Active Directory

Gestion des utilisateurs, mots de passe et groupes

Windows Server — Active Directory Users and Computers (ADUC)

Ce document décrit les procédures d'administration courantes dans l'Active Directory (AD) Windows Server : création d'un compte utilisateur, réinitialisation d'un mot de passe et création d'un groupe de sécurité ou de distribution.

> ⍰ **Info :** Toutes les opérations décrites nécessitent les droits d'administrateur du domaine ou des délégations appropriées sur l'unité d'organisation (OU) concernée.

Partie 1 — Création d'un compte utilisateur

La création d'un compte utilisateur dans l'AD se réalise via la console ADUC (Active Directory Users and Computers), accessible depuis le Gestionnaire de serveur ou directement via la commande dsa.msc.

1.1 Ouvrir la console ADUC

1. Ouvrez le menu Démarrer et tapez dsa.msc, puis appuyez sur Entrée.
2. La console Active Directory Users and Computers s'affiche.
3. Dans l'arborescence de gauche, naviguez jusqu'à l'**Unité d'Organisation (OU)** dans laquelle vous souhaitez créer l'utilisateur (ex : OU=Utilisateurs,DC=mondomaine,DC=local).

1.2 Créer le nouvel utilisateur

4. Faites un **clic droit** sur l'OU sélectionnée → **Nouveau** → **Utilisateur**.
5. L'assistant de création d'utilisateur s'ouvre. Renseignez les informations suivantes :

Prénom *	Ex : Jean
Initiales	Ex : P
Nom *	Ex : Dupont
Nom d'ouverture de session (UPN) *	Ex : j.dupont@mondomaine.local
Nom de connexion (pré-Win 2000) *	Ex : DOMAINE\j.dupont

6. Cliquez sur **Suivant**.

1.3 Définir le mot de passe initial

7. Saisissez un mot de passe temporaire conforme à la stratégie de mot de passe du domaine.
8. Configurez les options suivantes selon la politique interne :

L'utilisateur doit changer le mot de passe	Coché (recommandé) — l'utilisateur devra définir son propre mot de passe à la première connexion
L'utilisateur ne peut pas changer le mot de passe	Décoché (sauf exception)
Le mot de passe n'expire jamais	Décoché (sauf comptes de service)
Le compte est désactivé	Décoché pour activer immédiatement

9. Cliquez sur **Suivant** puis sur **Terminer**. Le compte est créé.

✔ **Bonne pratique :** Après la création, complétez les onglets Général, Organisation, Téléphones et Adresse dans les propriétés du compte pour faciliter les recherches dans l'annuaire.

Sécurité : Le mot de passe temporaire doit être transmis à l'utilisateur via un canal sécurisé (en main propre ou messagerie chiffrée). Ne jamais l'envoyer en clair par e-mail.

Partie 2 — Réinitialisation du mot de passe utilisateur

La réinitialisation d'un mot de passe est une opération fréquente (oubli, verrouillage, départ/retour de congé). Elle se fait depuis la console ADUC ou via PowerShell.

2.1 Réinitialisation via la console ADUC

10. Dans ADUC, localisez le compte utilisateur (utilisez **Ctrl+F** ou le menu **Rechercher** pour une recherche rapide).
11. Faites un **clic droit** sur le compte → **Réinitialiser le mot de passe…**
12. La fenêtre de réinitialisation s'ouvre. Renseignez les champs :

Nouveau mot de passe *	Saisir le mot de passe temporaire
Confirmer le mot de passe *	Resaisir le même mot de passe
L'utilisateur doit changer le mot de passe	Cocher cette option (recommandé)
Déverrouiller le compte	Cocher si le compte est verrouillé

13. Cliquez sur **OK**. Un message de confirmation s'affiche.

2.2 Réinitialisation via PowerShell (méthode alternative)

Pour les administrateurs préférant la ligne de commande ou dans le cadre d'automatisations, voici la commande PowerShell correspondante :

```
# Réinitialiser le mot de passe d'un utilisateur AD
Set-ADAccountPassword -Identity "j.dupont" \
    -NewPassword (ConvertTo-SecureString "NouveauMdp123!" -AsPlainText -
Force) \
    -Reset

# Forcer le changement au prochain logon
Set-ADUser -Identity "j.dupont" -ChangePasswordAtLogon $true

# Déverrouiller un compte
Unlock-ADAccount -Identity "j.dupont"
```

⚠ **Attention :** Remplacez "j.dupont" par le SamAccountName réel de l'utilisateur et "NouveauMdp123!" par un mot de passe conforme à la politique du domaine.

Sécurité : Ne stockez jamais de mots de passe en clair dans des scripts PowerShell. Utilisez Get-Credential ou un coffre-fort de mots de passe (ex : KeePass, HashiCorp Vault).

Partie 3 — Création d'un groupe Active Directory

Les groupes AD permettent de gérer les accès aux ressources (partages réseau, applications, GPO…) de façon centralisée. Il existe deux grandes catégories de groupes.

3.1 Types de groupes AD

Groupe de Sécurité	Groupe de Distribution
Gestion des accès aux ressources : • Partages réseau • Droits sur les GPO • Accès aux applications • Droits locaux sur les machines	**Envoi d'e-mails groupés :** • Listes de diffusion Exchange • Pas d'affectation de droits • Utilisé avec Microsoft 365

3.2 Étendues de groupe

Domaine local	Accès aux ressources dans le domaine local uniquement. Peut contenir des membres de n'importe quel domaine.
Global	Regroupe des utilisateurs du même domaine. Peut être utilisé dans tout domaine de la forêt.

Universel	Peut contenir des membres de toute la forêt. Utilisé dans les environnements multi-domaines.

3.3 Créer un groupe via la console ADUC

14. Dans ADUC, naviguez jusqu'à l'**OU** de destination.
15. Faites un **clic droit** → **Nouveau** → **Groupe**.
16. La fenêtre de création de groupe s'ouvre. Renseignez les champs :

Nom du groupe *	Ex : GRP_Comptabilite_Lecture
Nom du groupe (pré-Win 2000) *	Ex : GRP_Comptabilite_Lecture
Étendue du groupe	Global (recommandé par défaut)
Type de groupe	Sécurité (pour la gestion des accès)

17. Cliquez sur **OK**. Le groupe est créé.

3.4 Ajouter des membres au groupe

18. Faites un **clic droit** sur le groupe créé → **Propriétés**.
19. Cliquez sur l'onglet **Membres** → **Ajouter…**
20. Saisissez le nom de l'utilisateur ou d'un autre groupe, cliquez sur Vérifier les noms puis sur OK.
21. Validez avec **Appliquer** puis **OK**.

3.5 Création via PowerShell (méthode alternative)

```
# Créer un groupe de sécurité global
New-ADGroup -Name "GRP_Comptabilite_Lecture" \
    -SamAccountName "GRP_Comptabilite_Lecture" \
    -GroupCategory Security \
    -GroupScope Global \
    -DisplayName "Comptabilite - Lecture" \
    -Path "OU=Groupes,DC=mondomaine,DC=local" \
    -Description "Accès en lecture aux dossiers comptabilité"

# Ajouter un utilisateur au groupe
Add-ADGroupMember -Identity "GRP_Comptabilite_Lecture" -Members "j.dupont"
```

✔ **Bonne pratique :** Adoptez une convention de nommage cohérente pour vos groupes : ex. GRP_[Service]_[Droits] (GRP_RH_Ecriture, GRP_IT_Admin…). Cela facilite grandement l'administration.

Récapitulatif des opérations

1

Créer un utilisateur

ADUC → clic droit sur l'OU → Nouveau → Utilisateur → renseigner les champs → définir le mot de passe initial.

2

Réinitialiser un mot de passe

ADUC → localiser le compte → clic droit → Réinitialiser le mot de passe → cocher "changer au prochain logon".

3

Créer un groupe AD

ADUC → clic droit sur l'OU → Nouveau → Groupe → choisir le type et l'étendue → ajouter les membres.