

TIP 3.10

Joindre un poste au domaine

Fiche de révision - Module Infrastructure TIP

1. Ce que réalise la jonction

Le poste devient membre du domaine, possède un objet ordinateur dans Active Directory, peut utiliser des comptes du domaine, recevoir des GPO et accéder aux ressources selon les droits attribués.

2. Prérequis essentiels

Contrôle	À vérifier
Édition Windows	Pro, Enterprise ou Education pour une jonction AD classique.
Nom du poste	Respecter la convention de nommage, ex. PC-COMPTA-07.
Réseau	IP, masque/préfixe, passerelle et connectivité cohérents.
DNS	Utiliser le DNS interne Active Directory prévu par l'organisation.
Heure	Date, heure et fuseau cohérents pour Kerberos.
Compte	Utiliser un compte disposant uniquement des droits nécessaires à la jonction.

3. Commandes de préparation

Commande	Utilité
hostname	Afficher le nom actuel du poste.
Get-NetIPConfiguration	Vérifier IP, passerelle et DNS.
Resolve-DnsName dc01.entreprise.local	Tester la résolution du contrôleur de domaine.
Resolve-DnsName -Type SRV "_ldap._tcp.dc._msdcs.entreprise.local"	Vérifier la découverte DNS des contrôleurs.
nltest /dsgetdc:entreprise.local	Demander à Windows de localiser un contrôleur de domaine.
w32tm /query /status	Examiner la synchronisation temporelle.

4. DNS : point critique

Un poste peut avoir Internet avec un DNS public et pourtant être incapable de joindre le domaine. Active Directory s'appuie sur le DNS interne et sur des enregistrements SRV pour localiser ses services.

5. Jonction graphique

sysdm.cpl → propriétés du nom de l'ordinateur → sélectionner Domaine → saisir le domaine → fournir les identifiants autorisés → valider → redémarrer.

6. Jonction PowerShell

Add-Computer -DomainName "entreprise.local" -Credential (Get-Credential) -Restart
 Pour cibler une OU : ajouter -OUPath avec le Distinguished Name approprié. Éviter d'inscrire des mots de passe en clair dans les scripts.

7. Après le redémarrage

Contrôle	Commande / vérification
Appartenance	Get-CimInstance Win32_ComputerSystem Select Name,Domain,PartOfDomain
Compte utilisé	whoami → vérifier DOMAINE\utilisateur et non PC\utilisateur.
Serveur de connexion	echo %LOGONSERVER%
Canal sécurisé	Test-ComputerSecureChannel
GPO	gpupdate /force puis gpresult /r si nécessaire.
Ressources	Tester les partages et services réellement nécessaires à l'utilisateur.

8. Erreurs fréquentes

Symptôme	Piste
Domaine introuvable	DNS, réseau, routage, pare-feu, contrôleur de domaine.
Identifiants refusés	Compte, mot de passe, état du compte, délégation de droits.
Nom de poste déjà utilisé	Vérifier l'objet AD existant avant toute suppression/réinitialisation.
Problème Kerberos	Vérifier l'heure, le DNS et la communication avec le domaine.
Relation d'approbation cassée	Tester le canal sécurisé et diagnostiquer avant de sortir le poste du domaine.

9. Ce qu'il ne faut pas faire

Ne pas utiliser un DNS public à la place du DNS AD. Ne pas employer systématiquement un compte Domain Admin. Ne pas oublier le redémarrage. Ne pas confondre compte local et compte du domaine. Ne pas sortir/rejoindre immédiatement le domaine comme premier réflexe face à un incident.

10. Méthode à retenir

Préparer → réseau → DNS → découverte du DC → heure → jonction → redémarrage → identité → canal sécurisé → GPO/ressources → documentation.

11. À retenir

Windows Pro/Enterprise/Education : jonction AD classique. DNS interne : indispensable. SRV : découverte des services du domaine. nltest /dsgetdc : localise un DC. Add-Computer : jonction PowerShell. Redémarrage : finalise l'opération. PartOfDomain : contrôle l'appartenance. whoami : vérifie l'identité utilisée. Test-ComputerSecureChannel : teste la relation sécurisée. Réflexe technicien : préparer et vérifier avant de joindre.