Autorisations de partage et autorisations NTFS

Dernière mise à jour : 16/05/24

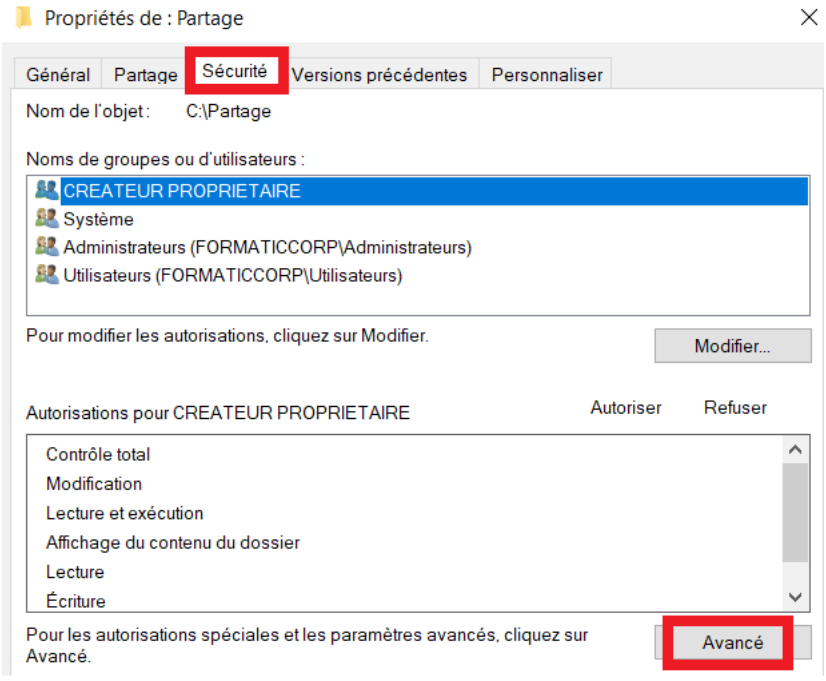
Les autorisations NTFS et les autorisations de partage servent toutes deux à empêcher les accès non autorisés.

Cependant, les **permissions NTFS** affectent à la fois les **utilisateurs locaux et les utilisateurs du réseau**.

Depuis **Windows NT**4, le système de fichiers des disques durs permet une gestion de la sécurité appelée **NTFS (New Technology File System)**. Outre l'encryption et la compression des fichiers, NTFS permet d'apposer des droits spécifiques à chaque dossier et fichier. A chaque dossier, fichier et imprimante est associé un fichier **ACL (Access Crontrol List)** qui indique qui possède quelles autorisations. On peut observer un ACL dans l'option Propriétés, onglet « Sécurité » d'un élément. 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.

Les principaux types d'autorisation d'accès :

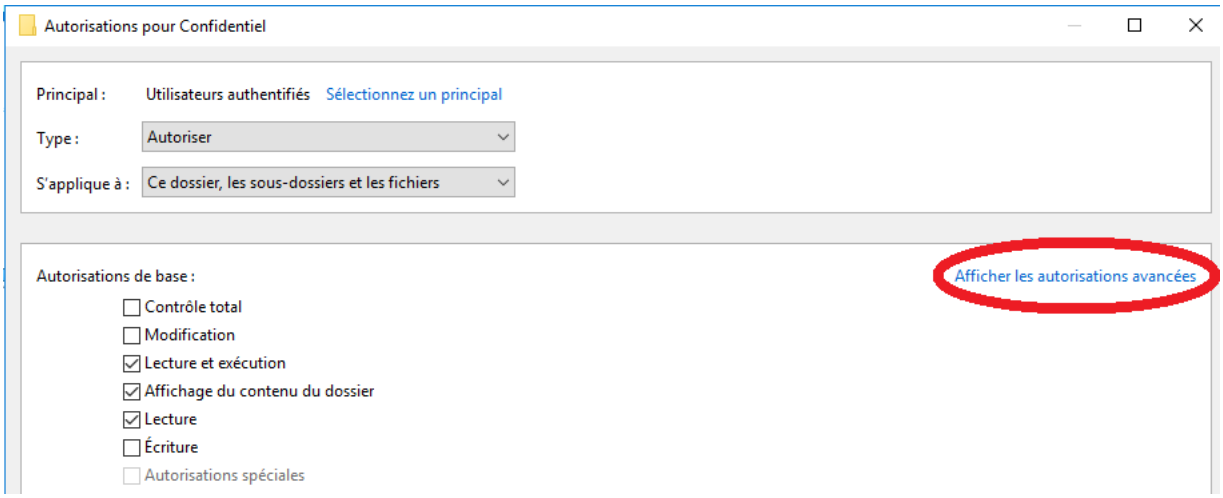
- **Contrôle total** – les utilisateurs peuvent modifier, ajouter, déplacer et supprimer des fichiers et des répertoires, ainsi que leurs propriétés associées. De plus, les utilisateurs peuvent modifier les paramètres des autorisations pour tous les fichiers et sous-répertoires.
- **Modification** – les utilisateurs peuvent afficher et modifier des fichiers et des propriétés de fichier, et supprimer ou ajouter des fichiers à un répertoire ou des propriétés de fichier à un fichier.
- **Lecture et exécution** – les utilisateurs peuvent exécuter des fichiers exécutables, y compris des scripts.
- **Lecture** – les utilisateurs peuvent voir les fichiers, leurs propriétés et leurs répertoires.
- **Écriture** – les utilisateurs peuvent écrire dans un fichier et ajouter des fichiers dans des répertoires.
- **Affichage du contenu du dossier** ou lister le contenu du dossier



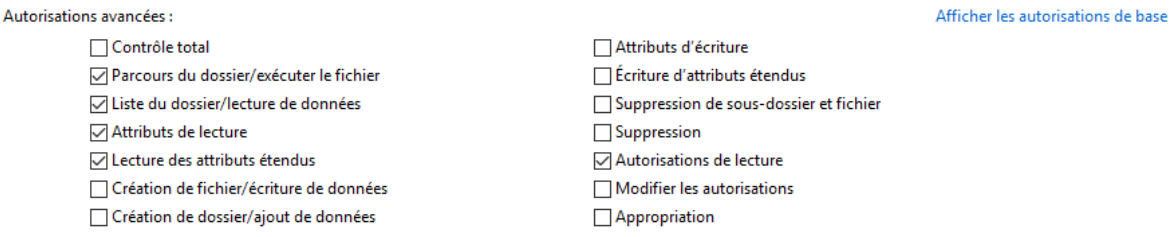
La notion d'**autorisation spéciales** concerne »le détail » des six groupes de permissions NTFS prédéfinis par défaut. Ces groupes de permissions correspondent en réalité au groupement de **droits spéciaux** ; on les utilise pour les droits « classiques », mais il est tout à fait possible d'assigner directement les droits spéciaux sur un objet :

Droits	Contrôle Total	Modifier	Lire et exécuter	Lister le contenu du dossier	Lecture	Ecriture
Traverser le dossier Exécuter le fichier	☑	☑	☑	☑		
Lister les dossiers Lire les données	☑	☑	☑	☑	☑	
Attributes de lecture	☑	☑	☑	☑	☑	
Attributes de lecture étendus	☑	☑	☑	☑	☑	
Créer des fichiers Ecrire des données	☑	☑				☑
Créer des dossiers Ajouter des données	☑	☑				☑
Attributs d'écriture	☑	☑				☑
Arributs d'écriture étendus	☑	☑				☑
Supprimer des sous-dossiers Supprimer des fichiers	☑					
Supprimer	☑	☑				
Lire les autorisations	☑	☑	☑	☑	☑	☑
Modifier les autorisations	☑					
Devenir propriétaire de l'objet	☑					
Syncrhoniser	☑	☑	☑	☑	☑	☑

Lors de l'ajout d'un nouveau droit NTFS, on peut avoir la liste complète en cliquant sur « Afficher les autorisations avancées :



Nous aurons alors le détail des six groupes de permissions NTFS prédéfinis (ou « de base ») :



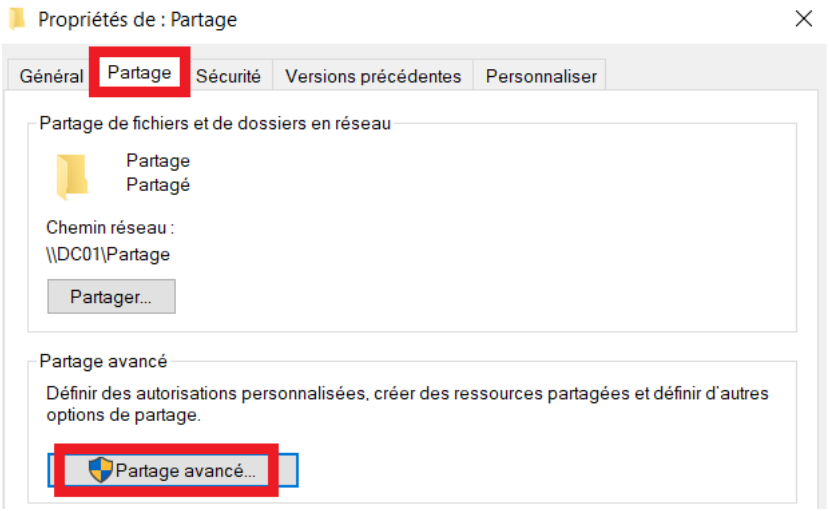
La notion d'**héritage** est un terme bien connut en programmation. On pourra faire en sortes que des dossiers et fichiers « enfants » héritent des propriétés de leur dossier « parent » .

En parallèle aux droits NTFS, windows gère aussi des droits **SMB (Server Message Block, SaMBa)** lors de l'utilisation des dossiers partages. Ces droits sont plus simples à gérer car moins nombreux, seulement 3.

Les **permissions de partage** gèrent l'accès aux dossiers partagés sur un réseau ; elles **ne s'appliquent pas aux utilisateurs** qui se connectent **localement**. Les autorisations de partage s'appliquent à tous les fichiers et dossiers du partage ; vous ne pouvez pas contrôler de manière granulaire l'accès aux sous-dossiers ou aux objets d'un partage.

Pour contrôler l'accès aux dossiers ou lecteurs partagés vous avez trois types d'autorisation de partage :

- **Lecture** – les utilisateurs peuvent afficher les noms des fichiers et des sous-dossiers, lire les données contenues dans les fichiers et exécuter des programmes. Par défaut, des autorisations « Lecture » sont attribuées au groupe « Tout le monde ».
- **Modification** – les utilisateurs peuvent faire tout ce qui est permis par l'autorisation « Lecture », ainsi qu'ajouter des fichiers et des sous-dossiers, modifier des données dans des fichiers et supprimer des sous-dossiers et des fichiers. Cette autorisation n'est pas attribuée par défaut.
- **Contrôle total** – les utilisateurs peuvent faire tout ce qui est permis par les autorisations « Lecture » et « Modification », et ils peuvent également modifier les autorisations pour les fichiers et dossiers NTFS uniquement. Par défaut, des autorisations « Contrôle total » sont attribuées au groupe « Administrateurs ».



Voici les principales différences entre les deux types de permissions :

- Les autorisations de partage sont faciles à appliquer et à gérer, mais les autorisations NTFS permettent un contrôle plus fin des dossiers partagés et de leur contenu.

- Si des autorisations de partage et des autorisations NTFS sont utilisées simultanément, l'autorisation la plus restrictive l'emporte toujours.

- Les autorisations de partage peuvent être utilisées lors du partage de dossiers dans les systèmes de fichiers FAT et FAT32 ; les autorisations NTFS ne le peuvent pas.

- Les autorisations NTFS s'appliquent aux utilisateurs qui sont connectés localement au serveur ; ce n'est pas le cas des autorisations de partage.

- À la différence des autorisations NTFS, les autorisations de partage vous permettent de limiter le nombre de connexions simultanées à un dossier partagé. Par défaut, nous avons 2^24, soit un peu plus de 16 millions de connexion simultanées possible sur vos dossiers partagés.

- Les autorisations de partage se configurent dans les propriétés des fichiers et dossiers puis « Partage avancé » des paramètres « Autorisations ». Les autorisations NTFS se configurent dans l'onglet « Sécurité », dans les propriétés du fichier ou du dossier.

Quand vous définirez des autorisations veillez à respecter au mieux les principes suivants :

- Attribuez des autorisations aux groupes et non aux comptes d'utilisateurs

- Appliquez le principe du moindre privilège

- N'utilisez les autorisations NTFS que pour les utilisateurs locaux

- Placez les éléments ayant les mêmes exigences de sécurité dans le même dossier

- Ne réglez pas les autorisations du groupe « Tout le monde » sur « Refuser »

- Évitez de refuser explicitement des autorisations à une ressource partagée

- Accordez au groupe « Administrateurs » l'autorisation « Contrôle total » sur le dossier partagé parent

- Surveillez de près l'appartenance au groupe « Administrateurs »

On pourra aussi choisir de n'utiliser que les permissions NTFS au sein de son réseau (si vous êtes dans un environnement « full Windows », pas de problèmes.

Faites maintenant un test de partage de dossier, attribuer à un groupe (par exemple votre GrpDeveloppeurs) de votre annuaire les droits totaux sur un dossier, et les droits de lecture uniquement pour un autre groupe (GrpSupport par exemple).

Testez en vous connectant avec différents utilisateurs sur vos machines clients :

- *Autorisations de partage « simple » / SMB*
- *Autorisations NTFS*
- *Notions d'héritages (Parents/Enfants)*
- *Lecture / Ecriture / Controle Total…*
- *Limitations du nombre d'utilisateurs simultanés*