TIP 0.8 - Comptes utilisateurs, groupes et droits

Fiche de révision - Fondamentaux TIP

Niveau : Débutant **Durée :** 45-60 min **Module :** Fondamentaux TIP

1. Comptes utilisateurs

Un compte utilisateur permet à Windows d'identifier la personne qui ouvre une session et de lui associer un profil, des paramètres, des fichiers personnels et des droits.

À retenir

Authentification = « Qui es-tu ? » | **Autorisation** = « Qu'as-tu le droit de faire ? »

2. Standard, administrateur et UAC

Élément	Rôle
Compte standard	Utilisation normale du poste avec privilèges limités.
Compte administrateur	Permet des modifications système et des opérations nécessitant des privilèges élevés.
UAC	Contrôle l'élévation de privilèges lorsqu'une action sensible est demandée.
Moindre privilège	N'accorder que les droits strictement nécessaires.

3. Groupes locaux

Les groupes permettent de gérer les droits plus simplement : **Utilisateur** → **Groupe** → **Droits**. On rencontre notamment les groupes **Utilisateurs**, **Administrateurs** et **Utilisateurs du Bureau à distance**.

Sur les éditions Windows compatibles, **lusrmgr.msc** permet de consulter les utilisateurs et groupes locaux.

Réflexe technicien

Privilégier les droits attribués à des groupes plutôt qu'à chaque utilisateur individuellement.

Autorisations NTFS et héritage

4. Principales autorisations

Autorisation	Ce qu'elle permet
Lecture	Consulter les fichiers et dossiers.
Écriture	Créer ou modifier certaines données.
Lecture et exécution	Lire et exécuter les fichiers autorisés.
Modification	Lire, créer, modifier, renommer et généralement supprimer.
Contrôle total	Ajoute notamment la gestion des autorisations.

Point important

Modification permet généralement de supprimer et renommer les fichiers et dossiers concernés.

5. Héritage et droits effectifs

Les autorisations d'un dossier parent peuvent être transmises à ses sous-dossiers et fichiers : c'est **l'héritage**. Les droits réellement obtenus par l'utilisateur sont appelés **droits effectifs**.

Ils résultent notamment des autorisations directes, des groupes, de l'héritage et des éventuels refus explicites.

L'autorisation **Refuser** doit être utilisée avec prudence car elle peut bloquer un accès accordé par ailleurs.

6. Vérifier les droits d'un dossier

Dans l'Explorateur : **clic droit** → **Propriétés** → **Sécurité**. Le bouton **Avancé** permet notamment de consulter le propriétaire, les entrées d'autorisation et l'origine des droits.

Réflexe technicien

Ne pas résoudre un « Accès refusé » en donnant systématiquement **Contrôle total**. Identifier le droit minimal nécessaire.

7. Commandes utiles

Commande	Utilité
whoami	Affiche le compte actuellement utilisé.
whoami /groups	Affiche les groupes du compte connecté.
net user	Liste les comptes locaux.
net user utilisateur	Affiche des informations sur un compte précis.
lusrmgr.msc	Ouvre la gestion des utilisateurs et groupes locaux.

Diagnostic, pratique et mémo

8. Méthode de diagnostic d'un problème d'accès

Séquence à retenir

Identifier l'utilisateur → vérifier ses groupes → analyser les autorisations → contrôler l'héritage → appliquer le droit minimal nécessaire → tester

9. Cas pratique

Un utilisateur peut lire les fichiers du dossier **D:\Partages\Projets** mais ne peut ni créer, ni modifier, ni supprimer. Le groupe **Utilisateurs** possède Lecture, tandis que **GG_Projets** possède Modification.

Si l'utilisateur doit travailler dans ce dossier, la correction cohérente consiste à l'ajouter au groupe **GG_Projets**, plutôt que de lui attribuer directement Contrôle total.

Point examen

Face à un problème d'accès : **identifier → groupes → autorisations → héritage → droit minimal → test**. Ne pas rendre l'utilisateur administrateur ou lui donner Contrôle total sans besoin réel.

10. À retenir

- **Authentification** : vérifie l'identité.
- **Autorisation** : détermine ce que l'utilisateur peut faire.
- **Compte standard** : usage courant avec privilèges limités.
- **Administrateur** : privilèges élevés pour certaines opérations système.
- **UAC** : contrôle l'élévation de privilèges.
- **Groupe** : permet d'attribuer des droits communs à plusieurs utilisateurs.
- **Modification** : permet généralement de créer, modifier, renommer et supprimer.
- **Contrôle total** : ajoute notamment la gestion des autorisations.
- **Héritage** : transmet certaines permissions depuis le dossier parent.
- **Droits effectifs** : droits réellement obtenus après combinaison des permissions.
- **whoami /groups** : affiche les groupes du compte connecté.
- **Principe clé** : appliquer le moindre privilège.

Réflexe final

Pour gérer les accès proprement, utiliser les groupes, comprendre l'héritage et attribuer uniquement les droits nécessaires.