Gestion des utilisateurs et stratégies de sécurité sous Windows 10 Et Active Directory

Introduction

La gestion des utilisateurs est une fonction fondamentale d'un système d'exploitation.
Elle permet :

- de **séparer les environnements de travail** pour chaque personne utilisant la machine ;
- de **protéger les données** en attribuant des droits distincts ;
- de **renforcer la sécurité** en contrôlant qui peut accéder au système et comment.

Sous Windows 10, la gestion des utilisateurs peut se faire à deux niveaux :

1. **Localement** sur une machine (comptes propres à ce poste).
2. **Centralisée** via **Active Directory** en entreprise (comptes gérés par un serveur).

Ce cours présente successivement la gestion locale, l'administration en ligne de commande, les stratégies locales de sécurité, puis Active Directory.

I. Gestion des comptes utilisateurs (locale)

1. Création de comptes

Sous Windows 10, on distingue deux grands types de comptes :

- **Comptes standard** : limités aux tâches courantes (navigation, bureautique). Ils ne peuvent pas installer de logiciels ou modifier la configuration du système.
- **Comptes administrateurs** : disposent de tous les droits, y compris l'installation de logiciels et la modification des paramètres système.

Exemple pratique :
Dans un foyer, on crée un compte administrateur pour le parent et des comptes standards pour les enfants. Ainsi, les enfants ne peuvent pas installer de jeux ou modifier les paramètres système sans accord.

3. Suppression de comptes

Lorsqu'on supprime un compte, Windows propose deux choix :

- **Supprimer tout** : les données personnelles de l'utilisateur sont effacées.
- **Conserver les fichiers** : les fichiers sont sauvegardés dans un dossier distinct (ex. `C:\Utilisateurs\NomUtilisateur`).

Exemple :
Un collègue quitte une entreprise : son compte est supprimé mais ses fichiers sont conservés pour transmission au remplaçant.

4. Personnalisation du bureau

Chaque compte possède son propre bureau :

- Fonds d'écran,
- Raccourcis,
- Applications installées uniquement pour cet utilisateur.

Cela illustre l'importance du cloisonnement : chaque utilisateur travaille dans son propre environnement.

II. Administration via la ligne de commande

Windows fournit des outils puissants pour l'administrateur, notamment la commande `net user`.

1. Activation et désactivation de comptes

```
net user Alice /active:no
```

→ désactive le compte Alice.

```
net user Alice /active:yes
```

→ le réactive.

Cas d'usage : un stagiaire présent uniquement quelques semaines : son compte peut être désactivé sans le supprimer.

5. Gestion des mots de passe

- Définir un mot de passe :

```
net user Alice MonMot2Passe!
```

- Obliger le changement de mot de passe à la prochaine connexion :

```
net user Alice /logonpasswordchg:yes
```

6. Politiques globales avec `net accounts`

- Longueur minimale du mot de passe :

```
net accounts /minpwlen:8
```

- Délai minimum avant modification :

```
net accounts /minpwage:2
```

- Un utilisateur doit attendre **au moins 2 jours** après avoir changé son mot de passe avant de pouvoir en définir un nouveau.

- Cela empêche de modifier plusieurs fois de suite un mot de passe pour "tourner" et revenir rapidement à l'ancien.

  - Interdire la réutilisation :

```
net accounts /uniquepw:5
```

Exemple : imposer un mot de passe d'au moins 8 caractères, modifiable tous les 2 jours minimum, et interdire de reprendre les 5 anciens mots de passe.

7. Restrictions horaires

```
net user Alice /time:Lundi-Vendredi,09:00-18:00
```

→ Alice ne peut se connecter qu'aux heures de bureau.
Exemple : limiter l'accès des postes informatiques scolaires uniquement pendant la journée.

8. Exemples simples net user

1. Créer un utilisateur

```
net user Alice MonMot2Passe! /add
```

→ Crée un compte nommé **Alice** avec le mot de passe **MonMot2Passe!**.

2. Supprimer un utilisateur

```
net user Alice /delete
```

→ Supprime le compte **Alice** du système.

3. Activer ou désactiver un compte

```
net user Alice /active:no
```

→ Désactive temporairement le compte Alice (il ne peut plus se connecter).

```
net user Alice /active:yes
```

→ Réactive le compte Alice.

4. Modifier le mot de passe d'un utilisateur

```
net user Alice NouveauMDP2025!
```

→ Change le mot de passe d'Alice en **NouveauMDP2025!**.

5. Forcer un utilisateur à changer son mot de passe à la prochaine connexion

```
net user Alice /logonpasswordchg:yes
```

→ Lors de sa prochaine connexion, Alice devra définir un nouveau mot de passe.

6. Interdire à un utilisateur de modifier son mot de passe

```
net user Alice /passwordchg:no
```

→ Alice n'aura pas le droit de changer son mot de passe par elle-même.

7. Restreindre les horaires de connexion

```
net user Alice /time:Lundi-Vendredi,09:00-18:00
```

→ Alice ne peut se connecter qu'entre 9h et 18h du lundi au vendredi.

```
net user Alice /time:all
```

→ Supprime les restrictions horaires.

8. Ajouter un utilisateur à un groupe (ex. administrateurs)

```
net localgroup Administrateurs Alice /add
```

→ Ajoute Alice au groupe **Administrateurs**.

9. Voir les informations sur un utilisateur

```
net user Alice
```

→ Affiche les informations du compte Alice (groupes, date de dernière connexion, expiration du mot de passe, etc.).

9. Plus complexes

1. Créer un utilisateur avec mot de passe et description

```
net user Bob Securite2025! /add /comment:"Utilisateur test"
```

→ Crée un compte **Bob** avec le mot de passe `Securite2025!` et ajoute une description visible dans la gestion des utilisateurs.

2. Créer un utilisateur sans mot de passe (déconseillé en production)

```
net user Invité "" /add
```

→ Crée un compte nommé **Invité** sans mot de passe.

3. Définir que le mot de passe n'expire jamais

```
net user Alice /passwordexp:no
```

→ Le mot de passe d'Alice ne sera jamais expiré (utile pour certains comptes techniques).

4. Définir que l'utilisateur ne peut pas changer son mot de passe

```
net user Alice /passwordchg:no
```

→ Alice doit conserver son mot de passe actuel, seul un administrateur pourra le modifier.

5. Définir la date d'expiration du compte

```
net user Stagiaire /expires:31/12/2025
```

→ Le compte **Stagiaire** sera automatiquement désactivé après le 31 décembre 2025.

6. Définir un répertoire personnel différent

```
net user Alice /homedir:C:\Utilisateurs\AlicePerso
```

→ Le dossier personnel d'Alice sera situé dans `C:\Utilisateurs\AlicePerso`.

7. Restreindre un utilisateur à un mot de passe obligatoire

```
net user Alice /passwordreq:yes
```

→ L'utilisateur **Alice** doit obligatoirement avoir un mot de passe (même si Windows permet en théorie de créer un compte sans).

8. Verrouiller temporairement un compte après échec d'authentification

Cela se configure surtout avec `net accounts`, mais on peut l'associer à `net user`.
Exemple :

```
net accounts /lockoutthreshold:3
```

→ Après 3 tentatives échouées, l'utilisateur est verrouillé.

9. Lister tous les utilisateurs du système

```
net user
```

→ Affiche la liste de tous les comptes créés sur la machine.

10. Vérifier les détails complets d'un utilisateur

```
net user Bob
```

→ Affiche toutes les informations de Bob :

- appartenance aux groupes
- date de dernière connexion
- expiration du mot de passe
- restrictions horaires

11. Ajouter un utilisateur à plusieurs groupes

```
net localgroup "Utilisateurs du Bureau à distance" Bob /add
net localgroup "Administrateurs" Bob /add
```

→ Bob devient à la fois administrateur et autorisé à utiliser le Bureau à distance.

12. Supprimer un utilisateur d'un groupe

```
net localgroup Administrateurs Bob /delete
```

→ Retire Bob du groupe Administrateurs (il reste utilisateur standard).

III. Stratégies locales de sécurité (édition Pro)

Disponible dans :
Panneau de configuration > Outils d'administration > Stratégie de sécurité locale
Exemples de stratégies possibles :

- **Forcer la fermeture de session** après expiration des horaires autorisés.
- **Notifier le changement de mot de passe** quelques jours avant expiration.
- **Activer ou renommer le compte invité** (souvent désactivé par sécurité).
- **Durée d'inactivité avant verrouillage automatique** (ex. 5 minutes).
- **Configurer Kerberos** pour définir les algorithmes de chiffrement utilisés lors de l'authentification.

Exemple concret :
Dans un laboratoire universitaire, on configure le verrouillage automatique après 5 minutes d'inactivité afin d'éviter que des étudiants ne laissent leur session ouverte.

I. IV. Active Directory et gestion centralisée

1. Définition et rôle d'Active Directory

Active Directory (AD) est un **service d'annuaire centralisé** développé par Microsoft.
Il permet de stocker et d'organiser les informations relatives aux **utilisateurs**, **ordinateurs**, **applications** et **ressources** d'un réseau.

a) Rôles principaux

- **Authentification** : vérification de l'identité (Kerberos, NTLM).
- **Autorisation** : contrôle des droits d'accès aux ressources.
- **Centralisation** : gestion unifiée des comptes et paramètres.
- **Sécurité** : application homogène de règles à l'échelle de l'entreprise.

Exemple : un employé utilise le même compte pour se connecter sur n'importe quel poste de l'entreprise et accéder à ses fichiers, emails et imprimantes.

2. Structure logique d'Active Directory

Active Directory est organisé en plusieurs niveaux hiérarchiques.

b) a) La forêt

- Élément le plus haut de la hiérarchie.
- Représente la limite de sécurité.
- Contient un ou plusieurs arbres.
- Tous les domaines d'une forêt partagent un **schéma unique**.

c) b) L'arbre

- Ensemble de domaines reliés entre eux par une relation hiérarchique.
- Les domaines d'un même arbre partagent le même **espace de noms DNS**.
- Exemple :
  - Domaine racine : *entreprise.local*
  - Domaine enfant : *compta.entreprise.local*

d) c) Le domaine

- Unité de base d'AD.
- Identifié par un nom DNS.
- Regroupe utilisateurs, ordinateurs et ressources.
- Relation de confiance automatique entre domaines d'un même arbre.

e) d) Les Unités d'Organisation (OU)

- Permettent d'organiser logiquement les objets dans un domaine.
- Hiérarchiques et imbriquées.

- Utilisées pour la **délégation d'administration** et l'application des **GPO**.
- Exemple : *OU Utilisateurs → Comptabilité, Informatique, RH*.

f) e) Les objets

- Éléments finaux de l'annuaire :
  - **Comptes utilisateurs** (employés, étudiants),
  - **Ordinateurs**,
  - **Groupes** (sécurité, distribution),
  - **Imprimantes**.

g) Hiérarchie récapitulative

- Une **forêt** contient **1 à n arbres**
- Un **arbre** contient **1 à n domaines**
- Un **domaine** contient **n UO**
- Une **UO** contient **n objets**

h) Schéma conceptuel

```
Forêt : ENTREPRISE
    |
    +-- Arbre : entreprise.local
            |
            +-- Domaine : entreprise.local
            |         |
            |         +-- UO : Utilisateurs
            |         |          +-- Alice (utilisateur)
            |         |          +-- Bob (utilisateur)
            |         |
            |         +-- UO : Ordinateurs
            |                    +-- PC-01
            |                    +-- PC-02
            |
            +-- Domaine enfant : compta.entreprise.local
                      |
                      +-- UO : Comptabilité
                                 +-- Utilisateur : Clara
```

3. Contrôleurs de domaine et catalogue global

a) Contrôleur de domaine (DC)

- Serveur qui héberge et gère l'annuaire AD.
- Valide l'authentification et applique les règles.
- Plusieurs DC assurent la **redondance** et la **réplication**.

b) Catalogue global (Global Catalog)

- Contient une copie partielle de tous les objets de la forêt.
- Permet une recherche rapide dans l'annuaire.

4. Comptes et groupes

a) Comptes

- **Utilisateur** : identifiant unique pour chaque personne.
- **Ordinateur** : chaque poste intégré au domaine a un compte.
- **Service** : utilisé par une application ou un service.

b) Groupes

- Simplifient l'attribution des droits.
- **Groupes de sécurité** : gèrent les autorisations.
- **Groupes de distribution** : servent aux listes de diffusion.

c) OU et délégation

- Les OU permettent d'attribuer des responsabilités limitées à certains administrateurs.

5. Stratégies de groupe (GPO – Group Policy Objects)

- Définissent des règles appliquées automatiquement aux utilisateurs et ordinateurs.

Exemples de GPO

- Mot de passe complexe obligatoire.
- Bloquer l'installation de logiciels.
- Appliquer un fond d'écran institutionnel.
- Restreindre les horaires de connexion.

Hiérarchie d'application

- Site → Domaine → OU.
- Les GPO peuvent être filtrées par groupes.

6. Services et protocoles associés

DNS : base du fonctionnement d'AD.

- **Kerberos** : protocole d'authentification sécurisé.
- **LDAP** : permet de lire et modifier l'annuaire.
- **FSMO Roles** : rôles uniques dans la forêt/domaine (maître RID, maître schéma, etc.).

7. Comparaison gestion locale vs AD

Gestion locale	Gestion AD
Comptes créés poste par poste.	Comptes centralisés sur DC.
Paramétrage manuel.	Déploiement automatisé via GPO.

Gestion locale	Gestion AD
Administration lourde.	Administration homogène.
Sécurité limitée.	Sécurité cohérente.
Pas de délégation.	Délégation par OU.

8. Extensions et évolutions

- **Azure AD** : version cloud pour Microsoft 365 et services en ligne.
- **ADFS** : fédération d'identités entre organisations.
- **NPS/RADIUS** : authentification pour Wi-Fi et VPN.

9. Sécurité et bonnes pratiques

- Principe du **moindre privilège**.
- Mise en place de GPO restrictives.
- Redondance des DC.
- Sauvegarde régulière de la base AD.
- Surveillance des journaux de sécurité.