

Introduction aux droits d'accès Windows

Les droits d'accès dans Windows sont un élément fondamental de la sécurité informatique, permettant de contrôler qui peut accéder à quelles ressources et avec quels privilèges.

Pourquoi gérer les droits d'accès ?

- 🛡️ **Sécurité** : Protection des données sensibles
- 👥 **Confidentialité** : Accès limité aux utilisateurs autorisés
- ✅ **Intégrité** : Prévention des modifications non autorisées
- 🏗️ **Organisation** : Structure claire des accès

Dans cette présentation, nous explorerons les différents types de droits dans Windows, leur configuration et leur application dans un environnement professionnel.



La gestion des droits est essentielle pour la sécurité des systèmes d'information

Principes généraux des droits d'accès

Utilisateurs

Entités individuelles qui se connectent au système Windows. Chaque utilisateur possède un identifiant unique et des droits spécifiques.

Groupes

Collections d'utilisateurs partageant les mêmes droits d'accès. Facilite la gestion des permissions à grande échelle.

Exemples : Administrateurs, Utilisateurs, Invités

Héritage des permissions

Les sous-dossiers héritent automatiquement des permissions du dossier parent, sauf configuration contraire.

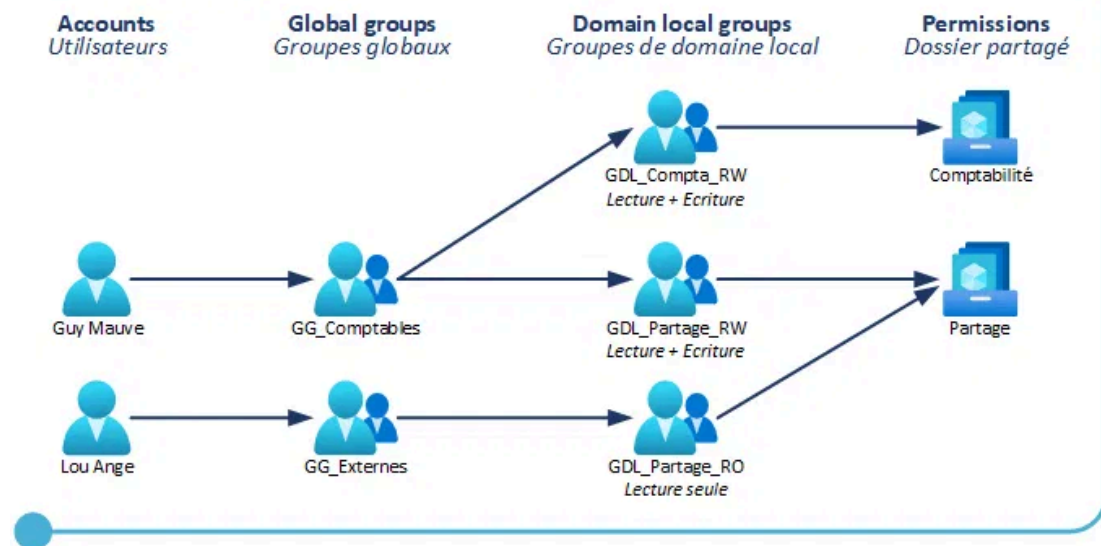
Permet une gestion cohérente et simplifiée des droits dans une arborescence.

Méthode AGDLP

Méthode recommandée par Microsoft pour la gestion des droits :

Accounts (comptes) → Global Groups → Domain Local groups → Permissions

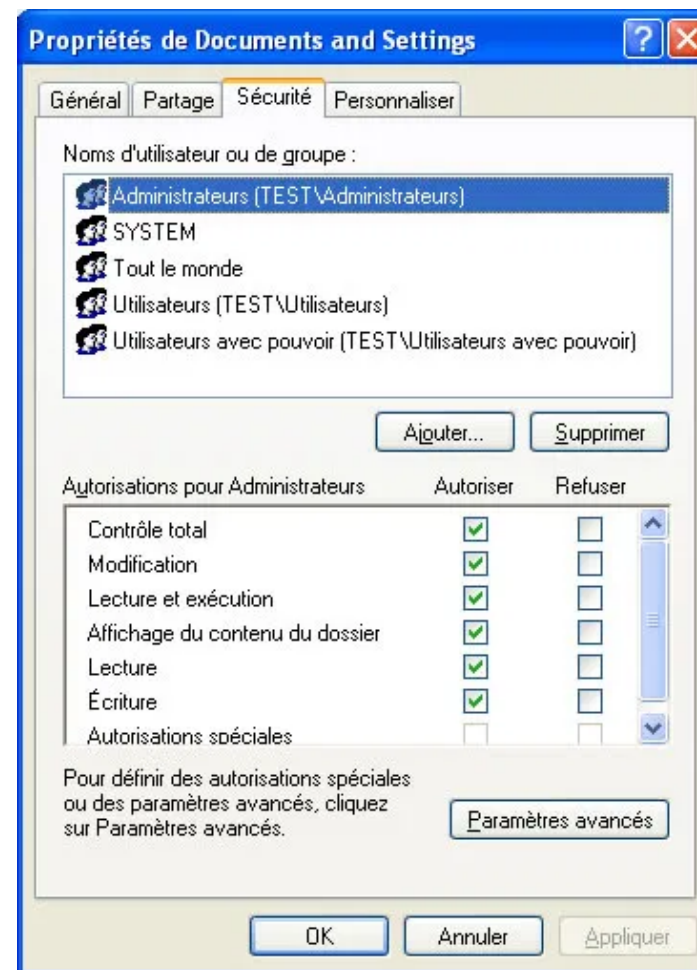
Méthode AGDLP



Les droits NTFS

NTFS (New Technology File System) est le système de fichiers standard de Windows qui permet une gestion fine des permissions au niveau du système de fichiers local.

Permission	Description
Lecture	Permet de voir le contenu des fichiers et dossiers, et d'afficher leurs attributs
Écriture	Permet de créer de nouveaux fichiers et dossiers, et de modifier le contenu existant
Exécution	Permet d'exécuter des programmes ou d'accéder au contenu des dossiers
Modification	Combine les droits de lecture, écriture et exécution, plus la suppression
Suppression	Permet de supprimer des fichiers ou dossiers
Contrôle total	Accorde tous les droits précédents, plus la possibilité de modifier les permissions



Interface de gestion des permissions

Windows offre une interface graphique intuitive pour configurer les permissions sur les fichiers et dossiers.

1 Accéder aux propriétés

Clic droit sur un fichier/dossier → Propriétés → onglet Sécurité

2 Gérer les utilisateurs et groupes

Ajouter ou supprimer des utilisateurs/groupes via le bouton "Modifier"

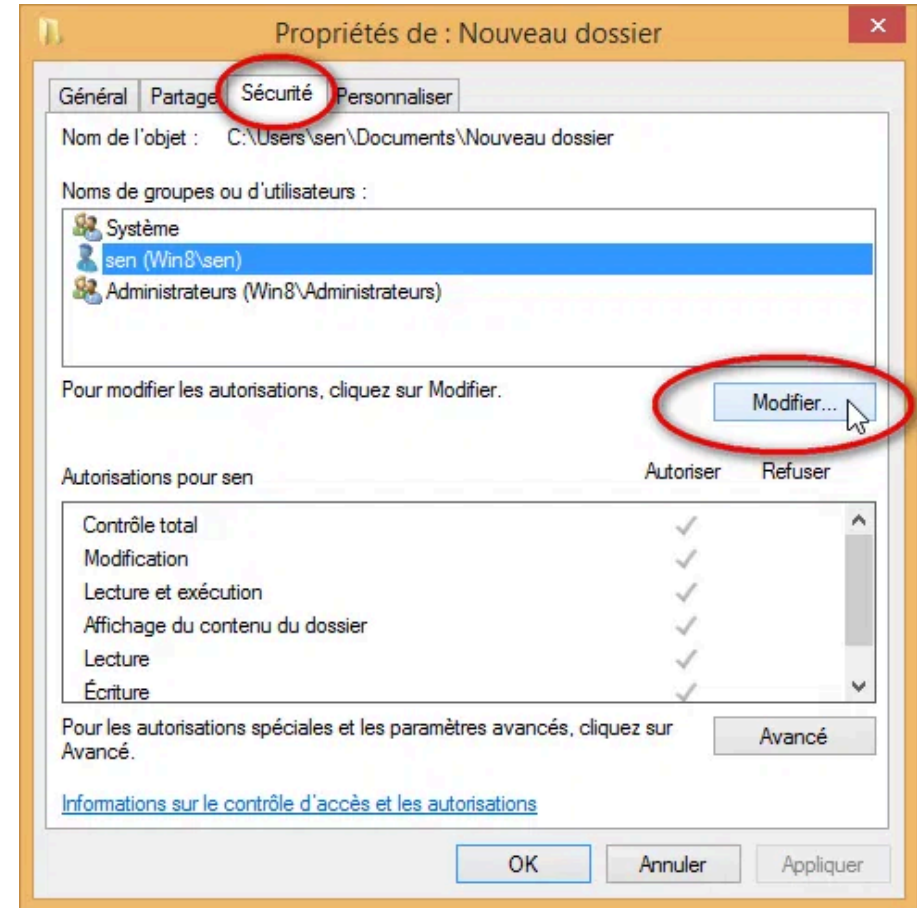
3 Configurer les permissions

Cocher ou décocher les cases correspondant aux permissions souhaitées

4 Paramètres avancés

Accéder aux options avancées pour une gestion plus fine (héritage, autorisations spéciales)

💡 Astuce : Pour appliquer des modifications à tous les sous-dossiers et fichiers, utilisez l'option "Remplacer toutes les entrées d'autorisation des objets enfants" dans les paramètres avancés.



Interface de configuration des permissions NTFS dans Windows

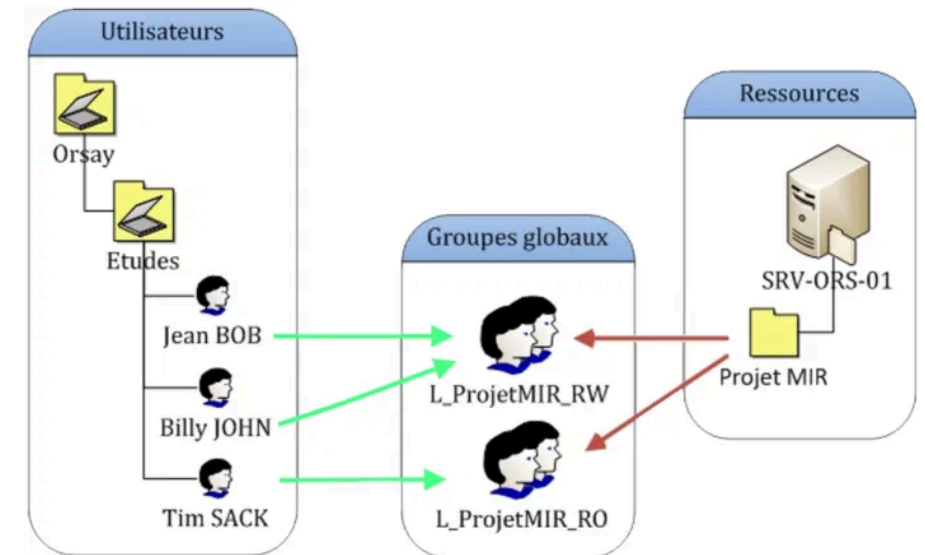
Les droits de partage réseau

Les droits de partage réseau contrôlent l'accès aux ressources partagées sur le réseau, indépendamment des permissions NTFS qui s'appliquent localement.

Niveau de partage	Description
Lecture	Permet de voir les fichiers et dossiers, et d'ouvrir les fichiers en lecture seule
Modification	Permet de voir, ajouter, modifier et supprimer des fichiers et dossiers
Contrôle total	Accorde tous les droits précédents, plus la possibilité de modifier les permissions

Points importants :

- Les droits de partage s'appliquent uniquement lors de l'accès via le réseau
- Les permissions effectives sont l'intersection des droits de partage et des droits NTFS
- Le droit le plus restrictif entre NTFS et partage est toujours appliqué



Interface de configuration des droits de partage réseau dans Windows

Exemple concret : dossier partagé en entreprise

Scénario :

Une entreprise souhaite mettre en place un dossier partagé "Projets" sur le serveur de fichiers avec des droits d'accès différenciés selon les groupes d'utilisateurs.

Groupe	Droits NTFS	Droits de partage
Administrateurs	Contrôle total	Contrôle total
Utilisateurs	Lecture, Écriture, Modification	Modification
Invités	Lecture seule	Lecture

Résultat :

- Les **Administrateurs** peuvent gérer entièrement le dossier et ses permissions
- Les **Utilisateurs** peuvent lire, créer et modifier des fichiers, mais pas changer les permissions
- Les **Invités** peuvent uniquement consulter les fichiers sans les modifier

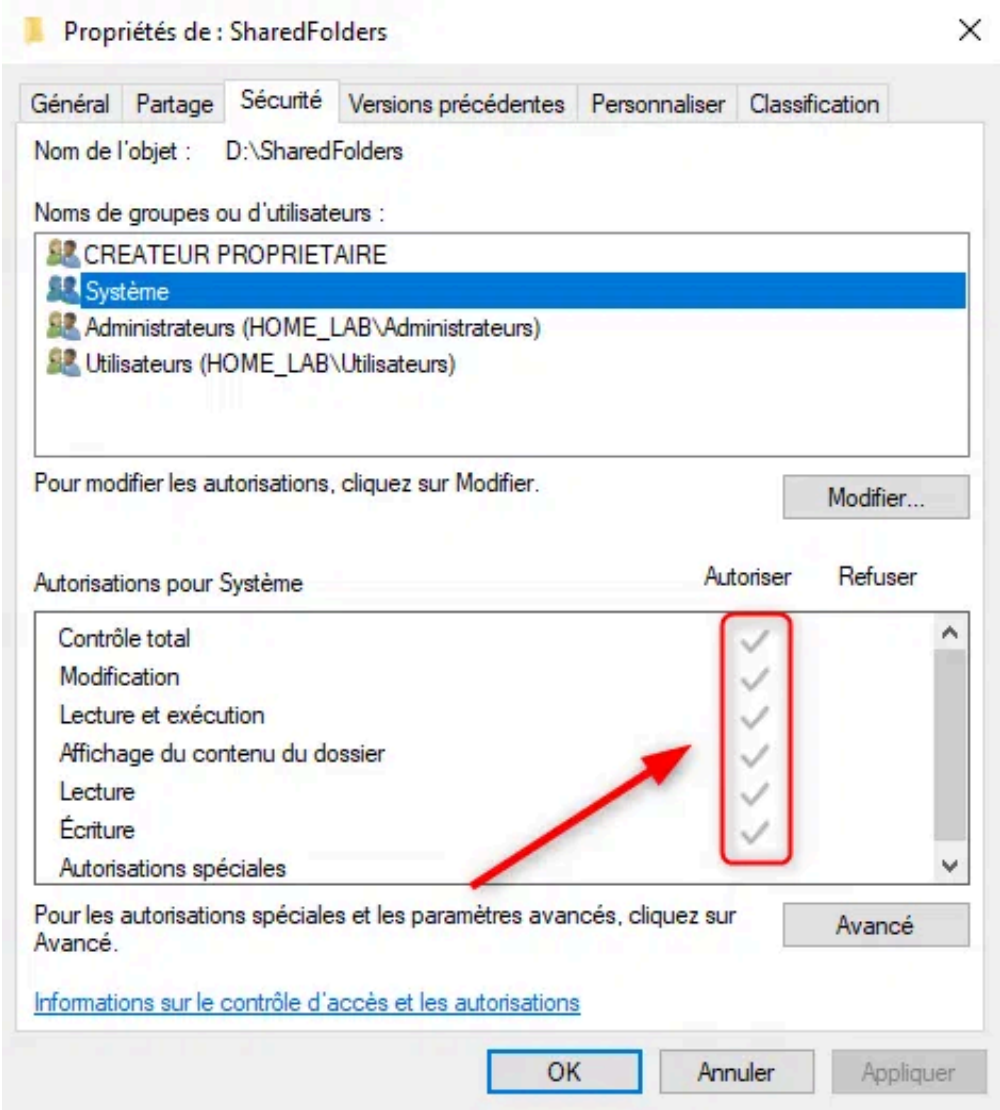


Schéma d'organisation des droits d'accès par groupe d'utilisateurs

Tableau récapitulatif des droits

Ce tableau récapitule les principaux droits d'accès dans Windows et leur signification pour les fichiers et dossiers.

Droit	Description	Fichier	Dossier	Héritable
Lecture	Afficher le contenu et les attributs	Lire le fichier	Lister le contenu	✓
Écriture	Modifier le contenu	Modifier le fichier	Créer des fichiers/dossiers	✓
Exécution	Exécuter ou traverser	Exécuter le programme	Accéder au contenu	✓
Modification	Lecture + Écriture + Exécution + Suppression	Modifier et supprimer	Modifier le contenu et la structure	✓
Contrôle total	Tous les droits précédents + gestion des permissions	Contrôle complet	Contrôle complet	✓
Autorisations spéciales	Droits granulaires spécifiques	Selon configuration	Selon configuration	Variable

Les droits effectifs sont toujours le résultat de la combinaison des droits explicites, des droits hérités et des droits de groupe.

Comparaison : droits NTFS vs droits de partage

Caractéristique	Droits NTFS	Droits de partage
Application	Localement et via le réseau	Uniquement via le réseau
Granularité	Fine (6 droits de base + autorisations spéciales)	Limitée (3 niveaux : Lecture, Modification, Contrôle total)
Persistance	Stockée avec le fichier/dossier	Stockée dans la configuration du partage
Héritage	Configurable et propageable	Non applicable
Priorité	Le plus restrictif s'applique	Le plus restrictif s'applique

Conclusion :

Pour une sécurité optimale, il est recommandé de configurer à la fois les droits NTFS et les droits de partage. Les droits NTFS offrent une protection plus fine et s'appliquent dans tous les contextes d'accès.

 Comparaison entre droits NTFS et droits de partage

Interaction entre les droits NTFS et les droits de partage