

TIP 3.9

Découvrir un domaine Windows et Active Directory

Fiche de révision - Module Infrastructure TIP

1. Groupe de travail ou domaine ?

Groupe de travail	Domaine Active Directory
Comptes gérés localement sur chaque PC.	Identités et objets gérés de manière centralisée.
Administration séparée machine par machine.	Administration centralisée des utilisateurs, postes, groupes et politiques.
Adapté aux environnements simples.	Adapté aux environnements professionnels structurés.

2. Active Directory Domain Services

AD DS est le service d'annuaire de Microsoft utilisé pour centraliser et organiser les objets d'un domaine : utilisateurs, ordinateurs, groupes, unités d'organisation et informations associées.

3. Contrôleur de domaine

Un contrôleur de domaine (DC) héberge AD DS et participe notamment à l'authentification, à l'accès à l'annuaire et à l'application de certaines politiques. Dans une infrastructure professionnelle, plusieurs DC peuvent améliorer la disponibilité et la résilience.

4. Principaux objets AD

Objet	Rôle
Utilisateur	Représente une identité du domaine.
Ordinateur	Représente un poste membre du domaine.
Groupe	Regroupe des identités ou équipements pour faciliter la gestion des droits.
OU	Organise logiquement des objets et facilite administration et application des GPO.

5. Authentification et autorisation

Notion	Question	Exemple
Authentification	Qui es-tu ?	AD valide l'identité de Sophie.
Autorisation	À quoi as-tu droit ?	Les groupes et permissions déterminent l'accès aux ressources.

6. Compte local vs compte de domaine

Compte local	Compte de domaine
PC-COMPTA-07\AdministrateurLocal	ENTREPRISE\smartin
Géré par la machine locale.	Géré par Active Directory.

7. DNS : indispensable à Active Directory

Les postes utilisent DNS pour localiser les services du domaine, notamment les contrôleurs de domaine. Un poste membre ou candidat à la jonction doit utiliser le DNS prévu par l'infrastructure AD. Un DNS public configuré directement sur le poste peut empêcher la découverte correcte des services internes.

8. Kerberos et NTLM

Mécanisme	À retenir
Kerberos	Protocole d'authentification privilégié dans un domaine Windows moderne ; repose notamment sur une heure cohérente et un DNS fonctionnel.
NTLM	Mécanisme plus ancien encore rencontré dans certains scénarios de compatibilité.

9. Outils et commandes utiles

Commande / outil	Utilité
hostname	Afficher le nom du poste.
whoami	Afficher l'identité actuellement utilisée.
systeminfo	Afficher diverses informations système, dont le domaine ou groupe de travail.
echo %USERDOMAIN%	Afficher le domaine associé à la session.
echo %LOGONSERVER%	Afficher le serveur de connexion utilisé dans certains contextes.
Get-CimInstance Win32_ComputerSystem	Vérifier Name, Domain et PartOfDomain.
dsa.msc	Ouvrir Utilisateurs et ordinateurs Active Directory si les outils RSAT sont installés.

10. Pourquoi joindre un poste au domaine ?

La jonction au domaine permet notamment d'utiliser des identités centralisées, d'appliquer des politiques de sécurité, de faciliter l'accès aux ressources professionnelles et de représenter le poste par un objet ordinateur dans Active Directory.

11. Réflexes de sécurité

Bonne pratique	Pourquoi
Comptes nominatifs	Assurer traçabilité et responsabilité.
Moindre privilège	Accorder uniquement les droits nécessaires.
Désactiver les comptes inutilisés	Limiter les accès non légitimes.
Protéger les comptes administratifs	Réduire l'impact d'un compromis.
Respecter les délégations	Le technicien agit dans le cadre défini par l'administrateur du domaine.

12. À retenir

AD DS : service d'annuaire Microsoft. Domaine : environnement centralisé. DC : contrôleur de domaine. Utilisateur : identité. Ordinateur : poste membre du domaine. Groupe : facilite la gestion des droits. OU : organise les objets. Authentification : qui es-tu ? Autorisation : à quoi as-tu droit ? DNS : indispensable au bon fonctionnement d'AD. Kerberos : authentification privilégiée. Réflexe technicien : vérifier identité, domaine, réseau et DNS avant d'aller plus loin.