

# Serveurs de fichiers

420-2S5-EM

Serveur 1 – Services intranet

# Les différents protocoles de partage

## FTP – File Transfer Protocol

- Créé en 1971 au Massachusetts Institute of Technology
- Protocole non-chiffré. (sFTP viendra pallier ça plus tard)
- Utilisé à travers internet, quoique de moins en moins populaire

## SMB – Server Message Block

- Aussi appelé CIFS (Common Internet File System)
- Souvent confondu avec Samba, une suite de logiciels d'interopérabilité sous Linux
- Protocole le plus répandu sous Windows et à travers les réseaux locaux

## NFS – Network File System

- Créé en 1984 par Sun Microsystems
- Surtout utilisé dans les environnements UNIX
- Tout de même utilisable avec Windows

# FTP – File Transfer Protocol

- Objectif principal: Le transfert de fichier
- Populaire dans les environnements web
- 2 modes : Actif & Passif
- Utilise 2 ports pour communiquer: 20 & 21
- Peu sécuritaire (il existe FTPS et SFTP maintenant)

# FTP - Mode Actif

- **Étape 1:** Le client se connecte au port 21 du serveur à partir d'un port aléatoire (socket) et communique son port pour le transfert de données.
- **Étape 2:** Le serveur communique un accusé de réception au port de commandes du client.
- **Étape 3:** Le serveur établit une connexion entre son port de données et le port de données du client.
- **Étape 4:** Le client envoie un accusé de réception au serveur

# FTP - Mode Passif

- **Étape 1:** Le client se connecte au port 21 du serveur à partir d'un port aléatoire (socket) et demande au serveur d'ouvrir un port de communication au hasard.
- **Étape 2:** Le serveur communique un accusé de réception au port de commande du client et lui transmet le numéro de port qu'il a ouvert.
- **Étape 3:** Le client établit une connexion entre son port de données et le port de données du client.
- **Étape 4:** Le serveur envoie un accusé de réception au client et l'échange démarre.

# Quel mode privilégier ?

- Généralement nous allons privilégier le mode passif dû à au « NAT » régulièrement présent chez les clients.
- En effet, dans le mode actif, comme c'est le serveur qui initie l'échange sur le canal de données, il faudra autoriser les connexions entrantes pour que l'on puisse joindre le client FTP.
- En contrepartie, en mode passif, c'est le client qui initie l'échange, ce qui cause moins d'ennuie car les serveurs attendent généralement des connexions entrantes.

# Sécurité du protocole FTP

- Le protocole FTP original est aujourd'hui considéré comme **non sécuritaire** pour plusieurs raisons:
- Les **données transmises sont non chiffrées**. Cela rend le protocole vulnérable aux interceptions et peut compromettre la confidentialité des informations.
- **L'authentification est également effectuée en texte clair.**
- **Aucun mécanisme de sécurité intégrés** tels que le chiffrement de bout en bout ou la vérification de l'intégrité des fichiers.

# Qu'est-ce que SMB ?

- C'est un protocole de type client/serveur.
- SMB est rétro compatible avec ses différentes versions\*
- Pour bien distinguer SMB, CIFS et Samba:
  - SMB est le protocole original
  - Historiquement, CIFS se voulait une extension (amélioration) du protocole original. Avec le temps, les deux termes se sont confondus.
  - Samba, quant à lui, est une implémentation libre et open source du protocole SMB/CIFS. En d'autres mots, c'est un ensemble logiciel permettant l'interopérabilité du protocole SMB avec les ordinateurs sous Microsoft.



# Rétrocompatibilité SMB

La négociation du protocole se fait automatiquement entre les machines:

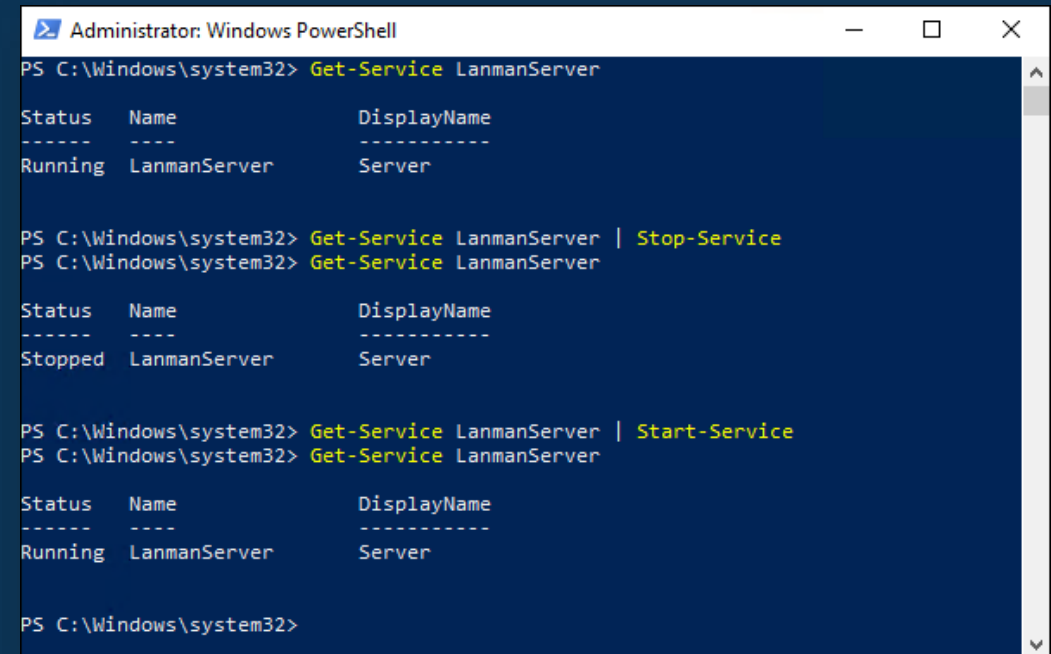
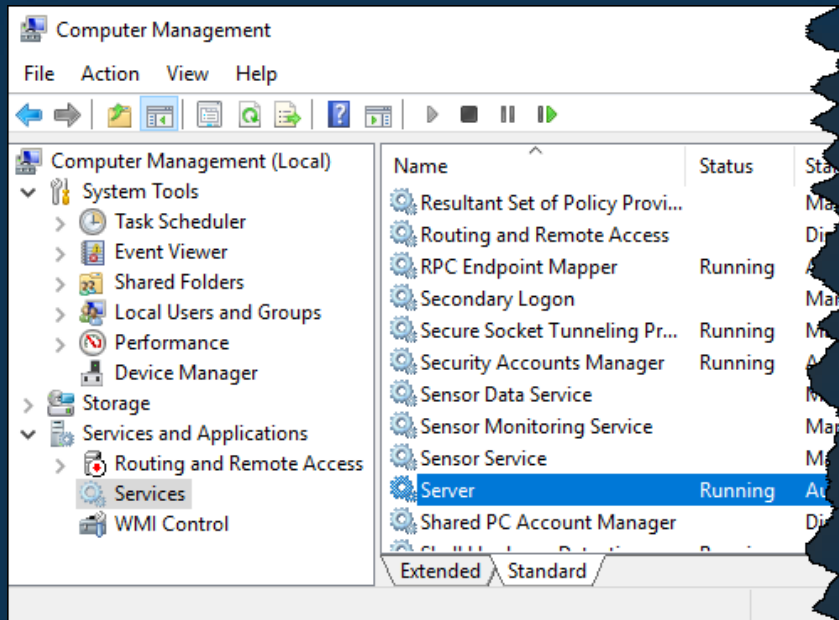
| OS                             | Win10/11<br>WS 2016/2019/2022 | Win 8.1<br>WS 2012 R2 | Win 8<br>WS 2012 | Win 7<br>WS 2008 R2 | Win Vista<br>WS 2008 | Win XP /2000<br>WS 2003 |
|--------------------------------|-------------------------------|-----------------------|------------------|---------------------|----------------------|-------------------------|
| Win 10/11<br>WS 2016/2019/2022 | SMB 3.1.1                     | SMB 3.0.2             | SMB 3.0          | SMB 2.1             | SMB 2.0.2            | SMB 1.0                 |
| Win 8.1<br>WS 2012 R2          | SMB 3.0.2                     | SMB 3.0.2             | SMB 3.0          | SMB 2.1             | SMB 2.0.2            | SMB 1.0                 |
| Win 8<br>WS 2012               | SMB 3.0                       | SMB 3.0               | SMB 3.0          | SMB 2.1             | SMB 2.0.2            | SMB 1.0                 |
| Win 7<br>WS 2008 R2            | SMB 2.1                       | SMB 2.1               | SMB 2.1          | SMB 2.1             | SMB 2.0.2            | SMB 1.0                 |
| Win Vista<br>WS 2008           | SMB 2.0.2                     | SMB 2.0.2             | SMB 2.0.2        | SMB 2.0.2           | SMB 2.0.2            | SMB 1.0                 |
| Win 2000 / XP<br>WS 2003       | SMB 1.0                       | SMB 1.0               | SMB 1.0          | SMB 1.0             | SMB 1.0              | SMB 1.0                 |

# SMB v1 et la faille de sécurité « EternalBlue »

- La version 1 du protocole SMB a été au cœur de l'exploitation d'une faille de sécurité majeure chez Microsoft. L'exploitation de cette faille a été baptisée (Eternal Blue). Son numéro de vulnérabilité officiel est le [CVE-2017-0144](#).
- Depuis que cette faille de sécurité a été découverte, celle-ci a été « patchée » à travers les différentes mises à jour de Windows. Cela dit, Microsoft ne s'est pas arrêté là et l'entreprise a désactivé la version 1 du protocole SMB par défaut dans toutes les versions Windows depuis Windows 10 (1709) et Windows Server (1709).

# Service de partage de fichiers Windows

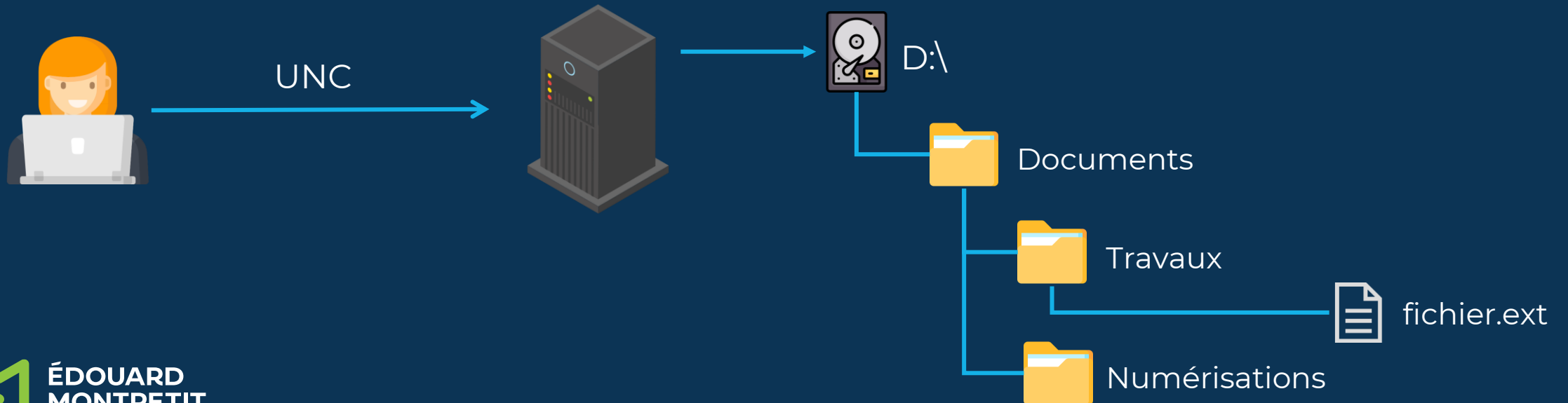
Le service du serveur de fichiers de Windows se nomme **Lanmanserver** (ou Server, tel qu'affiché dans le gestionnaire de services).



# Chemins UNC

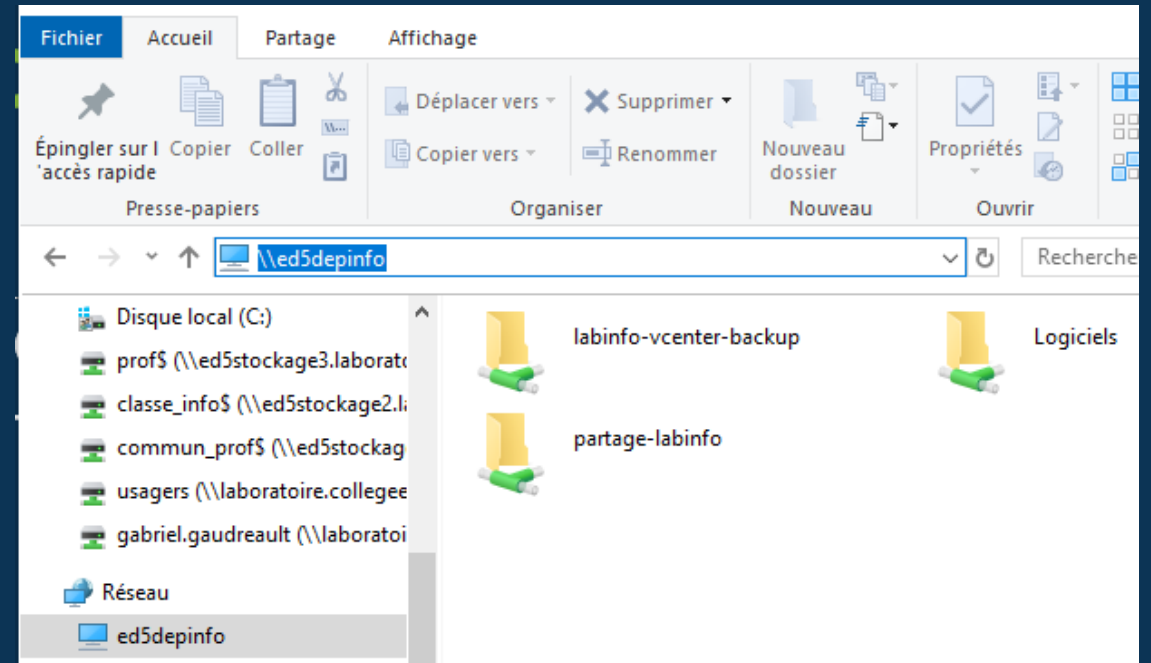
Pour accéder à un partage SMB sous Windows, il faut utiliser un chemin **UNC** (Universal Naming Convention).

**\\SERVEUR\Partage\**fichier.ext



# Partages dans l'explorateur

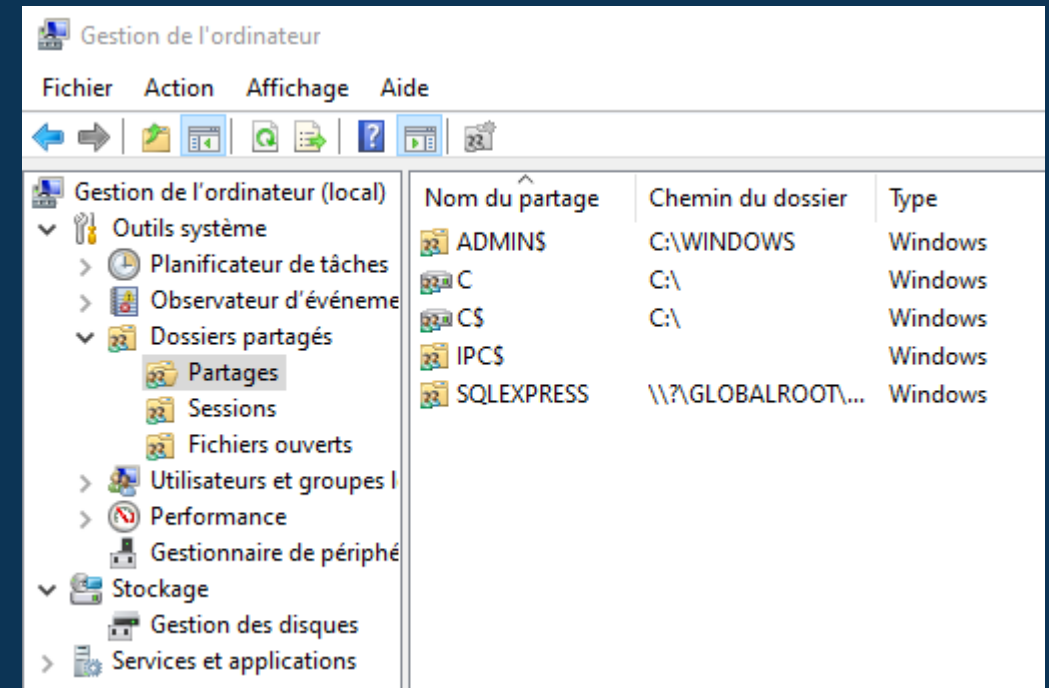
- En inscrivant seulement le nom du serveur sous forme de chemin UNC, vous pourrez consulter les **partages disponibles**.
- Les noms de partage se terminant par « \$ » sont **invisibles**. Il faut donc connaître leur nom pour accéder à leur contenu.



# Console des partages sous Windows




Sous Windows, vous pouvez gérer vos partages depuis la console des partages. Celle-ci est disponible dans la console de gestion de l'ordinateur ou entrant la commande « `fsmgmt.msc` ».

Il est possible de créer, de modifier et d'arrêter des partages directement dans la console.



# Partages administratifs

Par défaut, Windows crée des partages à des fins administratives lors de l'installation. Ces partages permettent d'accéder au système à travers le réseau, à condition d'être un administrateur.

| Partages   | Explications   |
|--|--|
|  <b>ADMIN\$</b> <b>C:\WINDOWS</b> | Point d'entrée vers le répertoire système de Windows (C:\Windows\) |
|  <b>CS\$</b> <b>C:\</b>          | Point d'entrée vers la racine de chaque volume (C, D, etc...)      |
|  <b>IPC\$</b>                   | Partage spécial pour gérer certaines connexions temporaires.       |

# Permissions du partage et permissions NTFS

Il y a deux types de permissions à gérer pour accéder à un élément partagé:

1. Les permissions du partage
2. Les permissions du système de fichier (local)

Un utilisateur doit être autorisé dans les deux types de permission pour accéder à l'élément:



Utilisateur



Permissions  
sur le partage



Permissions  
locales (NTFS)



Ressource



# Permissions de partage

- Vérification à l'entrée du réseau.
- Une seule permission pour tout le contenu du partage.
- Ne sont valides que lorsqu'on passe par un partage.
- Devraient être similaires et représentatives des permissions locales.

Autorisations pour MonPartage

Autorisations du partage

Noms de groupes ou d'utilisateurs :

- Julien Poulin (j.poulin@ad.ggaudreault.cemti.ca)
- Techniciens (ad\Techniciens)

Ajouter... Supprimer

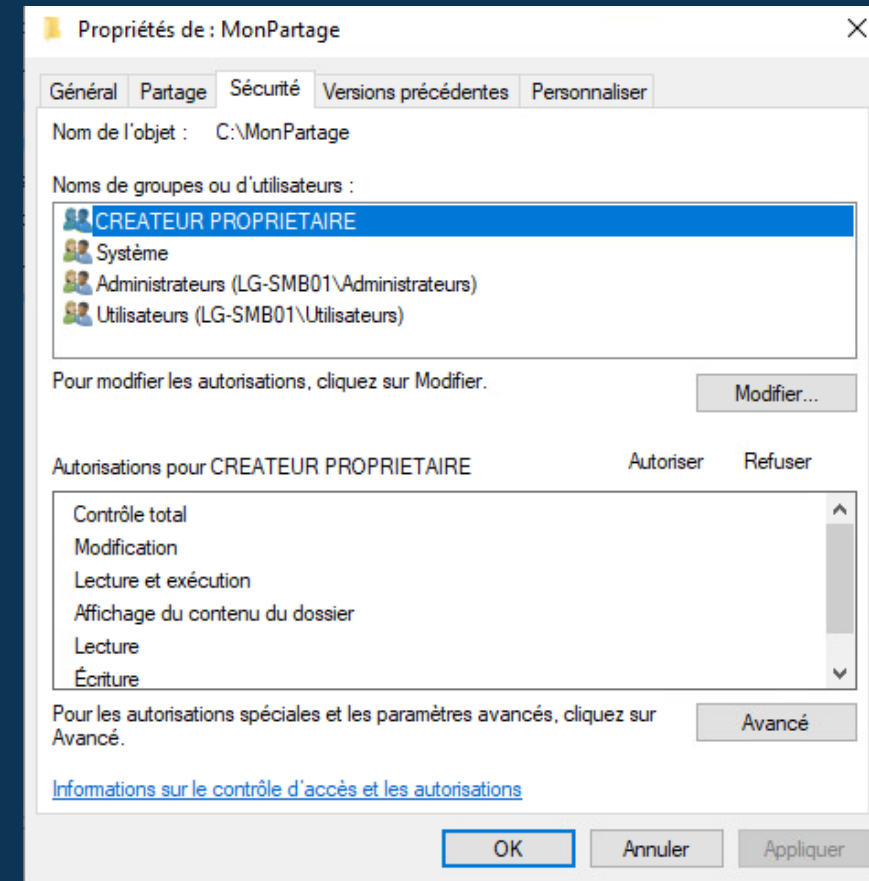
| Autorisations pour Techniciens | Autoriser                           | Refuser                  |
|--------------------------------|-------------------------------------|--------------------------|
| Contrôle total                 | <input type="checkbox"/>            | <input type="checkbox"/> |
| Modifier                       | <input type="checkbox"/>            | <input type="checkbox"/> |
| Lecture                        | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

[Informations sur le contrôle d'accès et les autorisations](#)

OK Annuler Appliquer

# Permissions locales (NTFS)

- Vérification à l'accès à l'élément.
- Permissions spécifiques pour chaque fichier et/ou répertoire.
- Elles sont valides en tout temps, à distance ou localement.
- Devraient représenter le droit d'accès au fichier, peu importe s'il est local ou distant.



# Permissions effectives

Lorsqu'un utilisateur accède à un fichier ou un répertoire partagé, sa permission effective (ou finale) est la plus restrictive des deux:

Exemples:

| Utilisateur   | Permissions de partage | Permissions locales | Permissions effectives |
|---------------|------------------------|---------------------|------------------------|
| Paul Meilleur | Contrôle total         | Lecture             | Lecture                |
| Rémi Fasol    | Lecture                | Modification        | Lecture                |
| Justin Ptipeu | Contrôle total         | Contrôle total      | Contrôle total         |

## Attention :

Des permissions sont souvent attribuées au groupe « Utilisateurs » ou au groupe « Utilisateurs authentifiés ». Ceux-ci comprennent tous les utilisateurs du système ainsi que tous les utilisateurs du domaine.

# Regroupements de permissions

Sous Windows, les permissions avancées (plus granulaires), sont regroupées en ensemble de permissions. Par exemple, l'ensemble « Contrôle total » contient toutes les permissions avancées. Voici un tableau dans lequel vous pourrez constater quel ensemble contient quelles permissions:

| Permissions avancées                 | Contrôle total | Modification | Lecture et Exécution | Affichage du contenu du dossier | Lecture | Écriture |
|--------------------------------------|----------------|--------------|----------------------|---------------------------------|---------|----------|
| Traverser dossier/Exécuter fichier   | x              | x            | x                    | x                               |         |          |
| Lister dossier/Lire les données      | x              | x            | x                    | x                               | x       |          |
| Lire les attributs                   | x              | x            | x                    | x                               | x       |          |
| Lire les attributs étendus           | x              | x            | x                    | x                               | x       |          |
| Créer fichiers/Écrire données        | x              | x            |                      |                                 |         | x        |
| Créer dossiers/Ajouter données       | x              | x            |                      |                                 |         | x        |
| Écrire les attributs                 | x              | x            |                      |                                 |         | x        |
| Écrire les attributs étendus         | x              | x            |                      |                                 |         | x        |
| Effacer sous-répertoires et fichiers | x              |              |                      |                                 |         |          |
| Effacer                              | x              | x            |                      |                                 |         |          |
| Lire les permissions                 | x              | x            | x                    | x                               | x       | x        |
| Changer les permissions              | x              |              |                      |                                 |         |          |
| S'approprier l'objet                 | x              |              |                      |                                 |         |          |
| Synchroniser                         | x              | x            | x                    | x                               | x       | x        |

Source: <https://mapage.clg.qc.ca/profdinfo/web/420-KA9-LC/permissions.html>