

TIP 3.12

Gérer groupes, unités d'organisation et droits

Fiche de révision - Module Infrastructure TIP

1. Groupe ou unité d'organisation ?

Groupe de sécurité	Unité d'organisation (OU)
Regroupe utilisateurs, ordinateurs ou groupes.	Organise logiquement les objets AD.
Peut recevoir des permissions.	Peut recevoir des GPO et des délégations.
Utilisé pour gérer les accès.	Utilisée pour structurer l'administration.

2. Type et portée des groupes

Élément	À retenir
Sécurité	Utilisable pour attribuer des permissions.
Distribution	Principalement destiné à la messagerie, pas aux droits de sécurité classiques.
Global	Souvent utilisé pour représenter un métier ou un rôle.
Domaine local	Souvent utilisé pour porter un niveau d'accès sur une ressource.
Universel	Utile surtout dans certaines architectures multi-domaines.

3. La méthode AGDLP

Accounts → Global groups → Domain Local groups → Permissions.
Exemple : smartin → GG_COMPTABILITE → GDL_COMPTA_MODIF → permission Modification sur le dossier.

4. Pourquoi utiliser AGDLP ?

La structure sépare l'identité, le métier et la permission. Un changement de service peut alors être géré principalement en modifiant les appartenances aux groupes, sans rechercher l'utilisateur dans toutes les ACL.

5. Commandes PowerShell - groupes

Commande	Utilité
New-ADGroup	Créer un groupe de sécurité avec une portée donnée.
Add-ADGroupMember	Ajouter utilisateur ou groupe à un groupe.
Remove-ADGroupMember	Retirer un membre.
Get-ADGroupMember	Afficher les membres d'un groupe.
Get-ADPrincipalGroupMembership	Afficher les groupes d'un utilisateur.

6. Bonnes pratiques d'appartenance

Ajouter un utilisateur à un groupe est une opération de sécurité : cela peut lui ouvrir des ressources. Toujours vérifier la demande, éviter les groupes trop privilégiés et appliquer le moindre privilège.

7. Les unités d'organisation

Une OU est un conteneur logique destiné à organiser les objets Active Directory. Elle peut servir de cible à des GPO et permettre une délégation d'administration. Placer un utilisateur dans une OU ne lui donne pas automatiquement accès à un partage.

8. Commandes PowerShell - OU

Commande	Utilité
New-ADOrganizationalUnit	Créer une OU.
Get-ADOrganizationalUnit	Lister ou rechercher les OU.
Move-ADObject	Déplacer un objet vers une autre OU.

9. Délégation d'administration

La délégation permet d'autoriser une équipe à effectuer certaines opérations sur une OU - par exemple réinitialiser des mots de passe ou gérer certains postes - sans lui donner les privilèges complets du domaine.

10. Groupes et droits NTFS

Groupe d'accès	Permission sur la ressource
GDL_COMPTA_LECTURE	Lecture
GDL_COMPTA_MODIF	Modification

11. Changements de groupe et session

Une modification d'appartenance à un groupe n'est pas toujours immédiatement visible dans une session déjà ouverte. Le jeton de sécurité de l'utilisateur est construit lors de l'authentification. Selon le contexte, une nouvelle ouverture de session peut être nécessaire. `whoami /groups` permet d'afficher les groupes présents dans le jeton courant.

12. Erreurs à éviter

Erreur	Pourquoi
Ajouter directement chaque utilisateur dans l'ACL	Difficile à maintenir et à auditer.
Utiliser l'OU comme mécanisme de permission	Une OU n'accorde pas automatiquement un droit sur une ressource.
Conserver les anciens groupes après changement de service	Crée des accès inutiles et viole le moindre privilège.
Ajouter à Domain Admins pour résoudre un accès	Privilege excessif, très mauvais contournement.

13. Méthode à retenir

Demande → identité → groupe métier → groupe d'accès → permission → test → documentation.

14. À retenir

Groupe de sécurité : gère les autorisations. OU : organise les objets. Global : souvent métier/rôle. Domaine local : souvent niveau d'accès. AGDLP : Accounts → Global → Domain Local → Permissions. New-ADGroup : crée un groupe. Add-ADGroupMember : ajoute un membre. Get-ADGroupMember : liste les membres. Get-ADPrincipalGroupMembership : groupes d'un utilisateur. `whoami /groups` : groupes présents dans la session. Moindre privilège : uniquement les droits nécessaires.