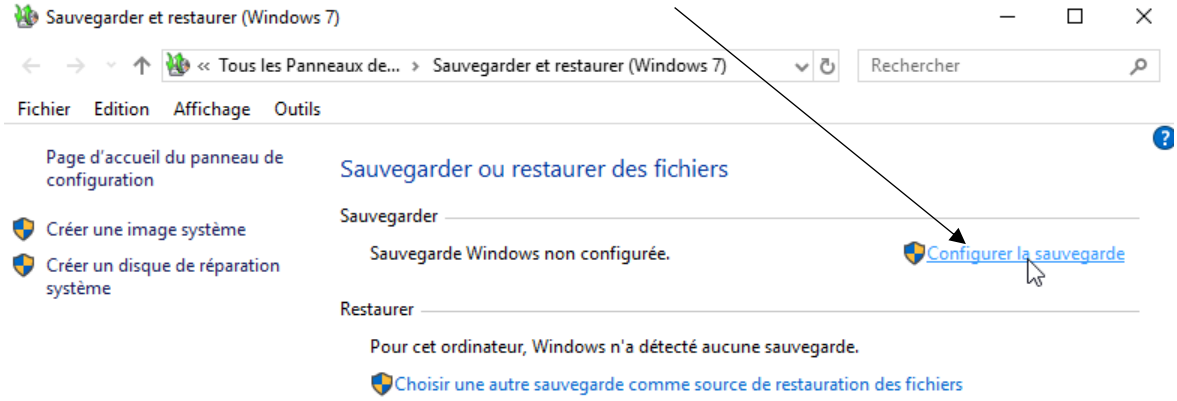
```
C:\Windows\system32>tst-ntfs c:\backup

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\backup\sstest1
  RW AUTORITE NT\SystPme
  RW BUILTIN\Administrateurs
  RW POSTE14\Administrateur
c:\backup\sstest2
  RW POSTE14\util
  RW POSTE14\Administrateur
  RW AUTORITE NT\SystPme
  RW BUILTIN\Administrateurs
c:\backup\sstest3
  RW POSTE14\util
```

Sauvegarde de Fichiers

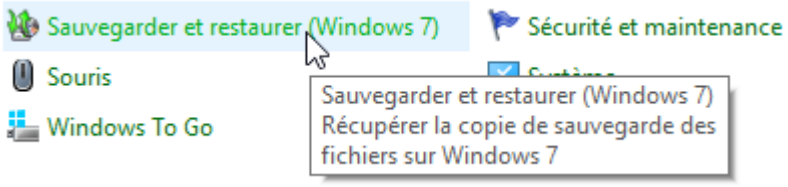
On peut y accéder via **paramètres Windows 10 / Mise à Jour et Sécurité** puis **Sauvegarde**, et on demande **d'Accéder à l'outils de sauvegarde et de restauration de Windows 7**



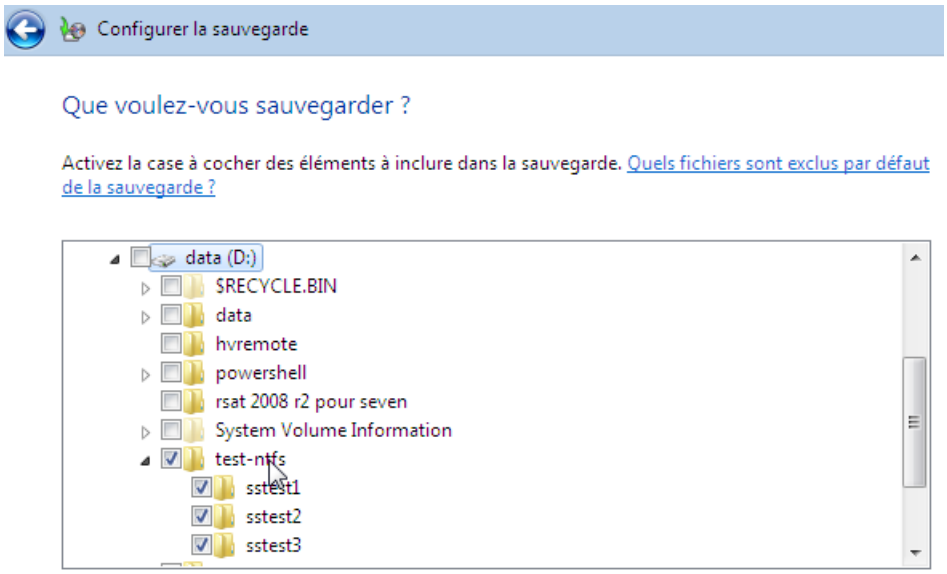
Et la on demande de **configurer la sauvegarde**



N.B : Pour l'instant on peut toujours aussi y accéder via l'ancien **Panneau de Configuration / Sauvegarder et restaurer (Windows 7)**

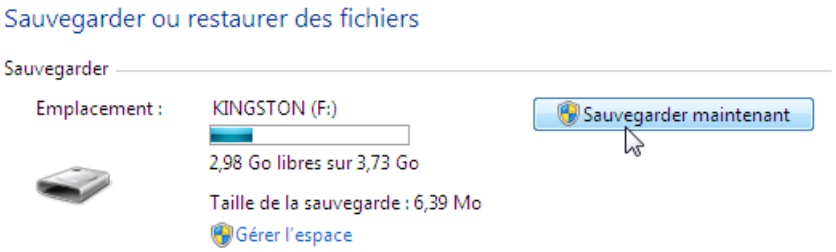


On choisit un emplacement de sauvegarde, et on demande de choisir….

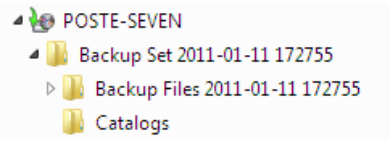


On enregistre les pramètres, et l'on quitte.

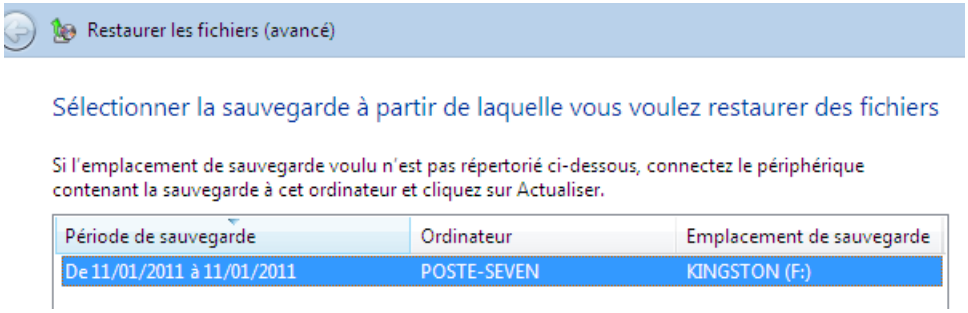
Il ne reste plus qu'à executer la sauvegarde



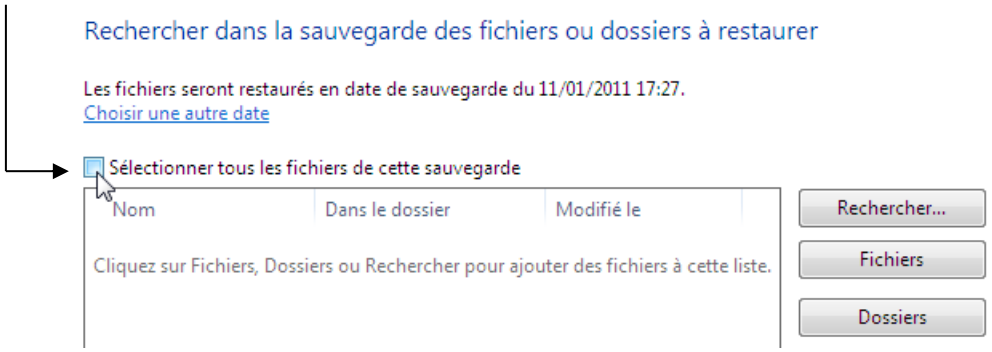
Sur la cible de destination, une structure est crée



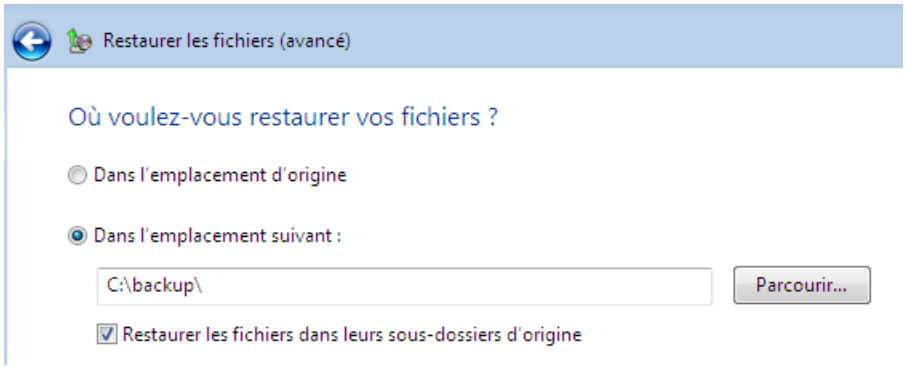
Effectuons la restauration, que nous allons faire dans le dossier ***C:\backup*** (et non pas le dossier d'origine… pour mieux comparer)



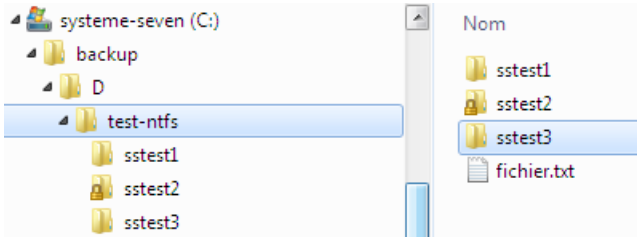
On sélectionne tous les fichiers de la sauvegarde



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



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



N.B : pour que la sauvegarde se fasse via cette méthode, le groupe **système** doit avoir un accès aux ressources

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 simpe :: 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**, (equivallent 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 vérrouillé **/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

------------------------------------------------------------------------------

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

------------------------------------------------------------------------------

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

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

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

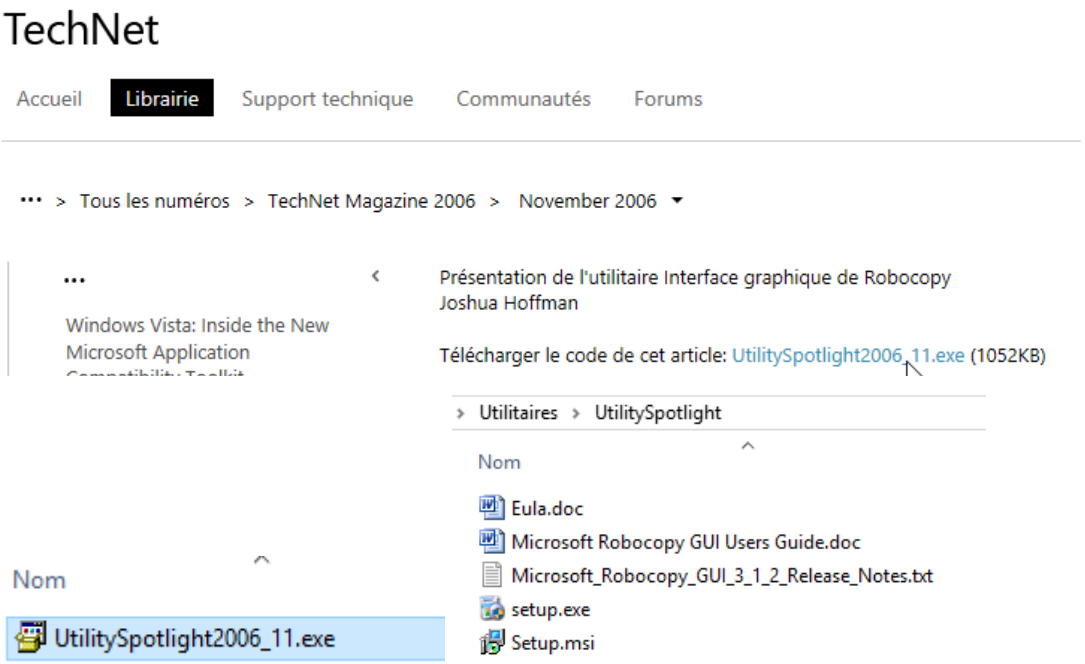
  robocopy C:\test-ntfs \\serveur\backup /MIR /Z

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

Ajout d'interface graphique

On peut ajouter une interface graphique à ROBOCOPY

Soit l'interface Microsoft, soit une interface d'un autre projet



Mais necessite le framework 2.0 de microsoft

LIENS SYMBOLIQUES

Liens Symboliques - Raccourcis:

Différence entre liens symboliques et raccourcis:

- Un **Raccourci** est une redirection au niveau du s**ystème d'exploitation, Windows**. 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 symboliques 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    <JONCTION>     Application Data [C:\Users\admin\AppData\Roaming]
10/12/2010  12:09    <JONCTION>     Cookies [C:\Users\admin\AppData\Roaming\Microsoft\Windows\Cookies]
10/12/2010  12:09    <JONCTION>     Local Settings [C:\Users\admin\AppData\Local]
```

Le lien garde les propriétés du dossier-fichier vers lequel il pointe, ce n'est pas un fichier avec ses propres propriétés 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 pourrons savoir combien pèse le dossier cible, géré 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 (avec son chemin absolu).

"lien" = Si le chemin du lien donné est **relatif** (\un-dossier\un-sous-dossier\cible) le **lien symbolique** est dit **relatif**.

Il est placé là où l'on se trouve au moment où l'on tape la commande

"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

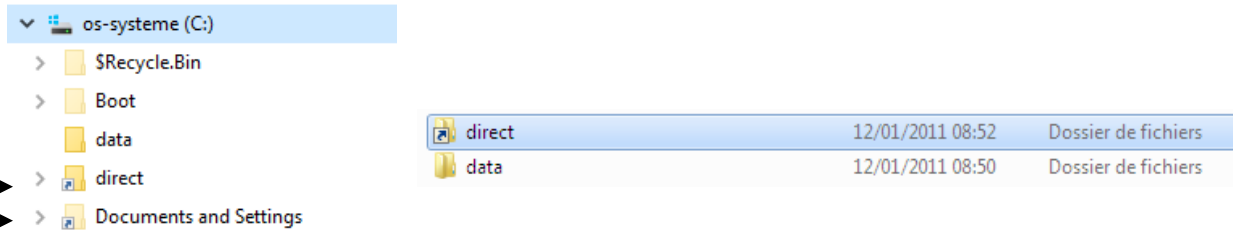
mklink /D c:\direct c:\data

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

Donnant

```
C:\>dir /al
 Le volume dans le lecteur C s'appelle os-systeme
 Le numéro de série du volume est FE8F-8891

 Répertoire de C:\

28/06/2018  14:27    <SYMLINKD>     direct [c:\data]
16/03/2017  21:58    <JUNCTION>     Documents and Settings [C:\Users]
               0 fichier(s)                0 octets
               2 Rép(s)  36 657 520 640 octets libres
```

Dans l'explorateur cela apparaît ainsi



N.B : Ne pas confondre un **Lien symbolique** avec une **jonction**, graphiquement on ne voit pas la différence, mais en invite de commande c'est plus explicite.

On peut effacer le lien symbolique par la commande classique **RD** comme dans **RD direct**…

```
C:\>dir /al
 Le volume dans le lecteur C s'appelle os-systeme
 Le numéro de série du volume est FE8F-8891

 Répertoire de C:\

28/06/2018  14:27    <SYMLINKD>     direct [c:\data]
16/03/2017  21:58    <JUNCTION>     Documents and Settings [C:\Users]
               0 fichier(s)                0 octets
               2 Rép(s)  36 657 520 640 octets libres

C:\>rd direct
```

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

mklink /D c:\direct d:\data

"lien" = relatif

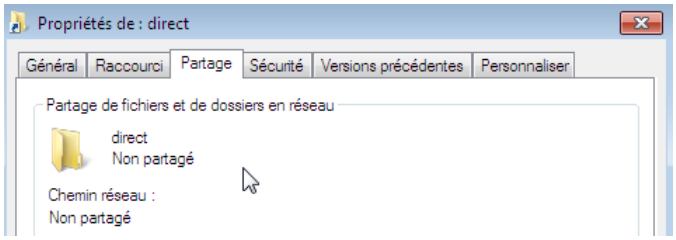
On se place sur le bureau du compte administrateur, on crée le lien symbolique suivant :

mklink /D direct c:\data

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

On obtient alors sur le bureau

et les propriétés sont biens celles d'un dossier…



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

Copie de Liens Symboliques:

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

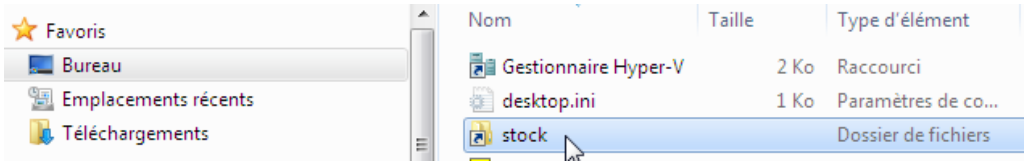
1. Soit un lien symbolique "***stock***" pointant sur un dossier **C:\stock** (contenant des fichiers et des dossiers) et posé sur le bureau de l'administrateur…

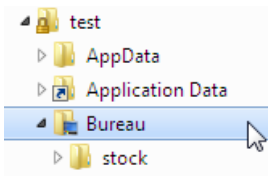
```
C:\Users\Administrateur\Desktop>mklink /D stock c:\stock
Lien symbolique créé pour stock <<===>> c:\stock
```

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 …





mais en fait on a copié le dossier !

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'admnistrateur.

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…

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

 Répertoire de C:\Users\test\Desktop

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

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 emplois" 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    <JONCTION>     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 apparait comme un raccourcis 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** c'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.

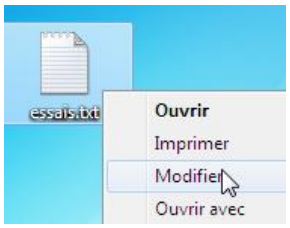
  Il apparait comme le fichier d'origine, (duplicata) Ce n'est que lorsqu' on supprime tous les liens réels que le fichier est supprimé.

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°

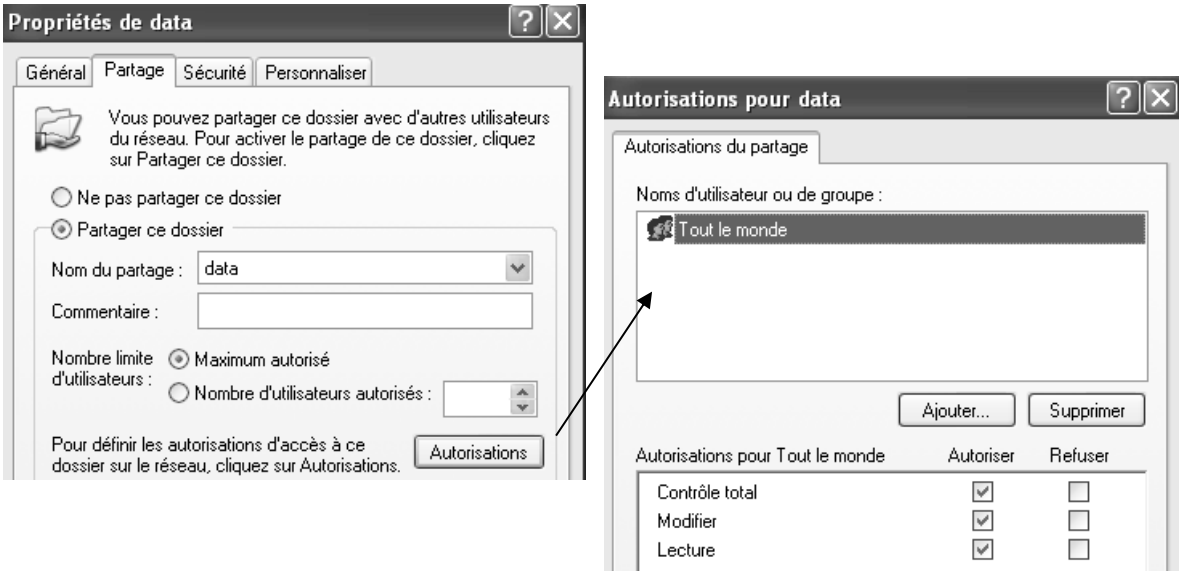
Objectif :

Faire que chaque utilisateur , andre, bertrand…puisse "tout faire chez lui", sauf détruire son 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 !)

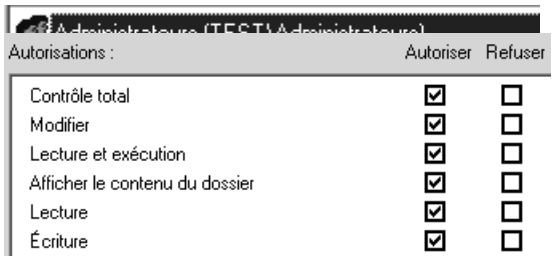
Permissions de sécurité :

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

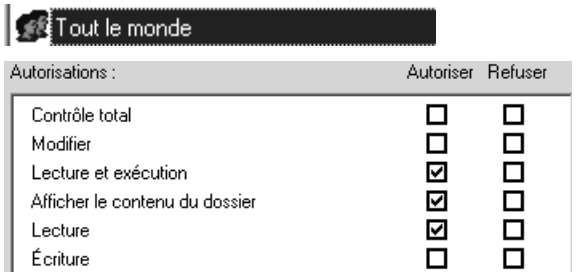
Ensuite on pose

- 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**

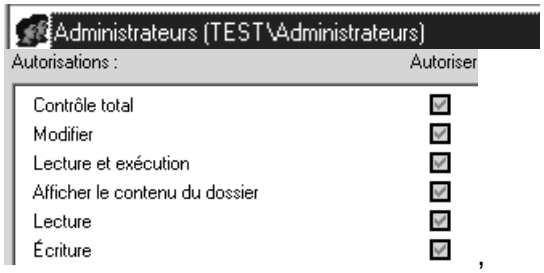
on a donc



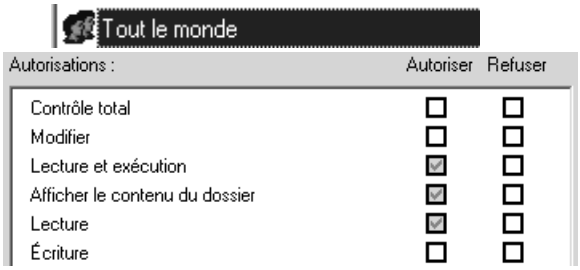
et



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



,

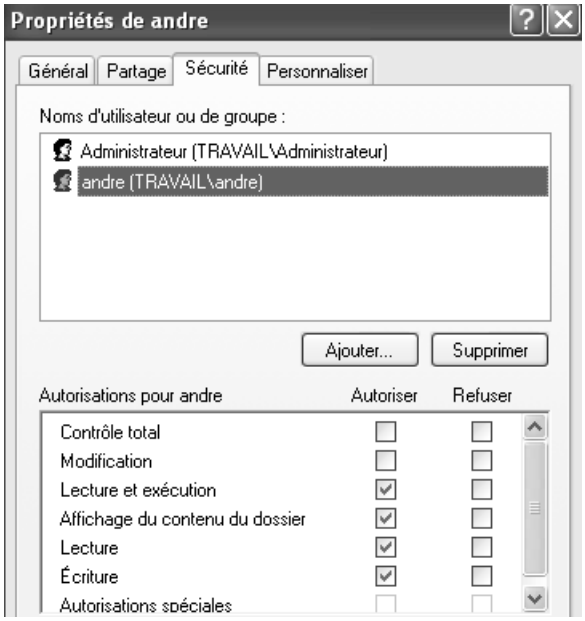


à l'heure actuelle les dossiers **andre** et **bertrand** sont en lecture seule pour tout le monde... Il faut maintenant autoriser andré a pouvoir aller que chez lui, et exclure tout le monde (et idem pour bertrand...)

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

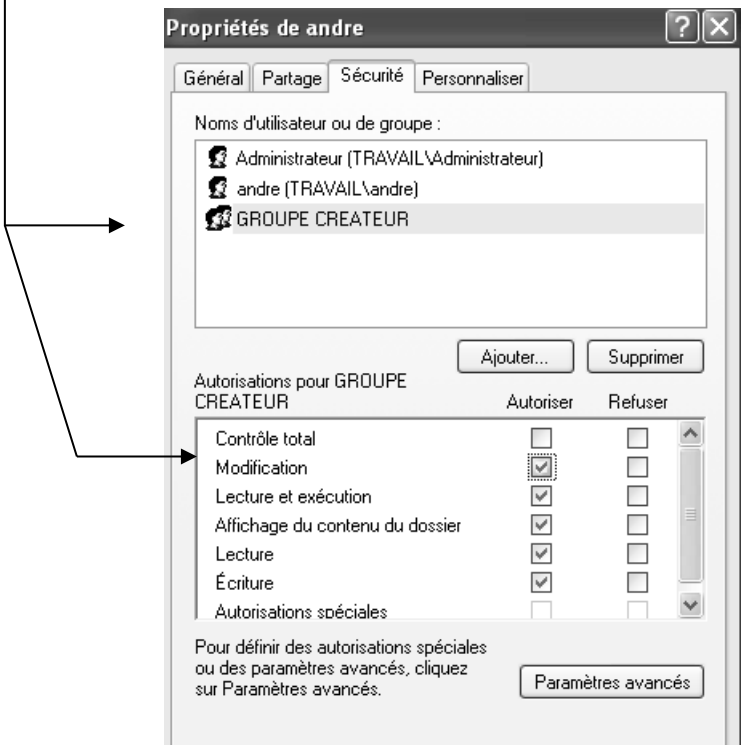
---

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 :

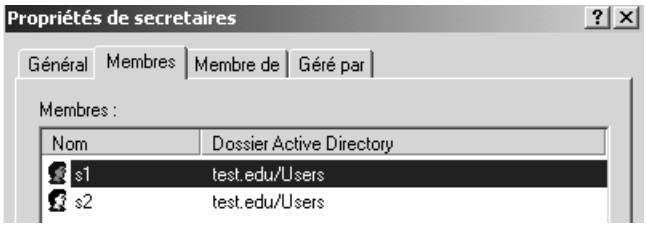
- son dossier, (de manière complète)
- aux dossiers des collègues (en lecture seule)
- au dossier commun des commerciaux (de manière complète)
- mais n'a pas accès aux dossier des secrétaires....

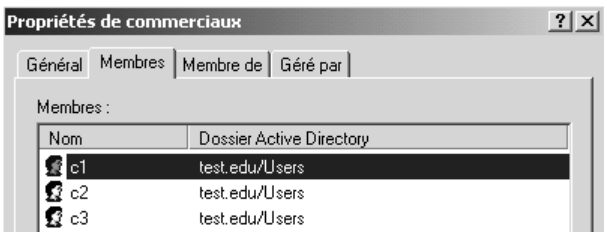
De manière analogue, les **secrétaires** peuvent avoir accès a :

- 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 :

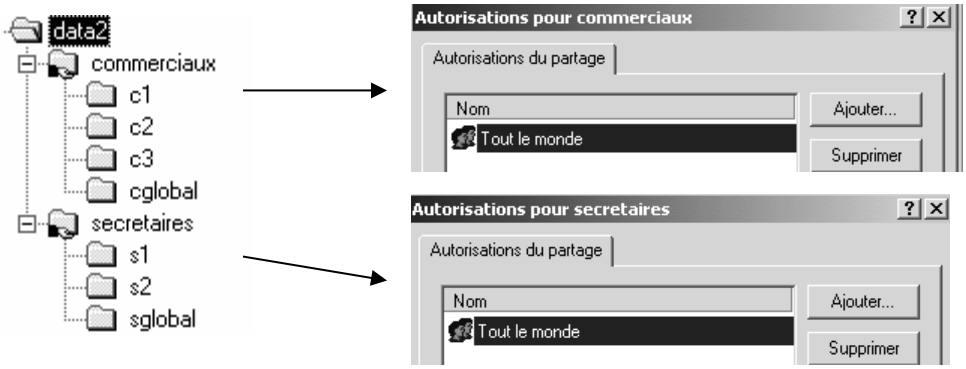
il faut créer un groupe global des secrétaires et y rentrer les utilisateurs appropriés (s1,s2...)., et un groupe global des commerciaux, et y rentrer les utilisateurs appropriés (c1, c2...).





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**,

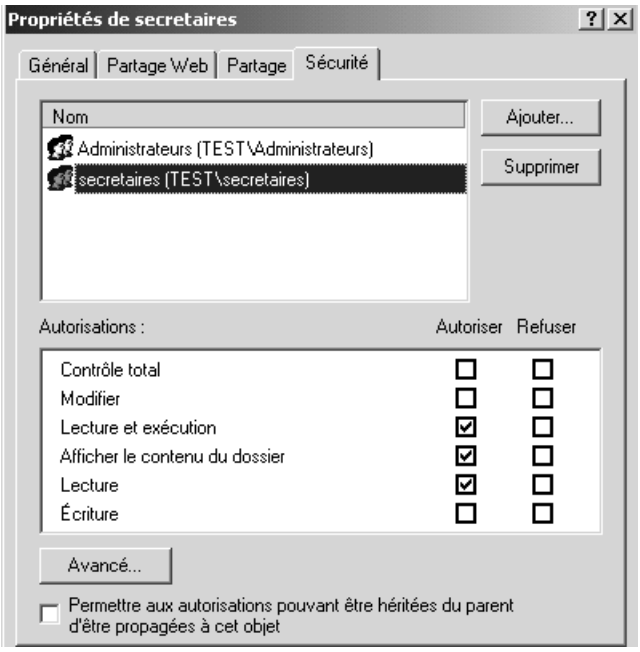


N.B: on pourrait décider de ne faire qu'un seul partage

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 !

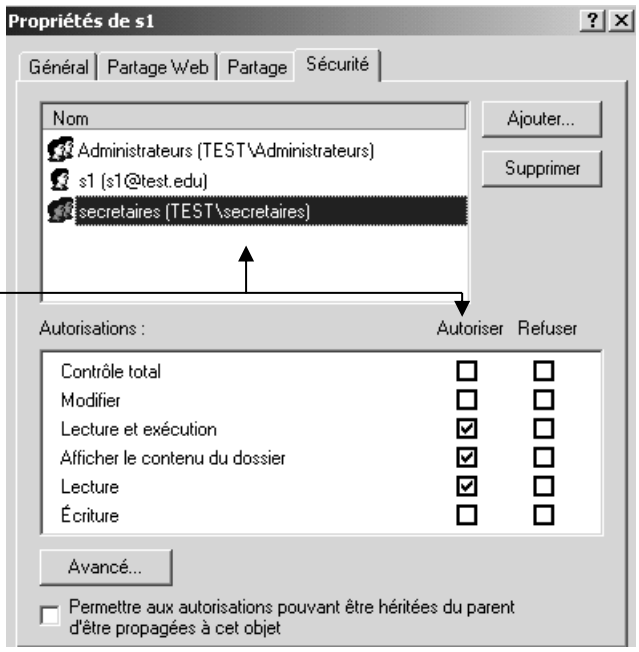
Pur chaque dossier individuel, **S1 S2** etc il faut autoriser l'utilisateur **S1** à **créer** chez lui, (mais pas **modifier**, sinon il pourrait supprimer son propre dossier) et les **administrateurs** en **contrôle total**

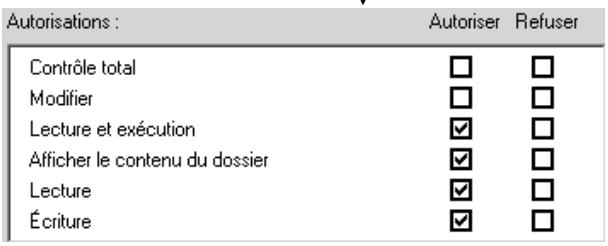
Donc on **supprime l'héritage**, (en supprimant les droits)

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**





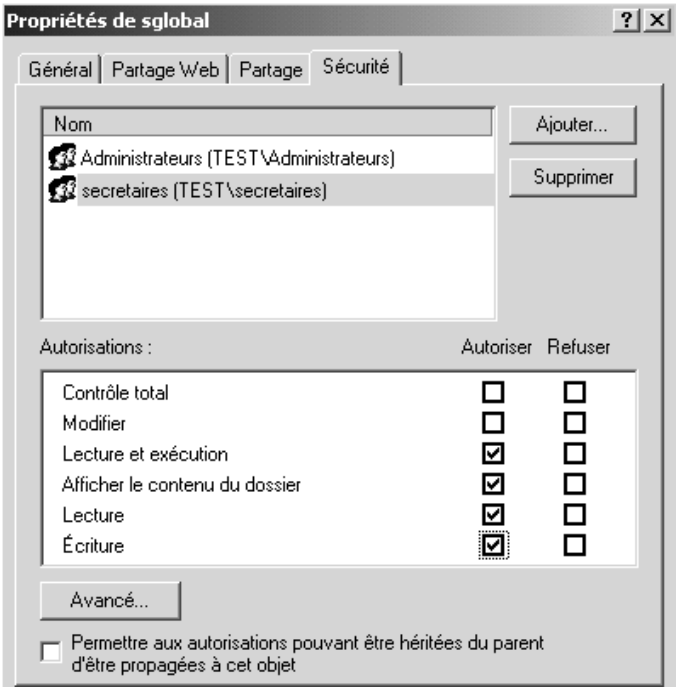
Pour le dossier **sglobal** il faut autoriser chaque secrétaire à pouvoir y écrire, ainsi que l'administrateur

on supprime l'héritage

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

et le groupe **secretaires**

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



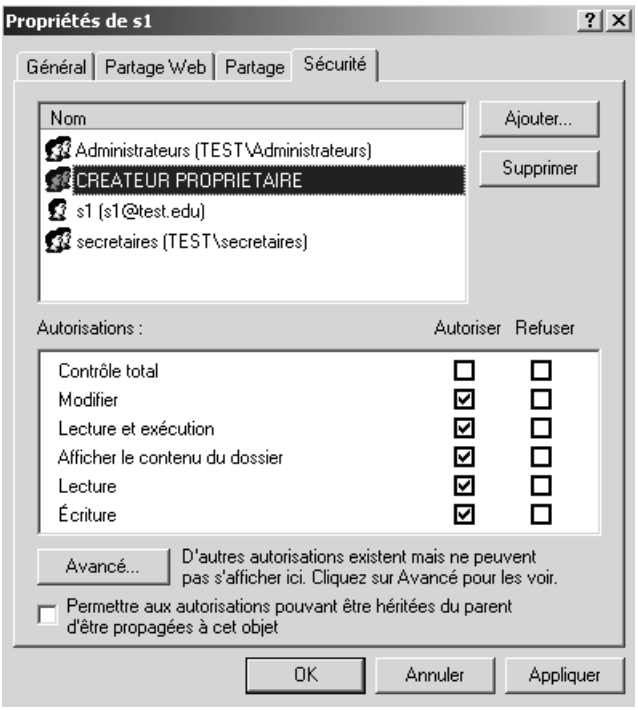
Créateur propriétaire :

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 **sglobal**, 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 :

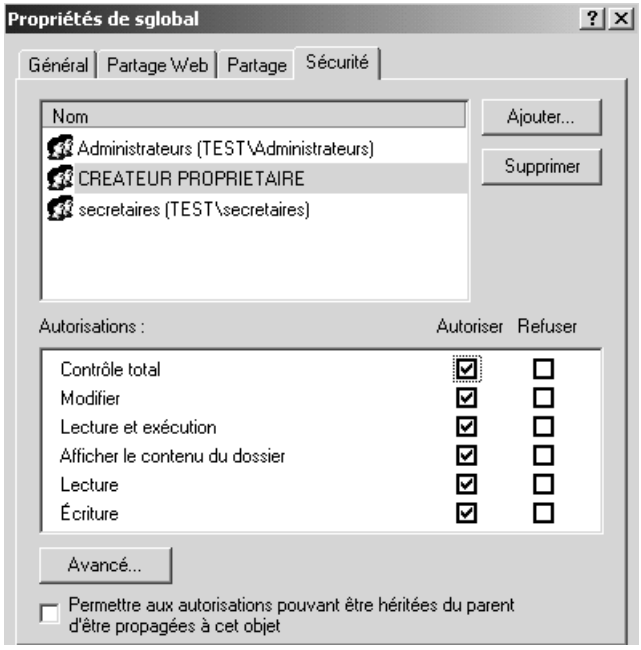
Imaginons un ensemble de secrétaires ayant chacune un espace propre réservé nommé **s1**, **s2** etc et disposant d'un espace commun à toutes nommé **sglobal** (pour secrétaire global)

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

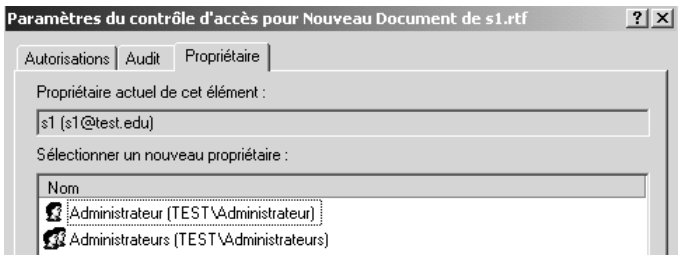
Administrateur en **Contrôle total**

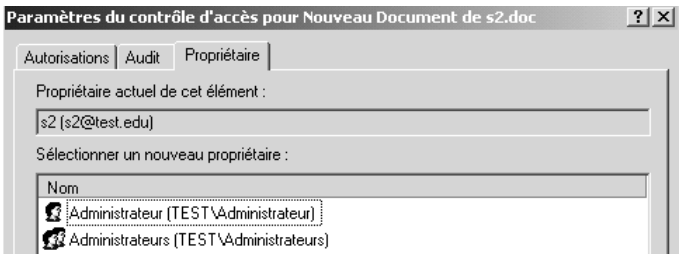
Créateur propriétaire en **contrôle total**

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



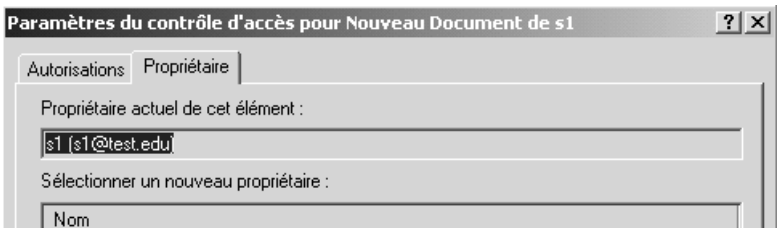
on peut donc arriver à ce que dans ce dossier, il y ait des documents de divers propriétaires...





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 sûr pas changer les permissions!



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

Raisonnement :

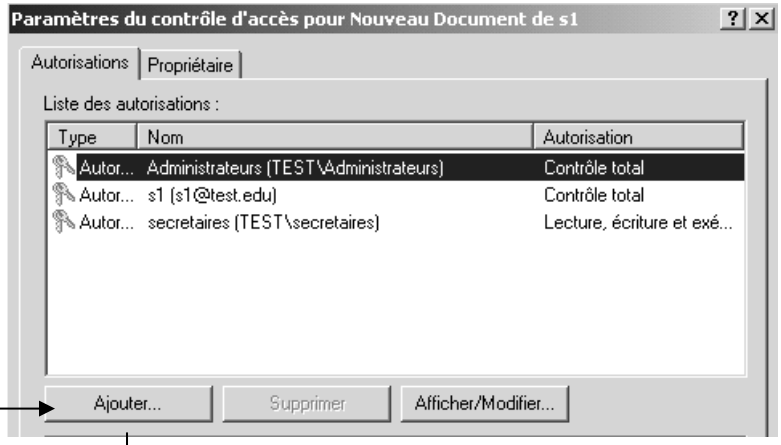
Pour que **s2** puisse s'approprier le document...(depuis un poste NT...) **s1** doit donner à **s2** la permission voulue, voire la permission de prendre possession de ce fichier...:

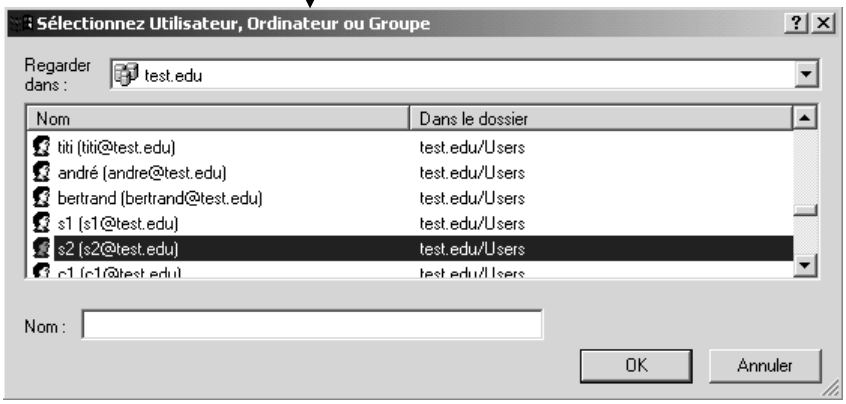
N.B: il ne peut le faire que s'il a un contrôle total sur ce fichier (la différence entre contrôle total et modifier c'est que modifier ne permet pas de changer les permissions, et donc d'ajouter ou d'enlever des droits à des utilisateurs...)

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

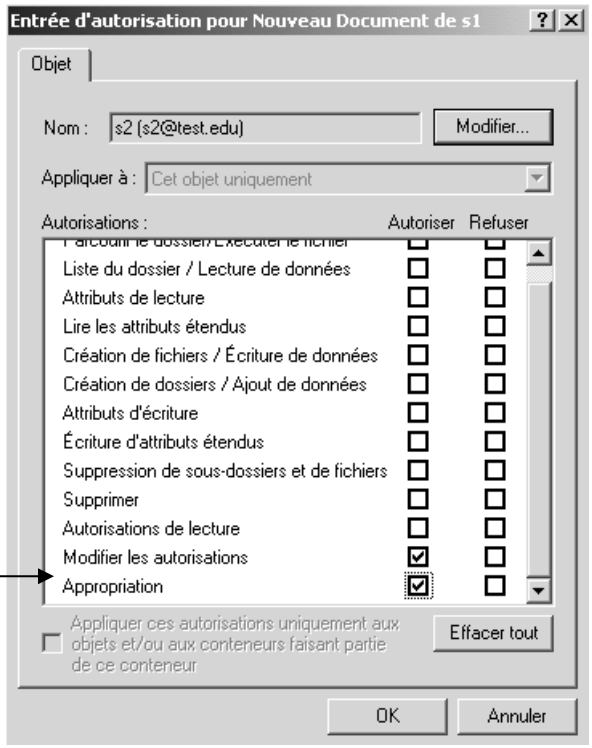
dans **permissions - securité - avancées** -

on demande **Ajouter**



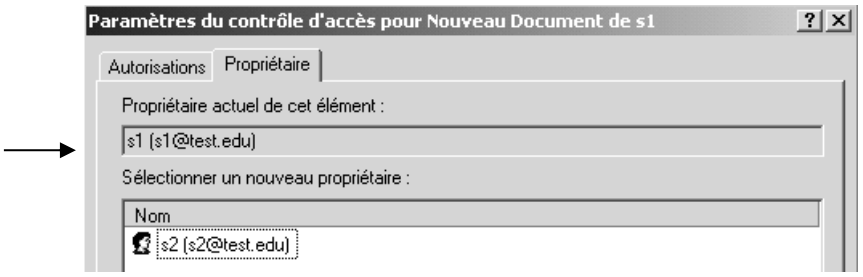


sélectionner **s2** puis valider

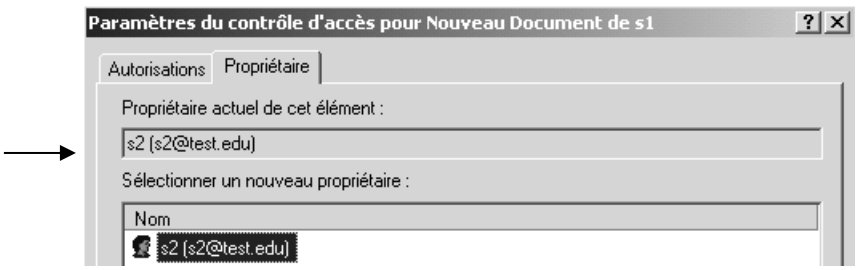


NB: il faut ici cocher au minimum **modifier** et **appropriation**, mais aussi toutes les autres permissions que l'on souhaite donner à S2

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…