



Travail en réseau

Un réseau permet, comme nous l'avons déjà vu, de partager des ressources : imprimantes, périphériques et surtout fichiers et dossiers. Le **partage de fichiers** consiste à rendre disponible à travers le réseau le contenu d'un ou plusieurs répertoires. Tous les systèmes Windows possèdent en standard des mécanismes permettant de mettre facilement en partage le contenu d'un répertoire. Néanmoins le partage de fichiers peut poser des problèmes de sécurité, car, par définition, il donne accès aux autres utilisateurs au contenu d'une partie du disque dur.

De ce fait, la sécurité des fichiers et le partage des fichiers sont tellement liés qu'il est difficile de parler de l'un sans aborder l'autre. La sécurité des fichiers protège les données vitales de vos systèmes en contrôlant les accès en fonction des besoins. Le partage de fichiers permet de rendre des données accessibles à autrui.

Les autorisations de partage ne servent que quand un utilisateur essaie d'accéder à un fichier ou dossier depuis un autre ordinateur du réseau, alors que les autorisations d'accès servent aussi bien pour les accès en local que pour les accès depuis le réseau. Lors d'un accès à distance aux données, sont d'abord appliquées les autorisations de partage puis les autorisations d'accès.

D'une certaine façon, les autorisations d'accès aux fichiers et les autorisations de partage de fichiers standard se comportent comme des enveloppes placées autour de vos données. Les autorisations d'accès, qui sont la première enveloppe, protègent vos données par rapport aux accès locaux. Si un utilisateur ouvre une

session locale sur une machine, les autorisations d'accès lui permettent ou lui interdisent d'accéder aux fichiers et dossiers. Les autorisations de partage, qui constituent la seconde enveloppe, servent quand vous voulez autoriser les accès distants. Si un utilisateur accède à distance aux données, les autorisations de partage lui accordent ou lui interdisent l'accès initial ; mais, comme vos données sont également enveloppées dans une couche de sécurité de fichier, l'utilisateur doit aussi passer à travers les autorisations d'accès pour pouvoir travailler sur les fichiers et dossiers.

Deux facteurs influent fortement sur les options de sécurité des fichiers dont vous disposez :

- Le type de formatage du disque.
- Le système d'exploitation ainsi que les paramètres de l'ordinateur.

Le format du disque local conditionne les options disponibles en matière de sécurité des fichiers.

Partage de fichiers

Le système d'exploitation et les paramètres d'un ordinateur déterminent les modalités du partage des fichiers. Windows reconnaît deux modèles de partage de fichier :

- Le partage de fichiers standard permet de partager les fichiers de n'importe quel dossier de votre ordinateur. Deux ensembles d'autorisations servent à déterminer qui a accès aux fichiers partagés : les autorisations d'accès et les autorisations de partage. C'est la combinaison de ces deux autorisations qui permet de décider qui dispose de l'accès aux fichiers partagés et avec quel niveau d'accès.
- Le partage du dossier Public permet de partager les fichiers du dossier `%SystemDrive%\Users\Public` d'un ordinateur. Les autorisations d'accès du dossier Public déterminent quels sont les utilisateurs et groupes qui disposent de l'accès aux fichiers publiquement partagés et quel est leur niveau d'accès. Quand vous copiez ou déplacez des fichiers vers le dossier Public, leurs autorisations d'accès sont modifiées de façon à refléter celles du dossier Public.

Si Windows XP ne pouvait employer qu'un seul modèle de partage à la fois, les versions suivantes (Vista et ultérieure) peuvent employer simultanément les deux. L'avantage clé du partage standard est que les utilisateurs peuvent partager n'importe quel dossier situé sur un ordinateur sans avoir à déplacer fichiers ou dossiers de leur emplacement initial. En revanche, les dossiers Public sont des boîtes ouvertes : les fichiers et dossiers qui y sont stockés sont disponibles pour tous les utilisateurs de l'ordinateur et sur le réseau.

Partage standard

Vous pouvez configurer le partage par défaut pour les membres d'un groupe résidentiel Windows 7, en lecture-écriture ou uniquement en lecture. Vous pouvez également n'activer le partage qu'avec des personnes spécifiques.

Pour partager la première ressource d'un ordinateur, vous devez être un administrateur local. Le fait de partager la première ressource autorise le partage d'autres ressources sur la machine et permet à tout utilisateur de partager les ressources dont il est propriétaire ou pour lesquelles il dispose des autorisations idoines. La création d'une ressource partagée se fait en plusieurs temps : vous partagez le fichier pour qu'il soit accessible, puis définissez les autorisations de partage et enfin vérifiez et modifiez si nécessaire les autorisations NTFS. Vous pouvez créer des partages à l'aide de l'explorateur Windows, de la console Gestion de l'ordinateur ou de l'utilitaire de ligne de commande NET SHARE. Vous pouvez également lancer directement l'assistant Création d'un dossier partagé pour partager un dossier du poste local en saisissant **shrpwbw** dans une invite de commandes élevée, puis en cliquant sur Suivant quand l'assistant démarre.

Par défaut, lorsque vous créez le premier partage de dossier standard sur un ordinateur, Windows crée l'exception Partage de fichiers et d'imprimantes dans le Pare-feu Windows. Cette exception entrante autorise les autres ordinateurs du réseau à envoyer du trafic SMB (*Server Message Block*) à travers le Pare-feu Windows pour accéder au partage. Pour ce faire, Windows ouvre le port UDP 137 (résolution de nom NetBIOS), le port UDP 138 (transmission et réception de datagrammes NetBIOS), le port TCP 139 (service NetBIOS Session) et, si nécessaire, des ports dynamiques pour ICMPv4 et ICMPv6.

Partage du dossier Public

Le partage du dossier Public permet aux utilisateurs de partager fichiers et dossiers depuis un unique emplacement. Il permet aux utilisateurs de repérer rapidement tout les fichiers qu'ils ont partagés publiquement avec autrui et de les classer par types.

Utilisation du partage du dossier Public

Pour accéder aux dossiers publics dans l'explorateur Windows, cliquez sur Démarrer puis sur Ordinateur. Dans l'explorateur Windows, cliquez sur le bouton le plus à gauche dans la liste d'adresses puis cliquez sur Public. Avec le partage public, vous copiez ou déplacez les fichiers que vous voulez partager vers le dossier %SystemDrive%\Users\Public d'un ordinateur.

Le dossier Public renferme plusieurs sous-dossiers permettant de classer les fichiers publics : Bureau public, Documents publics, Images publiques, Musique publique, Vidéos publiques, Enregistrements TV publics et Téléchargements publics.

Tous les fichiers placés dans l'un de ces sous-dossiers sont accessibles à chaque utilisateur qui ouvre une session sur la machine (ou qui s'y connecte via le réseau, si l'accès réseau est autorisé sur le dossier Public).

Par défaut, toute personne disposant d'un compte utilisateur et d'un mot de passe sur un ordinateur peut accéder au dossier Public. Quand vous copiez ou déplacez des fichiers vers le dossier Public, leurs autorisations d'accès sont modifiées de façon à refléter celles du dossier Public.

Il existe deux grandes façons de modifier la configuration de partage par défaut du dossier Public :

- Autoriser les utilisateurs disposant d'un accès réseau à voir et ouvrir les fichiers publics, mais les empêcher de modifier, créer ou supprimer des fichiers publics. Quand vous configurez cette option, le groupe implicite Tout le monde dispose des autorisations Lecture et exécution plus Lecture sur les fichiers publics, et les autorisations Lecture et exécution, Affichage du contenu du dossier plus Lecture sur les dossiers publics.

- Autoriser les utilisateurs ayant l'accès réseau à voir et gérer les fichiers publics. Cela leur permet d'ouvrir, modifier, créer et supprimer des fichiers publics. Quand vous configurez cette option, le groupe implicite Tout le monde a les autorisations Contrôle total sur les fichiers publics et sur le dossier public.

Partages spéciaux

Dans Windows, plusieurs partages spéciaux sont automatiquement créés et réservés aux administrateurs ou au système d'exploitation. La plupart des partages spéciaux sont cachés aux utilisateurs grâce à l'ajout du signe dollar (\$) à la fin du nom de partage. Comme administrateur, vous pourriez être amené à créer des partages cachés personnels ou à employer les partages spéciaux prédéfinis.

Les partages administratifs par défaut, accessibles uniquement aux administrateurs, sont les suivants :

- **CS\$** : accès à la partition ou au volume racine. Les autres partitions sont également accessibles par leur lettre, suivie du caractère « \$ ».
- **ADMIN\$** : accès au répertoire `%systemroot%`, permettant la gestion d'une machine sur le réseau.
- **IPC\$** : permet la communication entre les processus réseau.
- **PRINT\$** : accès à distance aux imprimantes.

Les outils privilégiés pour la gestion des partages spéciaux ou autres partages cachés sont les commandes *Net share* et Gestion de l'ordinateur. Pour voir la liste de tous les partages du poste local, y compris les partages spéciaux destinés aux administrateurs, il suffit de taper **net share** sur une invite de commande.

Utilisation d'une ressource partagée

Pour utiliser un dossier partagé, il existe deux méthodes :

- L'utilisation directe de la ressource grâce à son adresse. L'adresse d'une ressource partagée est sous la forme suivante :
`\\ordinateur\nom_du_partage`

- `ordinateur` représente le nom de l'ordinateur ou son adresse IP.
 - `nom_du_partage` correspond au nom donné à la ressource partagée.
- La connexion d'un lecteur réseau, permettant de lier la ressource partagée à une lettre de lecteur virtuel. Pour connecter un lecteur réseau, cliquez sur Démarrer, puis sur Ordinateur. Dans l'explorateur Windows, cliquez sur le bouton Connecter un lecteur réseau de la barre d'outils. S'ouvre alors la boîte de dialogue Connecter un lecteur réseau, dans laquelle vous effectuez les réglages nécessaires.

Autorisations NTFS

Si FAT (FAT16 ou FAT32) procure un contrôle très limité et peu fiable sur les accès fichier, NTFS permet de contrôler ceux-ci en assignant des autorisations qui permettent ou interdisent spécifiquement l'accès. Vous pouvez définir des autorisations pour des utilisateurs individuels et pour des groupes d'utilisateurs. Les autorisations NTFS sont toujours évaluées lors de l'accès à un fichier. Elles sont très complexes et se décomposent en plusieurs éléments.

Autorisations de base

Le propriétaire d'un fichier ou dossier peut autoriser ou interdire l'accès à cette ressource à un utilisateur ou à un groupe. Vous pouvez examiner depuis l'explorateur Windows les autorisations de base actives en cliquant avec le bouton droit de la souris sur un fichier ou dossier, en choisissant Propriétés, puis en cliquant sur l'onglet Sécurité de la boîte de dialogue des propriétés. La liste Groupes ou noms d'utilisateurs affiche tous les utilisateurs et groupes pour lesquels ont été définies des autorisations sur la ressource. Si des autorisations sont estompées (inaccessibles), cela veut dire qu'elles ont été héritées d'un dossier parent. Cochez des cases dans la colonne Autoriser pour ajouter des autorisations, décochez-les pour supprimer des autorisations, puis cliquez sur OK.

❑ **Identités spéciales**

Les identités spéciales les plus utilisées sont Créateur propriétaire et Utilisateurs, les autres servent plus rarement. Les identités spéciales sont automatiquement membres de certains groupes. Pour configurer des autorisations pour une identité spéciale, saisissez le nom de l'identité spéciale comme vous le feriez pour le nom de n'importe quel autre utilisateur ou groupe.

Autorisations spéciales

Windows emploie depuis Vista des autorisations spéciales pour contrôler en détail les autorisations des utilisateurs et groupes. En coulisses, chaque fois que vous manipulez les autorisations de base, Windows gère un ensemble d'autorisations spéciales associées qui spécifient très exactement les actions permises.

Dans l'explorateur Windows, vous pouvez voir les autorisations spéciales d'un fichier ou dossier en cliquant dessus avec le bouton droit de la souris puis en appelant Propriétés. Dans la boîte de dialogue des propriétés, allez dans l'onglet Sécurité puis cliquez sur Avancé pour afficher la boîte de dialogue Paramètres de sécurité avancés. Cette boîte de dialogue affiche les autorisations de façon analogue à l'affichage de l'onglet Sécurité, si ce n'est qu'elles sont classées par type (Autoriser ou Refuser) avec leurs modalités d'héritage, plus les ressources concernées par les autorisations.

Pour modifier ces autorisations, dans la boîte de dialogue Paramètres de sécurité avancés, cliquez sur Modifier les autorisations. Vous voyez alors une version modifiable de l'onglet Autorisations dans laquelle vous pouvez spécifier des autorisations spéciales à l'aide des boutons Ajouter, Modifier et Supprimer.

❑ **Possession de fichier**

Le propriétaire par défaut d'un fichier ou dossier est la personne qui l'a créé. La propriété d'une ressource peut être acquise ou transférée de plusieurs façons. Le propriétaire d'un fichier ou dossier peut, à tout moment, transférer la propriété à un autre utilisateur ou groupe. Un membre du groupe Administrateurs peut, à tout moment, prendre possession d'un fichier ou dossier, ou bien en transférer la propriété à un autre utilisateur ou groupe, même si ce dernier n'a pas accès à la ressource d'après les autorisations. Tout utilisateur possédant l'autorisation Appropriation sur le

fichier ou dossier peut en prendre possession, ce qui est aussi le cas d'un membre du groupe Opérateurs de sauvegarde (ou d'ailleurs de toute personne ayant le droit utilisateur Restaurer les fichiers et les répertoires).

Héritage d'autorisations

Dans la hiérarchie des fichiers et dossiers employée par Windows, le dossier racine d'un disque local et le dossier `%UserProfile%` sont par défaut les dossiers parent de tous les fichiers et dossiers qu'ils contiennent. Toute ressource ajoutée hérite des autorisations de l'un ou l'autre de ces deux dossiers. Vous pouvez modifier ce comportement en ajustant les paramètres d'héritage d'un dossier de façon qu'il n'hérite plus des autorisations de son dossier parent. Cela a pour effet de créer un nouveau dossier parent ; les sous-dossiers ou fichiers que vous créez dedans héritent de ses autorisations.

L'héritage est automatique, et les autorisations héritées sont attribuées lors de la création d'un fichier ou dossier. Il est toutefois possible de faire en sorte qu'un fichier ou un dossier ne dispose pas des mêmes autorisations qu'un parent. Pour voir les autorisations héritées sur un fichier ou dossier, cliquez dessus avec le bouton droit de la souris dans l'explorateur Windows puis appelez Propriétés. Dans l'onglet Sécurité, cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres de sécurité avancés. La colonne Autorisation énumère les autorisations assignées actuellement à la ressource. Si l'autorisation est héritée, la colonne Héritée de indique le dossier parent d'où provient l'autorisation. Si d'autres ressources héritent à leurs tours de l'autorisation, la colonne Appliquer à indique les types de ressources qui hériteront de l'autorisation.

Autorisations effectives

Les autorisations NTFS sont complexes et parfois difficiles à gérer. Il arrive qu'une modification, même mineure, entraîne des conséquences imprévues. Les autorisations effectives disent exactement quelles sont les autorisations accordées effectivement à un certain utilisateur ou groupe : elles dépendent de toutes les autorisations accordées ou refusées, que ces autorisations aient été définies explicitement ou qu'elles aient été obtenues des groupes auxquels

appartient l'utilisateur. Pour afficher les autorisations effectives d'un utilisateur ou d'un groupe sur un fichier ou dossier, dans l'explorateur Windows, cliquez avec le bouton droit de la souris sur le fichier ou dossier puis appelez Propriétés. Dans l'onglet Sécurité de la boîte de dialogue des propriétés, cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres de sécurité avancés.

Pour voir les autorisations effectives appliquées à un utilisateur ou à un groupe, allez dans l'onglet Autorisations effectives, cliquez sur Sélectionner, tapez le nom de l'utilisateur ou du groupe, puis cliquez sur OK.

Contrôle des accès aux partages réseau

Quand un utilisateur accède à un fichier ou dossier *via* le réseau et que le partage de fichiers standard est activé, deux niveaux d'autorisations entrent en jeu ; c'est la combinaison de ces deux niveaux qui détermine les actions que peut faire l'utilisateur sur le fichier ou dossier. Le premier niveau d'autorisations est celui des autorisations définies sur le partage lui-même. Elles définissent le niveau maximal d'accès. Un utilisateur ou groupe ne peut jamais disposer de plus d'autorisations que celles accordées par le partage. Le second niveau d'autorisations concerne les autorisations définies sur les fichiers et dossiers. Ces autorisations servent à restreindre encore plus les actions permises.

Il existe trois autorisations de partage : Propriétaire/copropriétaire (disposant d'un contrôle total), Collaborateur (Lecture et Modifier) et Lecteur (autorisation Lecture uniquement).

Vous pouvez redéfinir ce comportement en interdisant spécifiquement une autorisation. Les autorisations refusées sont prioritaires par rapport aux autorisations accordées. Si vous ne voulez pas qu'un utilisateur ou groupe possède une autorisation, configurez les autorisations du partage de façon que l'utilisateur ou le groupe se voie refuser cette autorisation.

Diagnostique et dépannage des ressources partagées

Si l'accès aux ressources partagées ne fonctionne pas, la cause peut être parmi les suivantes :

- La connexion réseau entre les machines est incorrecte. Veuillez diagnostiquer le réseau. Les deux ordinateurs doivent être connectés au réseau et configurés avec les paramètres TCP/IP adéquats (dont le masque de sous réseau).
- Les utilisateurs n'appartiennent pas au même domaine. Dans ce cas, ou si l'utilisateur a ouvert une session sur son ordinateur comme utilisateur local plutôt que comme utilisateur du domaine, vous devez veiller à ce que l'utilisateur se connecte au partage avec des éléments d'identification alternatifs et que ces éléments d'identification alternatifs sont ceux d'un compte utilisateur adéquat du domaine pertinent.
- Un pare-feu (ou antivirus) sur l'ordinateur partageant la ressource, sur l'ordinateur accédant à la ressource ou sur le réseau empêche l'accès. L'exception de Pare-feu Windows Partage de fichiers et d'imprimantes doit être activée sur l'ordinateur qui partage des ressources. Le Pare-feu Windows prend en charge de nombreux profils actifs et le profil actif et applicable doit être configuré correctement. Si vous employez un pare-feu de tierce partie, les connexions entrantes doivent être autorisées sur les ports UDP 137 et 138, le port TCP 139 et tous les ports pour ICMPv4 et (si applicable pour les requêtes d'écho) ICMPv6.
- Le nombre d'utilisateurs maximal (qui dépend du système d'exploitation, de sa version et du paramétrage reconnu) est dépassé.
- Un caractère spécial (tel qu'un espace) dans le nom d'une ressource partagée peut empêcher l'accès pour des systèmes d'exploitation plus anciens.
- Les droits du système de fichiers NTFS peuvent interférer avec les droits du partage car les interdictions ont priorité sur les autorisations.
- Vérifiez les paramètres du partage avancé dans le Centre réseau et partage. Pour partager avec succès des fichiers sur un ordinateur de bureau qui exécute Windows Vista ou ultérieur, Partage de fichiers et d'imprimantes doit être

activé pour le profil réseau actif et la stratégie Empêcher les utilisateurs de partager des fichiers dans leur profil ne doit pas être activée. Un ordinateur peut être simultanément connecté à plusieurs réseaux et le type de réseau de chaque réseau actif doit être correctement configuré dans le Centre réseau et partage.

- Vérifiez le type de réseau du réseau actif. Dans le Centre réseau et partage, le type de réseau doit être configuré correctement sur les deux ordinateurs. Si le type de réseau est fixé à Public, de nombreux paramètres de partage et de connexion sont verrouillés et restreints.