

TIP 3.11

Créer, modifier et désactiver des comptes Active Directory

Fiche de révision - Module Infrastructure TIP

1. Cycle de vie d'un compte

Création → activation → évolution → suspension → fin de vie.
Chaque étape doit correspondre à une demande autorisée et être documentée.

2. Principaux attributs

Attribut	Exemple / rôle
Name	Sophie Martin
sAMAccountName	smartin - utilisé notamment sous DOMAINE\utilisateur.
UPN	smartin@entreprise.local - identifiant de type utilisateur@domaine.
Department	Comptabilité
Title	Gestionnaire comptable
Enabled	Indique si le compte est activé.

3. Avant la création

Vérifier la demande, la convention de nommage, l'absence de doublon, l'OU cible, les attributs attendus et la politique de mot de passe. Exemple de recherche : `Get-ADUser -Filter 'SamAccountName -eq "smartin"'`.

4. Créer un utilisateur

Outil	Exemple
Console graphique	dsa.msc → OU cible → Nouvel utilisateur.
PowerShell	New-ADUser avec Name, GivenName, Surname, SamAccountName, UPN, Path, AccountPassword, Enabled.

5. Mot de passe initial

Ne pas écrire de mot de passe en clair dans un script. Utiliser un secret saisi de manière sécurisée, par exemple avec `Read-Host -AsSecureString`, et appliquer les règles de l'organisation. Lorsque prévu, imposer un changement à la première ouverture de session.

6. Modifier les attributs

Commande	Utilité
Set-ADUser	Modifier service, fonction, bureau, téléphone ou autres attributs.
Get-ADUser -Properties ...	Vérifier uniquement les attributs nécessaires.

7. Mot de passe et verrouillage

Action	Commande / remarque
Réinitialiser le mot de passe	Set-ADAccountPassword -Reset -NewPassword ...
Forcer le changement	Set-ADUser -ChangePasswordAtLogon \$true
Vérifier le verrouillage	Get-ADUser -Properties LockedOut ou Search-ADAccount -LockedOut
Déverrouiller	Unlock-ADAccount -Identity utilisateur

8. Désactivation et réactivation

Action	Commande
Désactiver	Disable-ADAccount -Identity smartin
Réactiver	Enable-ADAccount -Identity smartin
Vérifier	Get-ADUser -Identity smartin -Properties Enabled

9. Désactiver n'est pas supprimer

Désactivation	Suppression
L'objet reste dans AD.	L'objet est supprimé.
Attributs et groupes restent visibles.	Action plus impactante nécessitant une procédure.
Réactivation possible.	Récupération/recréation selon contexte et sauvegardes.

10. Expiration et audit

Besoin	Commande
Définir une expiration	Set-ADAccountExpiration -Identity utilisateur -DateTime ...
Lister les comptes expirés	Search-ADAccount -AccountExpired -UsersOnly
Date de création	Get-ADUser -Properties whenCreated
Dernier changement de mot de passe	Get-ADUser -Properties PasswordLastSet

11. Réflexes sécurité

Vérifier l'identité avant toute réinitialisation de mot de passe. Ne jamais partager ou réutiliser un compte nominatif. Ne pas réutiliser le compte d'un ancien salarié pour son remplaçant. Désactiver rapidement un compte lors d'un départ selon la procédure. Tracer chaque modification.

12. Méthode à retenir

Vérifier la demande → rechercher l'existant → créer/modifier → sécuriser → contrôler → documenter.

13. À retenir

Get-ADUser : rechercher/vérifier. New-ADUser : créer. Set-ADUser : modifier. Set-ADAccountPassword : réinitialiser un mot de passe. Unlock-ADAccount : déverrouiller. Disable-ADAccount : désactiver. Enable-ADAccount : réactiver. sAMAccountName : identifiant historique. UPN : utilisateur@domaine. Désactivation ≠ suppression. Une personne = une identité nominative.