**Droits et Autorisations**

*Par THOREZ Nicolas*

***I – NTFS***

Un ACL donne, pour chaque utilisateur ou groupe renseigné dans sa liste, un groupe de droits. Il existe 6 droits, chacune étant un ensemble d'autorisations choisis parmi 13 autorisations spéciales.

|  |  |
| --- | --- |
| **Autorisations Spéciales** | **Spécificités** |
| Parcours de dossier / Exécuter de fichier | Permet à l'utilisateur de se déplacer dans les dossiers pour atteindre d'autres dossiers ou fichiers / permet ou interdit l'exécution de fichiers programmes |
| Liste du dossier / Lecture de données | Permet ou interdit l'affichage des noms des fichiers et des sous-dossiers contenus dans le dossier / permet ou interdit l'affichage des données des fichiers |
| Attributs de lecture | Permet ou interdit l'affichage des attributs d'un fichier ou d'un dossier |
| Lecture des attributs étendus | Permet ou interdit l'affichage des attributs étendus d'un fichier ou d'un dossier |
| Création de fichiers / Écriture de données | Permet ou interdit de créer des fichiers au sein du dossier / permet ou interdit de modifier le fichier et d'en remplacer le contenu actuel |
| Création de dossier / ajout de données | Permet ou interdit de créer des dossiers au sein du dossier / permet ou interdit de modifier la fin du fichier mais pas de modifier, de supprimer ou de remplacer les données existantes |
| Attribut d'écriture | Permet ou interdit de modifier les attributs d'un fichier ou d'un dossier tels que les attributs Lecture seule ou Masqué |
| Écriture d'attributs étendus | Permet ou interdit la modification des attributs étendus d'un fichier ou d'un dossier |
| Suppression de sous-dossier et fichier | Permet ou interdit de supprimer des sous-dossiers et des fichiers même si l'autorisation Supprimer n'a pas étéoctroyée pour le sous-dossier ou le fichier concerné |
| Suppression | Permet ou interdit de supprimer le fichier ou le dossier |
| Autorisations de lecture | Permet ou interdit les autorisations de lecture du fichier ou du dossier |
| Modifications des autorisations | Permet ou interdit de modifier les autorisations du fichier ou du dossier |
| Appropriation | Permet ou interdit de prendre possession du fichier ou du dossier |

|  |  |
| --- | --- |
| **Droits ACL** | **Autorisations correspondantes** |
| Contrôle total | Sur les dossiers, sous-dossiers et fichiers :• Toutes |
| Modification | Sur les dossiers, sous-dossiers et fichiers :• Parcours de dossier / Exécuter de fichier• Liste du dossier / Lecture de données• Attributs de lecture• Lecture des attributs étendus• Création de fichiers / Écriture de données• Création de dossier / ajout de données• Attribut d'écriture• Écriture d'attributs étendus• Suppression• Autorisations de lecture |
| Lecture et exécution | Sur les dossiers, sous-dossiers et fichiers :• Parcours de dossier / Exécuter de fichier• Liste du dossier / Lecture de données• Attributs de lecture• Lecture des attributs étendus• Autorisations de lecture |
| Affichage du contenu du dossier | Sur les dossiers, sous-dossiers et fichiers :• Parcours de dossier / Exécuter de fichier• Liste du dossier / Lecture de données• Attributs de lecture• Lecture des attributs étendus• Autorisations de lecture |
| Lecture | Sur les dossiers, sous-dossiers et fichiers :• Liste du dossier / Lecture de données• Attributs de lecture• Lecture des attributs étendus• Autorisations de lecture |
| Écriture | Sur les dossiers, sous-dossiers et fichiers :• Création de fichiers / Écriture de données• Création de dossier / ajout de données• Attribut d'écriture• Écriture d'attributs étendus |

En plus des droits et autorisations, chaque objet possède un propriétaire, visible dans l'option Propriétés, onglet Sécurité\Paramètres avancés\Propriétaire. A l'origine, le propriétaire d'un fichier est l'utilisateur qui le crée. Pour le cas des administrateurs, l'objet appartient au groupe des administrateurs.

Par défaut, les droits sont hérités des parents aux enfants. Il en est de même pour les droits rajoutés manuellement par un utilisateur. Cette héritage peut être contrôlé, via l'onglet avancé, afin de :

• hériter des parents les droits qui s'appliquent aux enfants;

• imposer un héritage spécifique aux enfants.

***II – SMB***

En parallèle aux droits NTFS, windows gère aussi des droits SMB (Samba) lors de l'utilisation des dossiers partages. Ces droits sont plus simples à gérer car moins nombreux, seulement 3. On y trouve :

|  |  |
| --- | --- |
| **Droits SMB** | **Autorisations accordées** |
| Contrôle total | • affichage des noms des fichiers et des sous-dossiers• accès aux sous-dossiers• affichage des données des fichiers• exécution des fichiers programmes• ajout de fichiers et de sous-dossiers• modification des données dans les fichiers• suppression de sous-dossiers et de fichiers• modification des autorisations (uniquement pour les fichiers et dossiers NTFS)• appropriation (fichiers et dossiers NTFS uniquement) |
| Modifier | • affichage des noms des fichiers et des sous-dossiers• accès aux sous-dossiers• affichage des données des fichiers• exécution des fichiers programmes• ajout de fichiers et de sous-dossiers• modification des données dans les fichiers• suppression de sous-dossiers et de fichiers |
| Lecture | • affichage des noms des fichiers et des sous-dossiers• accès aux sous-dossiers• affichage des données des fichiers• exécution des fichiers programmes |

Comme pour les droits NTFS, les droits SMB s'appliquent aux utilisateurs mentionnés dans l'option Propriétés, onglet Partage\Autorisations d'un dossier. Un utilisateur ayant les droits d'administration sur un dossier peut ajouter, supprimer un utilisateur ou un groupe et ajouter, supprimer ou modifier les droits d'un utilisateur ou d'un groupe.

L'ensemble des droits NTFS et SMB permettent de contrôler l'accès et l'utilisation des ressources mises à disposition sur un poste et un réseau.

**Propagation des autorisations NTFS**

Légende : Les dossiers et fichiers en jaune possèdent l’autorisation NTFS (héritée ou directe).
Les autorisations avec un carré rouge sont activés.



**Interprétation des codes d’autorisation NTFS sous ICACLS**

.

**L'option "Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur" n'est pas cochée**

|  |  |  |  |
| --- | --- | --- | --- |
| **S'applique à** | **Code** | **Ligne** | **Colonne** |
| Ce dossier seulement |  | 1 | 2 |
| Ce dossier et les sous-dossiers | (CI) | 1 | 3 |
| Les sous-dossiers seulement | (CI) (IO) | 3 | 2 |
| Ce dossier et les fichiers | (OI) | 1 | 4 |
| Fichiers seulement | (OI) (IO) | 3 | 3 |
| Ce dossier, les sous-dossiers et les fichiers | (CI) (OI) | 3 | 1 |
| Les sous-dossiers et les fichiers seulement | (CI) (OI) (IO) | 2 | 1 |

IO "Héritage uniquement"

Les autorisations NTFS ne s'appliquent pas au répertoire parent

Le tableau suivant vous permet d'interpréter les codes.

**L'option "Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur" est cochée**

|  |  |  |  |
| --- | --- | --- | --- |
| **S'applique à** | **Code** | **Ligne** | **Colonne** |
| Ce dossier et les sous-dossiers + **NP** | (CI) (NP) | 2 | 2 |
| Les sous-dossiers seulement + **NP** | (CI) (IO) (NP) | 4 | 1 |
| Ce dossier et les fichiers + **NP** | (OI) (NP) | 2 | 3 |
| Fichiers seulement + **NP** | (OI) (IO) (NP) | 4 | 2 |
| Ce dossier, les sous-dossiers et les fichiers + **NP** | (CI) (OI) (NP) | 2 | 4 |
| Les sous-dossiers et les fichiers seulement + **NP** | (CI) (OI) (IO) (NP) | 4 | 3 |

IO "Héritage uniquement"

Les autorisations NTFS ne s'appliquent pas au répertoire parent

NP "Ne pas transmettre l’héritage" signifie que l'option

"Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur" est cochée.

**Commandes ICACLS**

**C:\Windows\system32>icacls.exe /?**

**ICACLS nom /save fichierACL [/T] [/C] [/L] [/Q]**

 **Stocke les listes de contrôle d'accès discrétionnaire pour les fichiers et**

 **les dossiers qui correspondent au nom dans fichierACL pour une utilisation**

 **ultérieure avec /restore. Notez que les SACL, le propriétaire et les noms**

 **d'intégrité ne sont pas enregistrés.**

**ICACLS répertoire [/substitute AncienSID NouveauSID [...]] /restore fichierACL**

 **[/C] [/L] [/Q]**

 **Applique les listes de contrôle d'accès discrétionnaire stockées aux**

 **fichiers présents dans le répertoire.**

**ICACLS nom /setowner utilisateur [/T] [/C] [/L] [/Q]**

 **Modifie le propriétaire de tous les noms correspondants. Cette option ne**

 **force pas la modification du propriétaire ; utilisez pour cela l'utilitaire**

 **takeown.exe.**

**ICACLS nom /findsid SID [/T] [/C] [/L] [/Q]**

 **Recherche tous les noms correspondants qui contiennent une liste de**

 **contrôle d'accès mentionnant de façon explicite le SID.**

**ICACLS nom /verify [/T] [/C] [/L] [/Q]**

 **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.**

**ICACLS nom /reset [/T] [/C] [/L] [/Q]**

 **Remplace les listes de contrôle d'accès par les listes héritées par défaut**

 **pour tous les fichiers correspondants.**

**ICACLS nom [/grant[:r] Sid:perm[...]]**

 **[/deny Sid:perm [...]]**

 **[/remove[:g|:d]] SID[...]] [/T] [/C] [/L] [/Q]**

 **[/setintegritylevel Level:policy [...]]**

 **/grant[:r] Sid:perm - Octroie les droits d'accès utilisateur**

 **spécifiés. Avec :r, les autorisations remplacent toute autorisation**

 **explicite précédemment accordée.**

 **Sans :r, les autorisations sont ajoutées aux autorisations explicites**

 **précédemment accordées.**

 **/deny Sid:perm - Refuse de manière explicite les droits d'accès**

 **utilisateur 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.**

 **/remove[:[g|d]] SID - Supprime toutes les occurrences de SID dans la liste**

 **de contrôle d'accès. Avec**

 **:g, toutes les occurrences de droits accordés à ce SID sont**

 **supprimées. Avec**

 **:d, toutes les occurrences de droits refusés à ce SID sont supprimées.**

 **/setintegritylevel [(CI)(OI)]Ce niveau ajoute explicitement un ACE**

 **d'intégrité à tous les fichiers correspondants. Le niveau peut être :**

 **L[ow]**

 **M[edium]**

 **ou H[igh]**

 **Les options d'héritage de l'ACE d'intégrité peuvent précéder le niveau**

 **et ne sont appliquées qu'aux répertoires.**

 **/inheritance:e|d|r**

 **e - Active l'héritage.**

 **d - Désactive l'héritage et copie les ACE.**

 **r - Supprime toutes les ACE héritées.**

**Remarque :**

 **Les SID peuvent être spécifiés au format numérique ou sous forme de nom**

 **convivial. Si le format numérique est utilisé, ajoutez un \* avant le 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.**

 **/Q indique qu'icacls doit supprimer les messages de réussite.**

 **ICACLS conserve l'ordre canonique des entrées de contrôle d'accès :**

 **Refus explicites**

 **Octrois explicites**

 **Refus hérités**

 **Octrois hérités**

 **L'argument autorisation est un masque d'autorisation et peut être fourni**

 **sous deux formes :**

 **une série de droits simples :**

 **N - Aucun accès**

 **F - Accès complet**

 **M - Accès en modification**

 **RX - Accès en lecture et exécution**

 **R - Accès en lecture seule**

 **W - Accès en écriture seule**

 **D - Accès en suppression**

 **une liste séparée par des virgules de droits spécifiques entre**

 **parenthèses :**

 **DE - Suppression**

 **RC - Contrôle en lecture**

 **WDAC - Accès en écriture à la liste de contrôle d'accès**

 **WO - Accès en écriture du propriétaire**

 **S - Synchronisation**

 **AS - Accès à la sécurité système**

 **MA - Maximum autorisé**

 **GR - Lecture générique**

 **GW - Écriture générique**

 **GE - Exécution générique**

 **GA - Générique pour tout**

 **RD - Lecture de données/Liste du répertoire**

 **WD - Écriture de données/Ajout de fichiers**

 **AD - Ajout de données/Ajout de sous-répertoires**

 **REA - Attributs de lecture étendus**

 **WEA - Attributs d'écriture étendus**

 **X - Exécution/Parcours**

 **DC - Suppression de l'enfant**

 **RA - Attributs de lecture**

 **WA - Attributs d'écriture**

 **Les droits d'héritage peuvent précéder n'importe quelle forme et ne**

 **sont appliqués qu'aux répertoires :**

 **(OI) - Héritage d'objet**

 **(CI) - Héritage de conteneur**

 **(IO) - Héritage uniquement**

 **(NP) - Ne pas transmettre l'héritage**

 **(I) - Autorisation héritée du conteneur parent**

**Exemples :**

 **icacls c:\windows\\* /save fichierACL /T**

 **- Enregistre les listes de contrôle d'accès de tous les fichiers**

 **sous c:\windows et ses sous-répertoires dans fichierACL.**

 **icacls c:\windows\ /restore fichierACL**

 **- Restaure les listes de contrôle d'accès pour tous les fichiers**

 **contenus dans le fichierACL présent dans c:\windows et ses**

 **sous-répertoires.**

 **icacls fichier /grant Administrateur:(D,WDAC)**

 **- Octroie à l'utilisateur Administrateur les autorisations d'accès**

 **en suppression et en écriture à la liste de contrôle d'accès**

 **au fichier.**

 **icacls fichier /grant \*S-1-1-0:(D,WDAC)**

 **- Octroie à l'utilisateur défini par le SID S-1-1-0 les autorisations**

 **d'accès en suppression et en écriture à la liste de contrôle**

 **d'accès au fichier.**

**C:\Windows\system32>icacls.exe C:\\_Lab4dTest\Inutile**

**C:\\_Lab4dTest\Inutile AUTORITE NT\Système:(I)(OI)(CI)(F)**

 **BUILTIN\Administrateurs:(I)(OI)(CI)(F)**

 **BUILTIN\Utilisateurs:(I)(OI)(CI)(RX)**

 **BUILTIN\Utilisateurs:(I)(CI)(AD)**

 **BUILTIN\Utilisateurs:(I)(CI)(WD)**

 **CREATEUR PROPRIETAIRE:(I)(OI)(CI)(IO)(F)**