

# Les permissions NTFS

À chaque ouverture de session, les informations d'identification employées par l'utilisateur (nom d'utilisateur et mot de passe) sont transmises à un moniteur de sécurité locale qui accède au Gestionnaire de sécurité (SAM pour *Security Account Manager*). Ce dernier accorde un jeton d'accès (token) qui va déterminer les droits d'accès que possède cet utilisateur pour tout objet "sécurisable" (clé du Registre, fichier, dossier, service, processus, etc.). Ce descripteur de sécurité vérifie deux informations :

- Le SID de l'utilisateur.
- La liste DACL de l'objet auquel tente d'accéder l'utilisateur.

Ces deux notions vont être expliquées dans la suite de ce chapitre.

## 1. Les SID utilisateurs

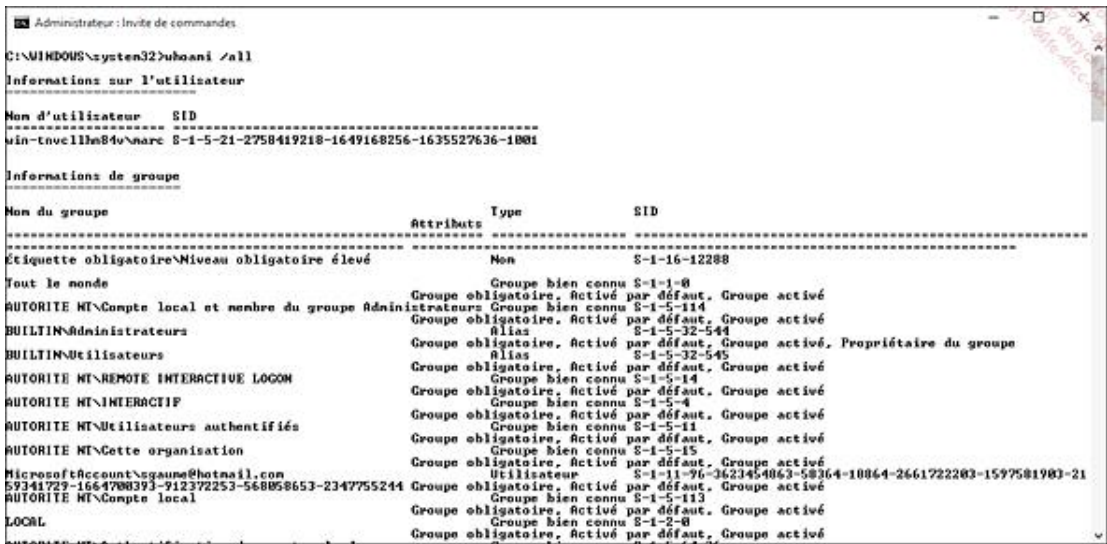
Un SID (*Security IDentifier*) est une manière unique d'identifier un utilisateur ou un groupe d'utilisateurs. Nous retrouvons ces identifiants dans les jetons d'accès, dans les ACL (*Access Control List*) et dans les bases de sécurité des comptes. Reportez-vous à la section suivante pour une description complète du mécanisme des ACL.

Les SID sont des données de longueur variable formant une représentation hiérarchique de l'acteur désigné. La syntaxe est la suivante : S-R-I-XXX-XXX-XXX.

- S : la lettre S (pour rappeler qu'il s'agit d'un SID).
- R : numéro du format binaire du SID.
- I : nombre entier identifiant l'autorité ayant émis le SID.
- XXX-XXX-XXX : suite de longueur variable, formée d'identifiants de sous-autorités ou d'identifiants relatifs (*Relative IDentifier* ou RID).

Vous pouvez afficher les SID de cette manière :

→ Depuis une invite de commandes, tapez : `whoami /all`.



Les informations suivantes sont visibles :

- Le SID correspondant au groupe Administrateurs est celui-ci : S-1-5-32-544.
- L'autorité ayant émis ce SID a pour identifiant le chiffre 5.
- La sous-autorité a pour identifiant le nombre 32.
- 544 est le RID du groupe Administrateurs.

Vous pouvez tester les résultats affichés par ces autres commandes :

- `whoami`
- `whoami /user /priv`
- `whoami /groups`

Les privilèges de l'utilisateur actuellement connecté seront affichés. Vous pouvez obtenir certains SID des utilisateurs ou des entités de sécurité en ouvrant cette arborescence du Registre : **HKEY\_LOCAL\_MACHINE - SOFTWARE - Microsoft - Windows NT - CurrentVersion - ProfileList**.

Enfin, les SID de certaines entités intégrées sont visibles dans cette autre arborescence : HKEY\_USERS.

## 2. Les listes de contrôle d'accès

Une liste de contrôle d'accès discrétionnaire (DACL ou *Discretionary Access Control Lists*, plus communément appelée ACL) est un mécanisme permettant de protéger des ressources telles que les fichiers et les clés du Registre. Les DACL contiennent des entrées de contrôles d'accès (ACE ou *Access Control Entry*) qui fonctionnent comme des enregistrements pour chaque utilisateur ou groupe d'utilisateurs désigné par son SID. Ces entrées associent une entité de sécurité (un compte d'utilisateur, un groupe de comptes, une entité système) à une règle définissant l'utilisation de la ressource. Les DACL et les ACE vous permettent d'accorder ou de refuser des droits aux ressources selon les autorisations que vous voulez associer aux comptes d'utilisateurs. Vous pouvez ainsi créer une ACE et l'appliquer à la DACL d'un fichier pour empêcher quiconque, à l'exception d'un administrateur, de modifier ce fichier.

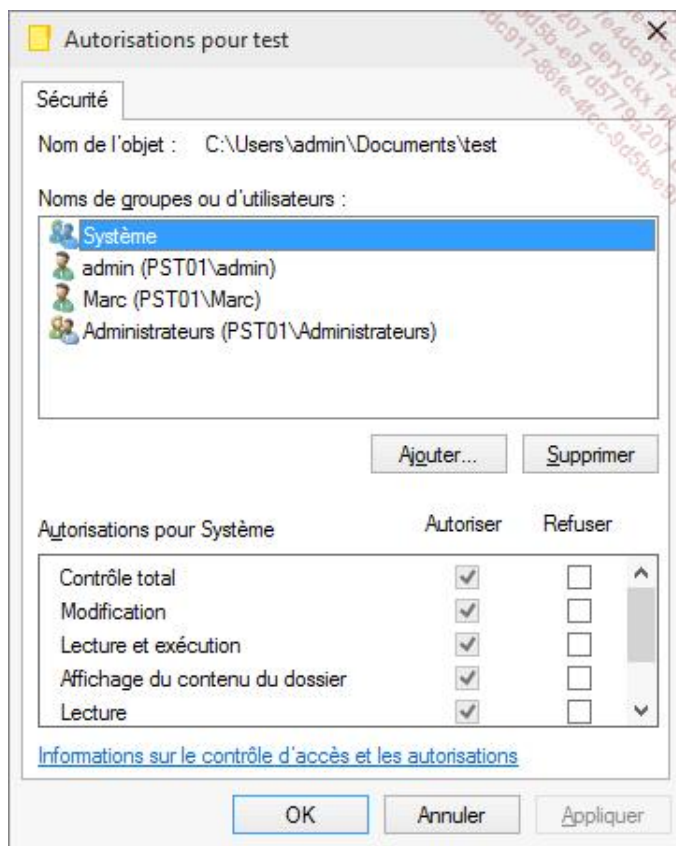
Une liste de contrôle d'accès système (SACL ou "ACE d'audit") est un mécanisme qui contrôle les messages d'audit associés à une ressource. Les SACL contiennent des ACE qui définissent les règles d'audit pour une ressource donnée.

Vous pouvez donc utiliser les DACL pour vous assurer que seul un administrateur peut modifier un fichier ; et les SACL pour vous assurer que toutes les tentatives d'ouverture d'un fichier qui aboutissent sont enregistrées. Il est courant de distinguer les ACE positives des ACE négatives :

- Dans l'Explorateur Windows, ouvrez votre répertoire d'utilisateur.
- Créez un nouveau dossier nommé *Test*.
- Effectuez un clic droit puis cliquez sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Sécurité**.

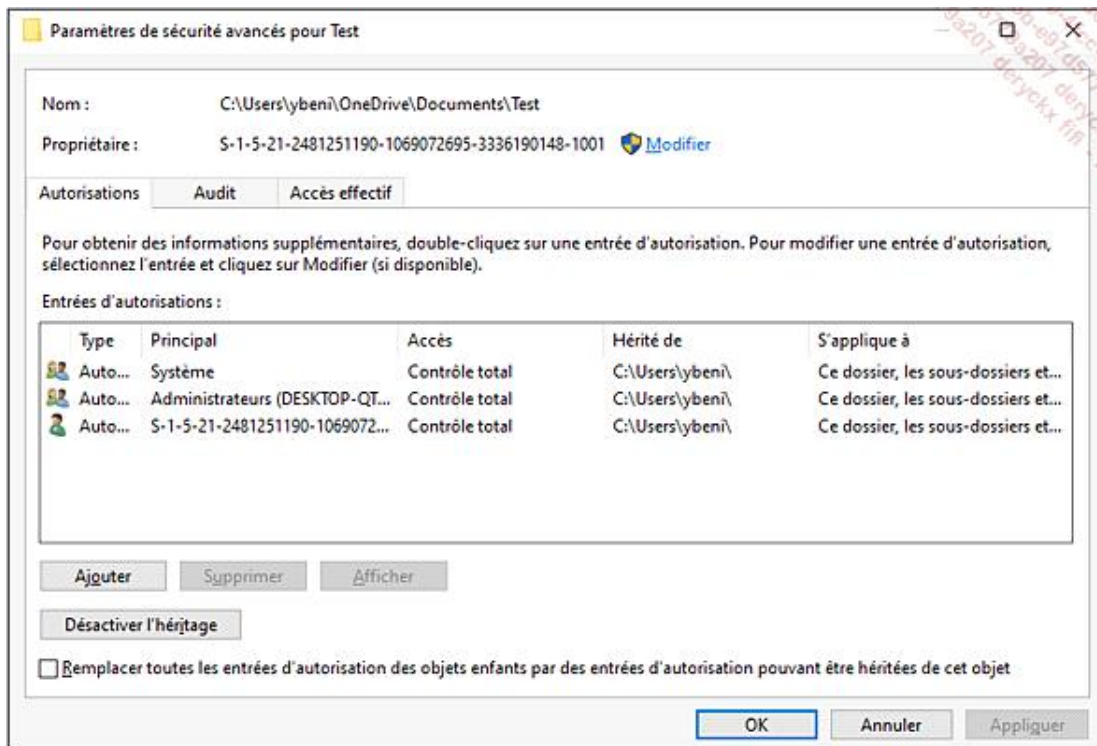


Notez que les ACE ou autorisations qui sont visibles sont toutes grisées puisqu'elles héritent du dossier parent.

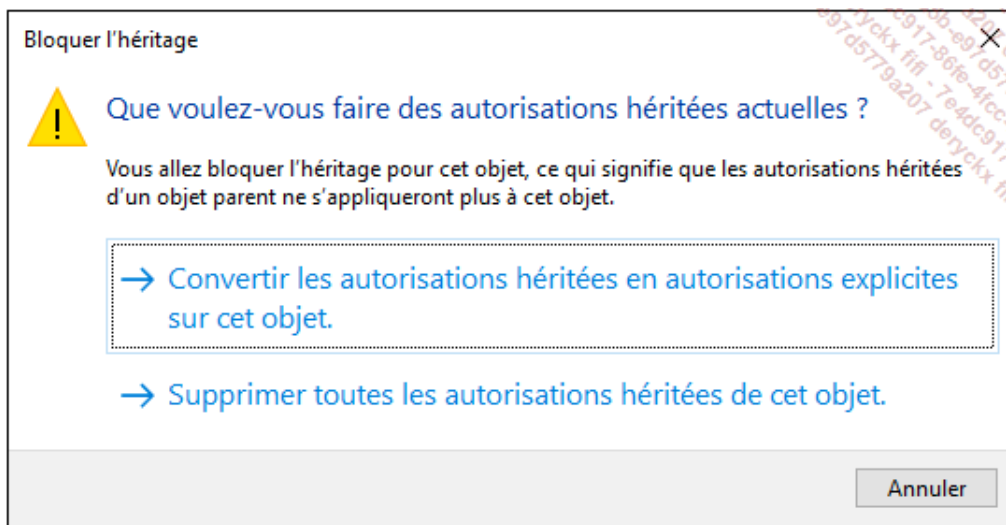


En fait, le dossier que vous venez de créer a hérité des permissions en vigueur dans le dossier parent. Ce mécanisme de chaînage est appelé "héritage". Nous allons tout d'abord le désactiver :

→ Cliquez sur le bouton **Avancé**.



→ Cliquez sur le bouton **Désactiver l'héritage**.



- Cliquez sur le lien **Convertir les autorisations héritées en autorisations explicites sur cet objet.**
- Cliquez sur le bouton **OK**.
- Cliquez ensuite sur **OK**.
- Cliquez sur le bouton **Modifier**.
- Sélectionnez votre nom d'utilisateur.

Vous pouvez maintenant cocher la case **Refuser** afin de paramétrer une ACE négative.

Quand le système procède à une vérification des accès, il commence systématiquement par les ACE négatives. Ainsi, les permissions "Refuser" ont toujours la priorité sur les permissions "Autoriser".

Dernier point : nous avons vu que le principe de base repose sur un souci de "non-dissémination de l'information". Il y a une particularité dans les systèmes d'exploitation NT : quand un utilisateur crée un fichier, il en est le propriétaire (owner). Le SID du propriétaire est placé dans le descripteur de sécurité que le système de fichiers NTFS maintient pour l'objet correspondant. Le propriétaire a le pouvoir de lire le descripteur de sécurité et donc, par exemple, de modifier l'ACL d'un fichier.

- Afin de connaître le propriétaire du dossier que vous venez de créer, cliquez sur l'onglet **Sécurité** puis sur le bouton **Avancé**.

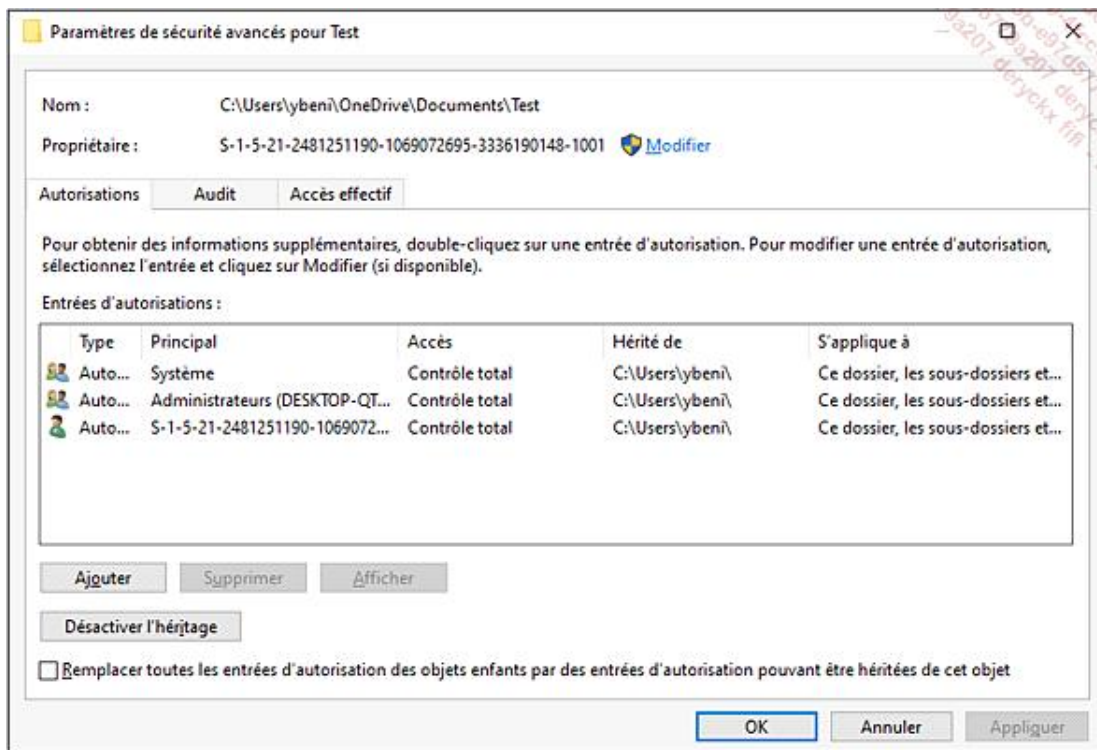
Vous visualisez directement le propriétaire du dossier. Vous pouvez cliquer sur le lien **Modifier** pour changer de propriétaire.

Puisque le propriétaire d'un objet a toujours le droit de lire et de modifier la DACL des objets lui appartenant, le contrôle d'accès est qualifié de discrétionnaire (à la discrétion du propriétaire).

### 3. S'approprier un objet

- Cliquez sur le bouton **Avancé**.

Vous visualisez directement le propriétaire du dossier dans les paramètres de sécurité avancés de celui-ci.



Par défaut, c'est votre compte d'utilisateur qui sera mentionné comme étant le propriétaire de la ressource. Vous pouvez le changer rapidement de cette façon :

→ Cliquez sur le lien **Modifier**.

Vous devez rechercher ou directement renseigner le compte ou le groupe utilisateur que vous souhaitez définir en tant que propriétaire. Vous pouvez ajouter d'autres groupes d'utilisateurs en cliquant sur le bouton correspondant.

→ Sélectionnez le groupe des administrateurs puis cliquez sur le bouton **Appliquer**.

→ Si vous désirez que cette opération s'applique à tous les objets enfants, cochez la case **Remplacer le propriétaire des sous-conteneurs et des objets**.

Une boîte de dialogue vous avertit que vous devrez fermer les propriétés de l'objet afin que la modification d'appropriation soit visible.

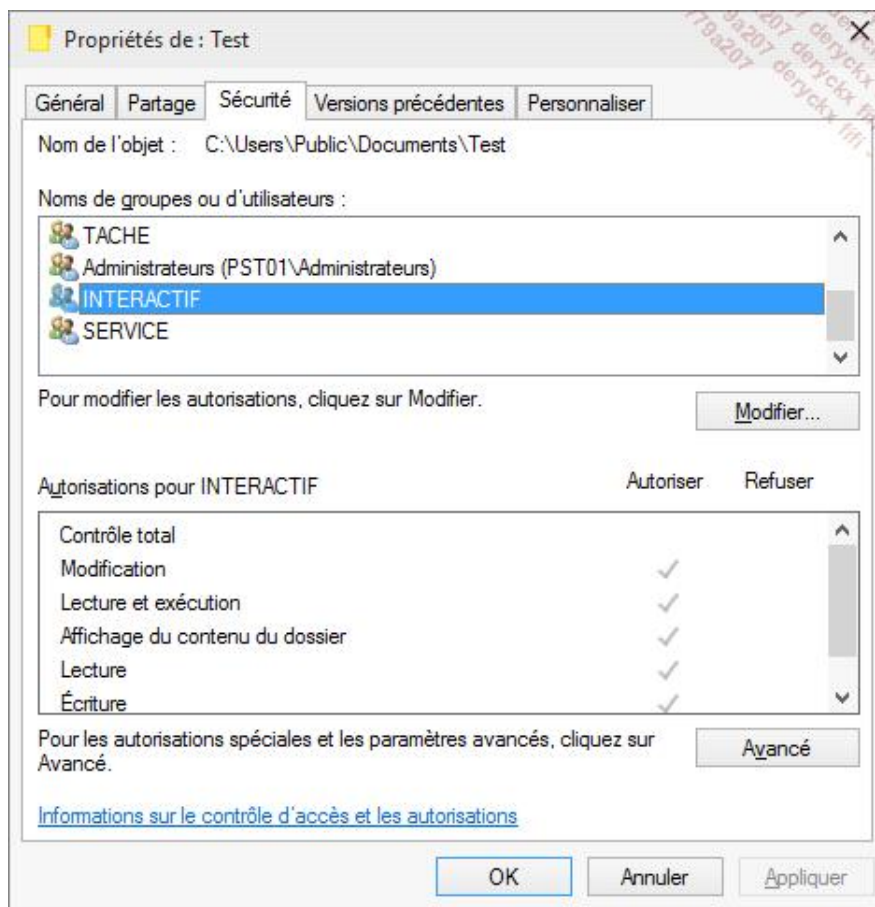
## 4. Utiliser les permissions NTFS

Prenons maintenant l'exemple d'un administrateur nommé Jean souhaitant partager un dossier en écriture pour un utilisateur nommé Marc et seulement en lecture pour un autre utilisateur nommé Anne.

→ Créez tout d'abord un dossier dans le dossier *Users\Public\Documents publics* nommé *Test*.

→ À l'intérieur, créez le fichier qui doit être visible. Il peut s'appeler *Fichier.txt*.

N'importe quel utilisateur aura accès à votre dossier et pourra modifier le document puisque l'entité système **INTERACTIF** possède des autorisations spéciales sur le contenu de ce dossier. Cette entité regroupe tous les utilisateurs qui ont ouvert une session interactive sur Windows.



- Commencez tout d'abord par désactiver le mécanisme d'héritage, copiez les permissions puis supprimez le groupe **INTERACTIF**.

Le dossier ne sera alors plus accessible pour les utilisateurs Marc et Anne.

Signalons que puisque vous faites partie du groupe des administrateurs vous n'avez pas de problème d'accès sur ce dossier.

- Une fois ce préalable effectué, ajoutez l'utilisateur nommé Anne.

Anne pourra visualiser le contenu du fichier sans pouvoir le supprimer ou le modifier, ni créer d'autres documents.

Par défaut, les trois autorisations génériques qui ont été ajoutées sont celles-ci : **Lecture et exécution - Affichage du contenu du dossier - Lecture**.

- Ajoutez maintenant un utilisateur nommé Marc.
- Cliquez sur le bouton **Avancé**, puis sélectionnez l'utilisateur Marc.
- Cliquez sur le bouton **Modifier**, puis sur le lien **Afficher les autorisations avancées**.
- Cochez ces quatre cases :

- **Création de fichier/écriture de données**
- **Création de dossier/ajout de données**
- **Attribut d'écriture**
- **Écriture d'attributs étendus**



L'utilisateur Marc peut quant à lui modifier le contenu du fichier, ajouter d'autres documents, mais en aucun cas :

- Changer le jeu des permissions NTFS.
- S'approprier le dossier.
- Supprimer le dossier ou le fichier.

## 5. S'approprier un répertoire

La commande **TakeOwn** permet à un administrateur (sous Windows) de récupérer l'accès à un fichier qui avait été refusé en modifiant le propriétaire du fichier.

La syntaxe est la suivante :

```
TAKEOWN [/S système] [/U utilisateur [/P mot_de_passe]] /F nom_fichier  
[/A] [/R [/D invite_de_commandes]]
```

Les commutateurs sont :

- **/s** : spécifie le système distant auquel se connecter.
- **/u** : [domaine\]utilisateur : spécifie le contexte utilisateur dans lequel la commande doit s'exécuter. Ce commutateur ne peut pas être employé sans **/s**.
- **/p** : [mot\_de\_passe] : définit le mot de passe du contexte utilisateur donné.
- **/f** : nom\_fichier : spécifie le nom de fichier ou de répertoire. Vous pouvez utiliser le caractère générique \* pour englober plusieurs fichiers.
- **/a** : attribue l'appartenance au groupe des administrateurs et non à l'utilisateur actuel. Si ce commutateur n'est pas spécifié, l'appartenance de fichier sera attribuée à l'utilisateur actuellement connecté.
- **/r** : traite la commande en mode récursif. L'opération portera donc sur l'ensemble des répertoires et des sous-répertoires.
- **/d** : invite\_commandes : permet de définir une réponse par défaut qui sera utilisée lorsque l'utilisateur actuel ne possède pas l'autorisation "lister le dossier" sur un répertoire. Ceci se produit lors du traitement récursif (/R) sur les sous-répertoires. Utilisez les valeurs "O" pour prendre possession ou "N" pour ignorer.

Voici un exemple d'utilisation.

Après une installation de Windows, certains répertoires placés sur une autre partition ne sont plus accessibles, même à partir d'un compte d'utilisateur possédant des privilèges d'administrateur. L'explication est simple : les ACL sont paramétrées en fonction de SID qui n'existe plus sur votre système. Vous pouvez dans ce cas utiliser ces deux commandes :

- `takeown /f Nom_Répertoire /r /d o`. Un message va vous avertir de cette manière : "Opération réussie : le fichier (ou dossier) : Emplacement et Nom\_Fichier" appartient désormais à l'utilisateur "Ordinateur1\Nom\_Utilisateur".
- `icacls Nom_Répertoire /grant administrateurs:f /t`.

L'accès au répertoire sera désormais possible ! Notez que vous devez exécuter l'invite de commandes en tant qu'administrateur, sinon vous aurez un message indiquant que l'accès sera refusé. Voici un autre exemple de

commandes permettant de vous approprier le fichier Hosts :

- `takeown /f c:\windows\system32\drivers\etc\hosts`
- `icaccls c:\windows\system32\drivers\etc\hosts /grant admin:f`



```
Administrateur : Invite de commandes

C:\WINDOWS\system32>takeown /f c:\windows\system32\drivers\etc\hosts
Opération réussie : le fichier (ou dossier) : "c:\windows\system32\drivers\etc\hosts" appartient désormais à l'utilisateur "PST01\admin".

C:\WINDOWS\system32>icaccls c:\windows\system32\drivers\etc\hosts /grant admin:f
Fichier traité : c:\windows\system32\drivers\etc\hosts
1 fichiers correctement traités ; échec du traitement de 0 fichiers

C:\WINDOWS\system32>
```

La syntaxe de `icaccls` est expliquée par la suite.

## 6. Modifier les listes de contrôle d'accès

À partir de l'invite de commandes, vous pouvez modifier les ACL des fichiers en vous servant d'un outil nommé `icaccls`. Voici les différentes syntaxes possibles :

```
icaccls Objets /save Nom_Fichier [/T] [/C] [/L]
```

Stocke les listes de contrôle d'accès pour tous les fichiers correspondants dans `Nom_Fichier`. Cette commande permet par la suite d'utiliser le paramètre `/restore`.

```
icaccls Nom_Répertoire [/substitute Ancien_SID Nouveau_SID [...]]
/restore Nom_Fichier [/C] [/L]
```

Applique les listes de contrôle d'accès stockées aux fichiers présents dans le répertoire.

```
icaccls Objets /setowner utilisateur [/T] [/C] [/L]
```

Modifie le nom du propriétaire pour tous les fichiers correspondants.

```
icaccls Objets /findsid SID [/T] [/C] [/L]
```

Recherche tous les fichiers correspondants qui contiennent une liste de contrôle d'accès mentionnant de façon explicite le SID.

```
icaccls Objets /verify [/T] [/C] [/L]
```

Recherche tous les fichiers dont la liste de contrôle d'accès n'est pas canonique ou dont les longueurs ne sont pas cohérentes avec les nombres d'entrées de contrôle d'accès.

```
icaccls Objets /reset [/T] [/C] [/L]
```



Remplace les listes de contrôle d'accès par les listes héritées par défaut pour tous les fichiers correspondants.

```
icacls Objets /grant[:r] SID:autorisation[...]
```

Octroie les droits d'accès utilisateur spécifiés.

- Avec le commutateur **:r**, les autorisations remplacent toute autorisation explicite précédemment accordée.
- Sans le commutateur **:r**, les autorisations sont ajoutées aux autorisations explicites précédemment accordées.

```
icacls Objets /deny ISD:autorisation
```

Refuse de manière explicite les droits d'accès aux utilisateurs spécifiés. Une entrée de contrôle d'accès de refus explicite est ajoutée aux autorisations mentionnées et les mêmes autorisations dans tout accord explicite sont supprimées.

```
icacls Objets /remove[:[g|d]] SID
```

Supprime toutes les occurrences de SID dans la liste de contrôle d'accès.

- Avec le commutateur **:g**, toutes les occurrences de droits accordés à ce SID sont supprimées.
- Avec le commutateur **:d**, toutes les occurrences de droits refusés à ce SID sont supprimées.

```
icacls Objets /setintegritylevel [(CI)(OI)]
```

Ce niveau ajoute explicitement une ACE d'intégrité (un niveau d'intégrité) au dossier correspondant. Le niveau peut être :

- **L[ow]**
- **M[edium]**
- **H[igh]**

Les options d'héritage de l'ACE d'intégrité peuvent précéder le niveau et ne sont appliquées qu'aux répertoires.

Les SID peuvent être spécifiés au format numérique ou sous forme de nom convivial. Si le format numérique est utilisé, ajoutez un astérisque avant l'indication du SID.

- **/T** indique que cette opération est effectuée sur tous les fichiers/répertoires correspondants qui se trouvent sous les répertoires spécifiés dans le nom.
- **/C** indique que cette opération se poursuivra sur toutes les erreurs de fichiers. Les messages d'erreurs continueront à s'afficher.
- **/L** indique que cette opération est effectuée directement sur un lien symbolique plutôt que sur sa cible.

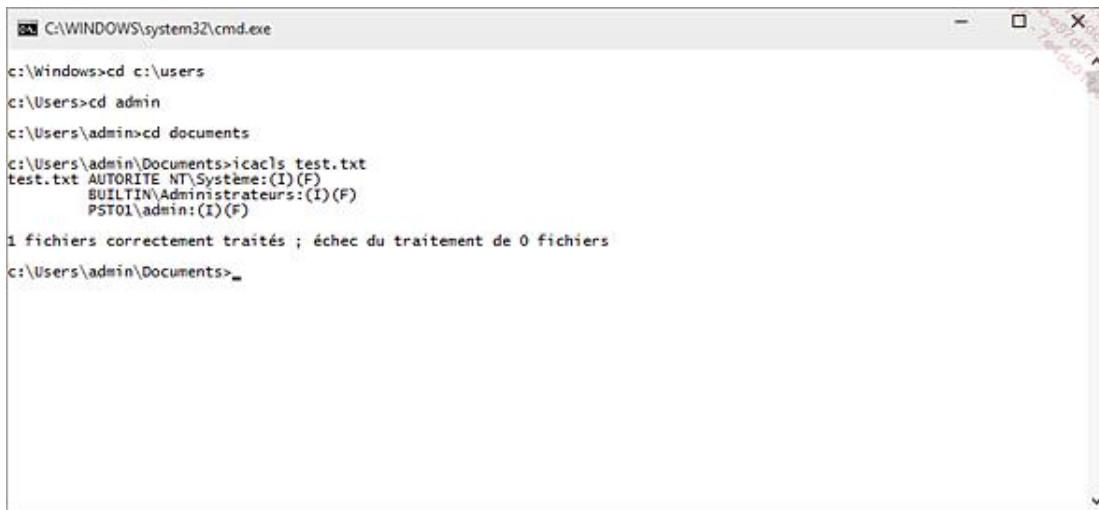
N'hésitez pas à consulter le fichier d'aide de cette commande pour obtenir plus d'informations.

## 7. Utiliser icacls

→ De la même façon que précédemment, créez un fichier nommé *Test* dans votre répertoire d'utilisateur.

→ Visualisez la liste des ACL en utilisant cette commande : `icaccls test`.

Trois utilisateurs ou groupes d'utilisateurs seront donc listés : vous, le groupe SYSTEM et le groupe des Administrateurs.



```
C:\WINDOWS\system32\cmd.exe
c:\Windows>cd c:\users
c:\Users>cd admin
c:\Users\admin>cd documents
c:\Users\admin\Documents>icaccls test.txt
test.txt  AUTORITE NT\Système:(I)(F)
          BUILTIN\Administrateurs:(I)(F)
          PST01\admin:(I)(F)

1 fichiers correctement traités ; échec du traitement de 0 fichiers
c:\Users\admin\Documents>
```

- Ils possèdent tous le contrôle total sur ce répertoire : (F).
- L'ACL est héritée : (I).

→ Afin de sauvegarder le masque des permissions, tapez `icaccls test.txt /save "Permissions du fichier Test"`.

Le fichier peut s'ouvrir avec le Bloc-notes Windows. Il énumère les SID des utilisateurs, ainsi que la liste des permissions en utilisant la syntaxe SDDL.