

# Cours: Gestion des partages et des autorisations NTFS

Cours :

cours\_gestion\_des\_partages\_et\_des\_autorisations\_ntfs.odt

## La gestion des ressources partagées

**Définition** : le **partage** permet d'accéder à des ressources (dossiers, imprimantes) d'un serveur **par le réseau**.

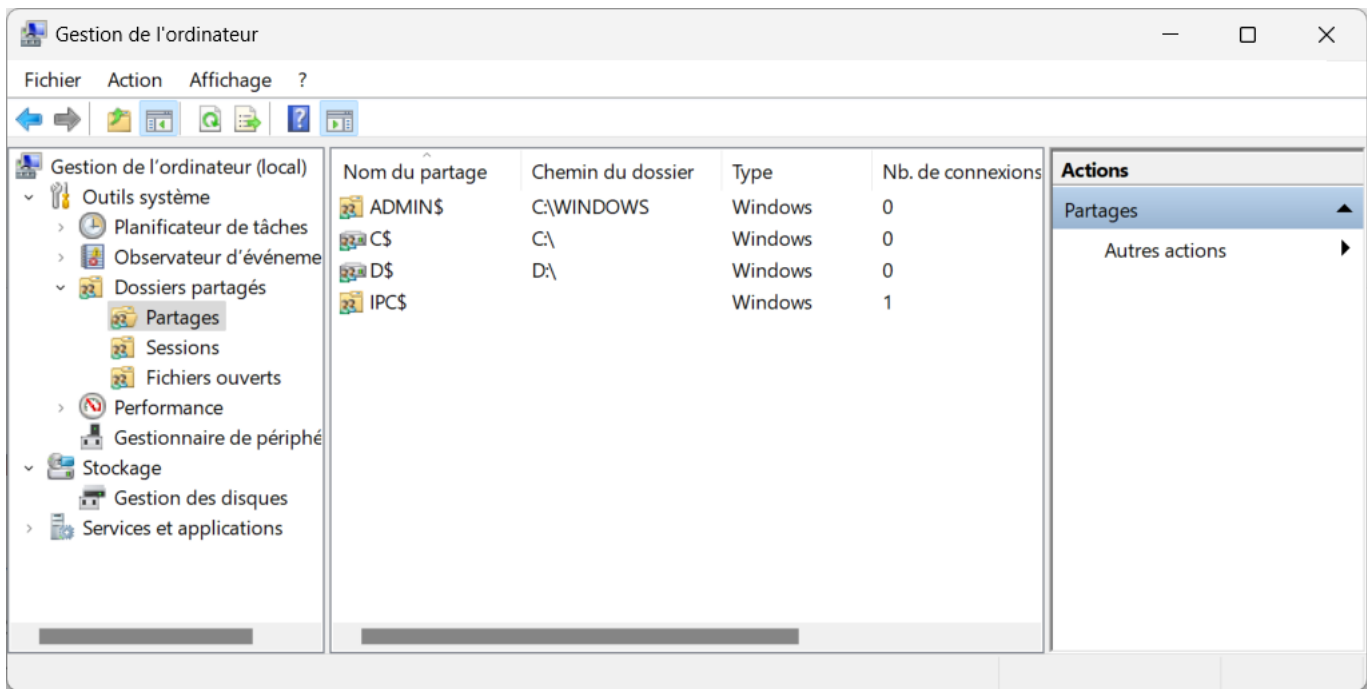
C'est le service Serveur qui permet le partage des ressources. Il utilise le protocole appelé **SMB** (Server Message Block) qui permet le partage des ressources (fichiers et imprimantes). Dans les dernières versions de Windows, il est appelé **CIFS**(Common Internet File System).

Le contrôle des accès se fait en attribuant des autorisations de partage à des comptes ou des groupes d'utilisateurs sur des dossiers partagés (et non aux fichiers).

Le contrôle des accès par les autorisation de partage n'est effectif que si les utilisateurs accèdent à la ressource par le réseau.

Il est possible de limiter le nombre d'utilisateurs connectés simultanément au dossier. Ce nombre est limité avec les stations de travail.

Il existe des **partages administratifs cachés** avec l'autorisation **Contrôle total** (CT) pour les **administrateurs** : C\$, D\$, ADMIN\$ (dossier système Windows), \$IPC (communication interprocesseur). Ces autorisations sont non modifiables.



### Les autres solutions d'accès à des dossiers réseaux

**Samba** est une mise en œuvre de SMB pour UNIX/LINUX Afin de permettre aux clients Windows d'accéder aux répertoires et fichiers UNIX en utilisant le protocole SMB. Les clients Windows ont l'impression qu'ils accèdent à un serveur Windows.

Le système **DFS** (Distributed File System) est une solution Microsoft qui facilite l'accès des ressources réseaux dispersées sur le réseau.

Le protocole **NFS** (Networked File System) permet de donner accès aux systèmes de fichiers présents sur le réseau comme s'ils étaient locaux.

### La création de dossiers partagés

les partages sont enregistrés dans la base de registre (HKLM, System, CurrentControlSet, Services, LanmanServer, Shares).

La création de partage est donc possible sur des partitions FAT et NTFS mais il faut avoir les droits nécessaires pour modifier la base de registre.

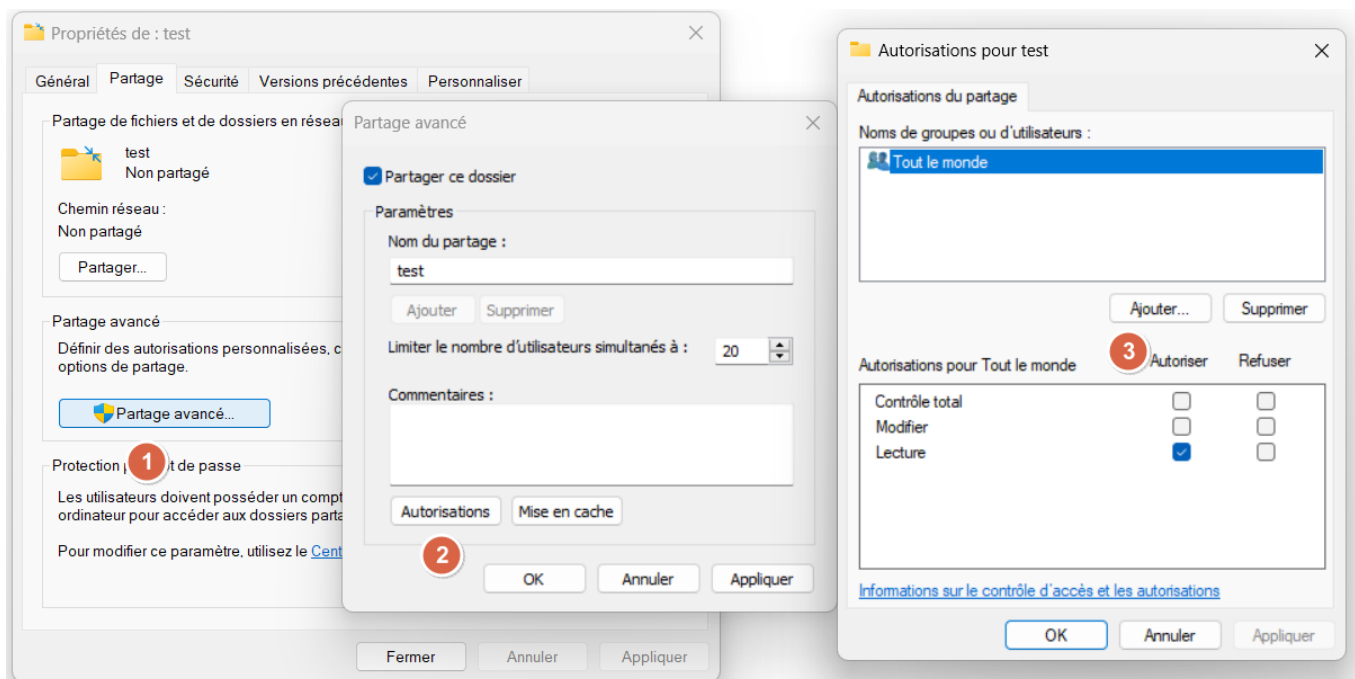
Pour pouvoir créer un partage :

- Il faut être membre d'un groupe ayant le droit de partager un dossier : **Administrateurs** et **Utilisateurs avec pouvoir**.
- donner un nom de partage **unique** sur le même serveur

Attention : l'autorisation par défaut définie lors d'un partage est Lecture pour le groupe Tout le monde.

Il y a plusieurs manières de créer un partage de dossier :

- utilisez l'**explorateur Windows**, accédez aux **propriétés** du dossier et définir le partage depuis l'**onglet Partage** ; utilisez le bouton **Partage avancé** pour définir précisément les autorisations d'accès.



- utilisez la console **Gestion de l'ordinateur** (limitation sur les clients Windows)
- les outils en **ligne de commande** en tant qu'administrateur (**cmd** - autorisation lecture par défaut ou **Powershell** en précisant les autorisations) :

```
net share nomenclature=unité:\dossier
```

```
New-SmbShare -Name nomenclature -Path unité:\dossier -FullAccess Userogroupe
```

Dans un réseau, la liste des ressources partagées est centralisée sur un ordinateur **Explorateur maître** du segment de réseau (après un processus d'élection).

Les partages peuvent être publiés dans **Active directory** (fonctionnement dans un domaine).

## Les autorisations de partage

- Lecture
- Modifier
- Contrôle total
- Refuser

Les autorisations sont **cumulatives** sauf l'**autorisation Refuser**.

S'il existe des autorisations NTFS, il y a combinaison des autorisations NTFS et de partage. La plus **restrictive** est effective.

Définissez les autorisations en utilisant de préférence les **groupes d'utilisateurs**.

## Connexion à des dossiers partagés

- par l'icône **Réseau**,
- **Connecter un lecteur réseau** avec l'explorateur ou clic droit sur **Réseau**, en lui attribuant une **lettre de lecteur**. Le nombre de connexions est limité par les lettres de l'alphabet.
- Commande **Exécuter** du menu démarrer sans définir de lettre de lecteur (nombre illimité de connexions possibles) en indiquant un nom UNC (Universal Naming Convention ). Exemple : `\\serveur\nomdepartage`
- En ligne de commande avec cmd ou Powershell

```
net use lettre_lecteur: \\nom_serveur\nom_partage
```

```
New-PSDrive -Name P -Root \\serveur\partage -PSProvider FileSystem -Persist -Credential nomdecompte
```

L'option « Se reconnecter à l'ouverture de session » crée une clé (base de registre) dans HKCU, Network

- par des scripts associés à des **GPO** au niveau du domaine

## Les autorisations NTFS

**NTFS** (New Technology File System ) est un système de fichiers supporté par les SE Windows et permet de :

- mettre des **autorisations d'accès** très spécifiques (**ACL**) sur les fichiers et les dossiers,
- **chiffrer** des fichiers avec EFS (Encrypting File System),
- **compresser** des fichiers,
- d'établir des **quotas** disque.

Une **ACL** (Access Control List) est une liste d'**Access Control Entry** (**ACE**) donnant ou supprimant des autorisations d'accès à un utilisateur ou un groupe.

Les autorisations sont vérifiées en **local** et par le **réseau**. L'autorisation par **défaut** est **Lecture** au groupe **Utilisateurs**.

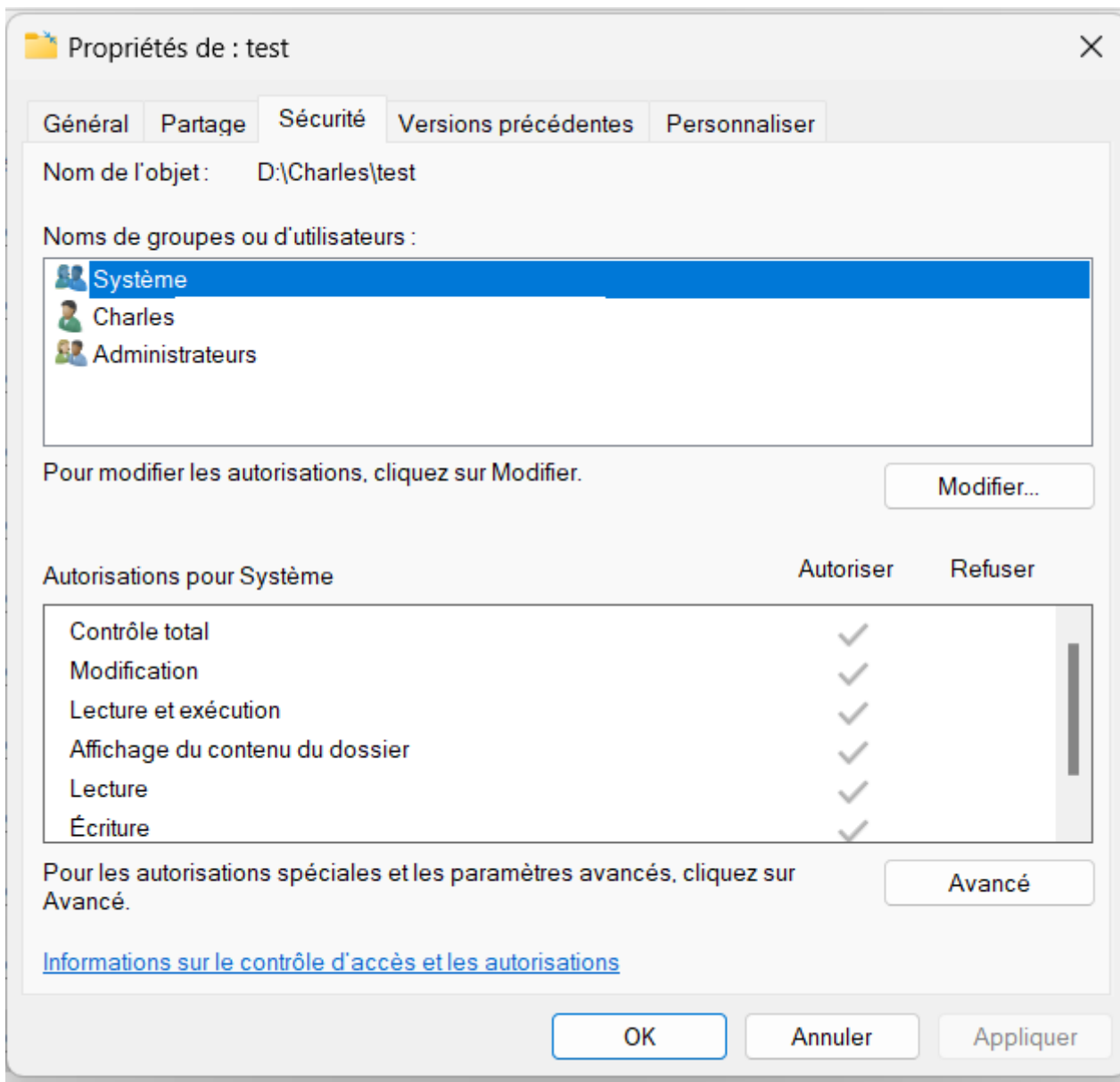
Il y a 6 autorisations standard :

- Lecture,
- Ecriture,
- Afficher le contenu du dossier;
- Lecture et exécution;
- Modifier;
- Contrôle total.

**Contrôle total** c'est :

- Modifier les autorisations
- et prendre possession d'un dossier en plus des autorisations précédentes.

Ce sont des autorisation spéciales



### Application des autorisations NTFS

- **héritage** des autorisations du parent,
- **cumul** des autorisations : la plus large l'emporte (combinaison),
- l'autorisation **Refuser** est **prioritaire** sur les autres. C'est à **éviter** car il suffit de ne rien mettre pour le groupe ou l'utilisateur.
- les autorisations sur les fichiers sont prioritaires par rapport aux autorisations sur les dossiers,
- **refuser** est prioritaire ( à éviter) ou bien ne rien mettre pour le groupe ou l'utilisateur

Il est nécessaire de **supprimez l'héritage** pour attribuer des autorisations différentes du dossier parent.

- Lors d'une **copie** de fichiers ou de dossiers, les autorisations sont celles du dossier de destination.
- Lors d'un **déplacement** dans la **même partition** il y a **conservation** des autorisations.
- Lors d'un **déplacement** dans une **partition différente** il y a **perte** des autorisations.

### Attribution des autorisations

Pour définir les autorisations, il faut être :

- administrateur,
- ou simple utilisateur disposant de l'autorisation **contrôle total**,
- ou **propriétaire** de la ressource.

## Quelques conseils sur l'utilisation des autorisation de partage et des autorisation NTFS

Regroupez les ressources dans des dossiers spécifiques :

- un dossier pour regrouper les dossiers personnels des utilisateurs (dossier de base),
- un dossier pour les applications,
- un dossier pour l'ensemble des dossiers communs à plusieurs utilisateurs (dossiers partagés)

Créez des partages uniquement sur ces dossiers spécifiques pour ne pas multiplier le nombre de partage.

Les autorisations NTFS permettent de gérer plus finement que les autorisations de partage l'accès aux ressources. Utilisez la démarche suivante :

- définissez un partage avec comme autorisation Contrôle total pour le groupe Tout le monde. Définissez ensuite très précisément les autorisations NTFS.
- Utilisez l'autorisation NTFS Lire et exécuter pour les dossiers d'application (évite les suppressions et les dégâts de certains virus).
- Utilisez l'autorisation NTFS Modifier pour des dossiers communs.
- Utilisez l'autorisation NTFS CT à chaque utilisateur pour son dossier personnel.
- Utilisez l'autorisation NTFS CT pour l'administrateur sur l'ensemble des dossiers (sauf les dossiers personnels).

Et bien sûr utilisez les groupes d'utilisateurs pour attribuer collectivement des autorisations.

Voici la démarche préconisée par Microsoft (dans un contexte de domaine unique, sans forêt) : **AGDLP**, qui signifie : Account, Global group, Domain Local group, Permission. On ne met pas d'autorisations d'accès directement sur les utilisateurs sauf si l'utilisateur est vraiment unique (dossier personnel / répertoire de base).

### Retour Bloc 2

- [Cours Bloc 2](#)

From:

/ - Les cours du BTS SIO

Permanent link:

</doku.php/si2/partage-ntfs?rev=1727074492>

Last update: 2024/09/23 08:54

