

TIP 3.13

Vérifier l'accès aux ressources et résoudre un incident AD

Fiche de révision - Module Infrastructure TIP

1. Méthode de diagnostic

Identifier → domaine → compte → groupes → session → réseau → ressource → permissions → corriger → valider.
L'objectif est de localiser la cause avant toute modification.

2. Authentification ou autorisation ?

Notion	Question	Exemple
Authentification	Qui es-tu ?	L'utilisateur ne parvient pas à ouvrir sa session.
Autorisation	À quoi as-tu droit ?	La session s'ouvre mais le partage répond « Accès refusé ».

3. Vérifications côté poste et domaine

Commande	Utilité
whoami	Vérifier l'identité réellement utilisée.
Get-CimInstance Win32_ComputerSystem	Contrôler Domain et PartOfDomain.
Get-NetIPConfiguration	Vérifier IP, passerelle et DNS.
Resolve-DnsName dc01...	Tester la résolution du contrôleur.
nltest /dsgetdc:entreprise.local	Vérifier la découverte d'un DC.
Test-ComputerSecureChannel	Tester le canal sécurisé poste/domaine.

4. Vérifier l'état du compte

Élément	Commande / interprétation
Compte actif	Get-ADUser -Properties Enabled → Enabled doit correspondre à la situation attendue.
Compte verrouillé	LockedOut ou Search-ADAccount -LockedOut.
Expiration	AccountExpirationDate pour les comptes temporaires.
Mot de passe	PasswordLastSet aide à vérifier une réinitialisation récente.

5. Groupes AD et jeton de session

Get-ADPrincipalGroupMembership smartin affiche les groupes AD de l'utilisateur. Get-ADGroupMember permet de vérifier l'imbrication des groupes. whoami /groups affiche les groupes présents dans le jeton de sécurité de la session actuelle. Après un changement de groupe, une nouvelle ouverture de session peut être nécessaire.

6. Vérifier la ressource partagée

Commande	Utilité
Resolve-DnsName SRV-FICHIERS	Résoudre le nom du serveur.
Test-NetConnection SRV-FICHIERS -Port 445	Tester le service SMB.
Get-SmbShare	Vérifier que le partage existe.
Get-SmbShareAccess -Name COMPTABILITE	Examiner les permissions du partage.
(Get-Acl "D:\Partages\Comptabilite").Access	Examiner les permissions NTFS.

7. Partage + NTFS

Partage	NTFS	Résultat via le réseau
Lecture	Modification	Lecture
Contrôle total	Lecture	Lecture
Contrôle total	Modification	Modification

8. Symptômes typiques

Symptôme	Piste prioritaire
Impossible d'ouvrir la session	Authentification, compte, DNS, DC, heure.
Un seul utilisateur : accès refusé	Compte, groupes, jeton, droits effectifs.
Tout un service est bloqué	Serveur, réseau, SMB, partage, permissions communes.
Compte verrouillé à répétition	Chercher un ancien mot de passe enregistré ou des tentatives anormales.
Relation d'approbation échouée	DNS, réseau, heure, objet ordinateur, canal sécurisé.

9. Kerberos et heure

klist affiche les tickets Kerberos de la session. w32tm /query /status permet de vérifier la synchronisation temporelle. En cas de problème d'authentification de domaine, DNS et heure sont des contrôles essentiels.

10. Erreurs à éviter

Erreur	Pourquoi
Tout le monde : Contrôle total	Masque la cause et expose inutilement la ressource.
Ajouter l'utilisateur à plusieurs groupes « pour tester »	Crée des privilèges inutiles et rend le diagnostic confus.
Sortir/rejoindre immédiatement le domaine	Peut compliquer l'incident sans traiter la cause.
Déverrouiller sans chercher la cause	Le verrouillage risque de revenir immédiatement.

11. À retenir

whoami : identité utilisée. Get-ADUser : état du compte. Search-ADAccount -LockedOut : comptes verrouillés. Get-ADPrincipalGroupMembership : groupes AD. whoami /groups : groupes dans la session. Test-ComputerSecureChannel : canal sécurisé. TCP 445 : SMB. Get-SmbShareAccess : droits du partage. Get-Acl : ACL NTFS. klist : tickets Kerberos. Réflexe technicien : identifier la cause, corriger au minimum, tester et documenter.