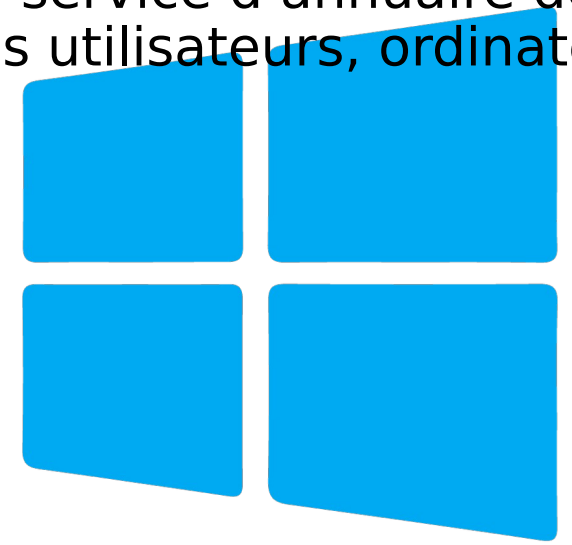
COURS THEORIQUE – ACTIVE DIRECTORY SUR WINDOWS SERVER 2025

Introduction à Active Directory (AD)

- Active Directory est un service d’annuaire développé par Microsoft permettant de gérer les utilisateurs, ordinateurs et ressources d’un réseau d’entreprise.



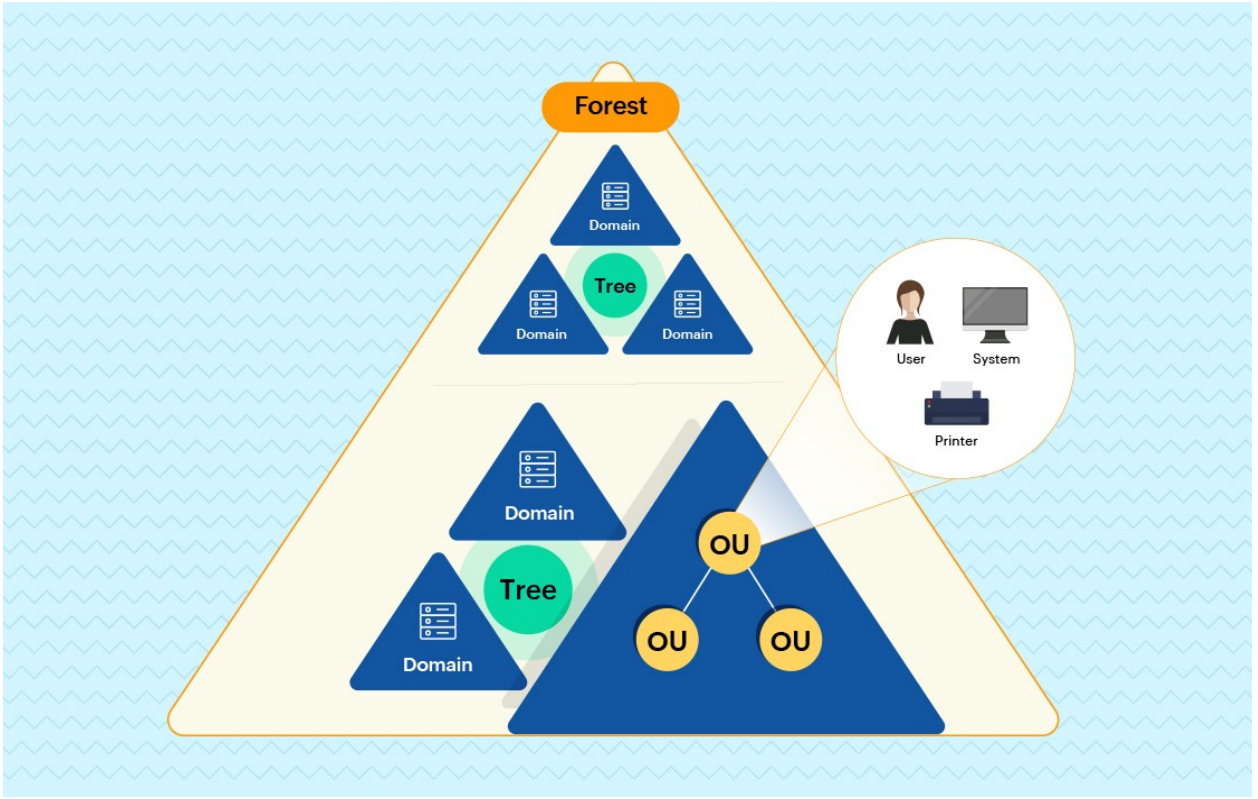
Microsoft
Active Directory

Objectifs Principaux d'Active Directory

- Centraliser l’authentification des utilisateurs.
- Gérer les permissions d’accès aux ressources.
- Appliquer des stratégies de groupe (GPO).
- Organiser logiquement les objets dans des unités organisationnelles (OU).

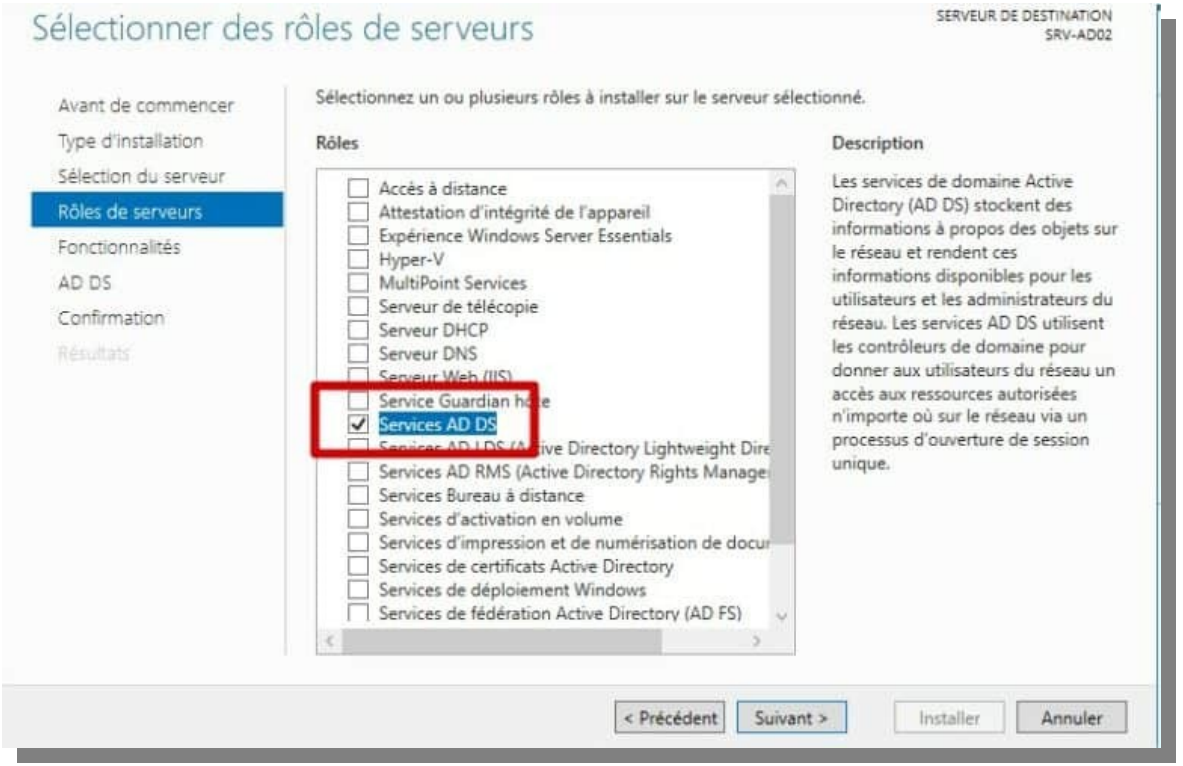
Composants d’Active Directory

- Contrôleur de domaine (DC) : serveur qui héberge la base AD.
- Forêt (Forest) : ensemble de domaines AD.
- Domaine : unité logique d’administration.
- OU (Organizational Unit) : conteneur logique pour organiser les objets.
- GPO (Group Policy Object) : règles de configuration appliquées aux objets AD.



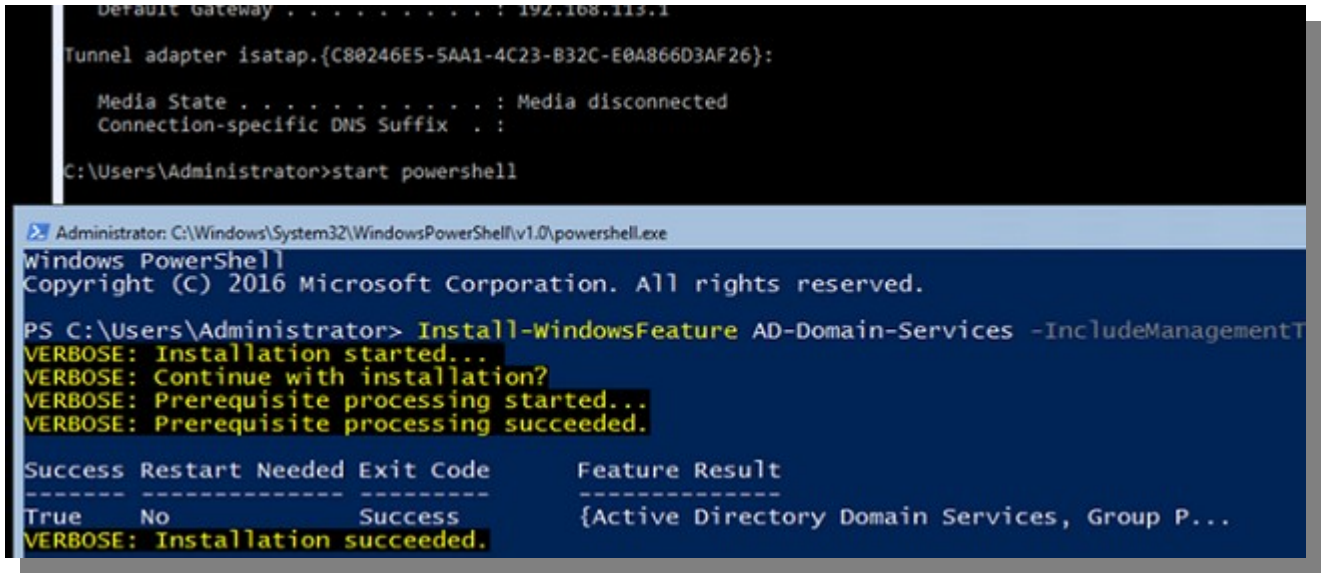
Installation d’un Contrôleur de Domaine (DC)

- Installer le rôle "Services de domaine Active Directory (AD DS)".
- Promouvoir le serveur en contrôleur de domaine via le gestionnaire de serveur.
- Choisir : nouveau domaine / domaine existant.
- Définir le nom du domaine (ex: entreprise.local).



Commandes PowerShell

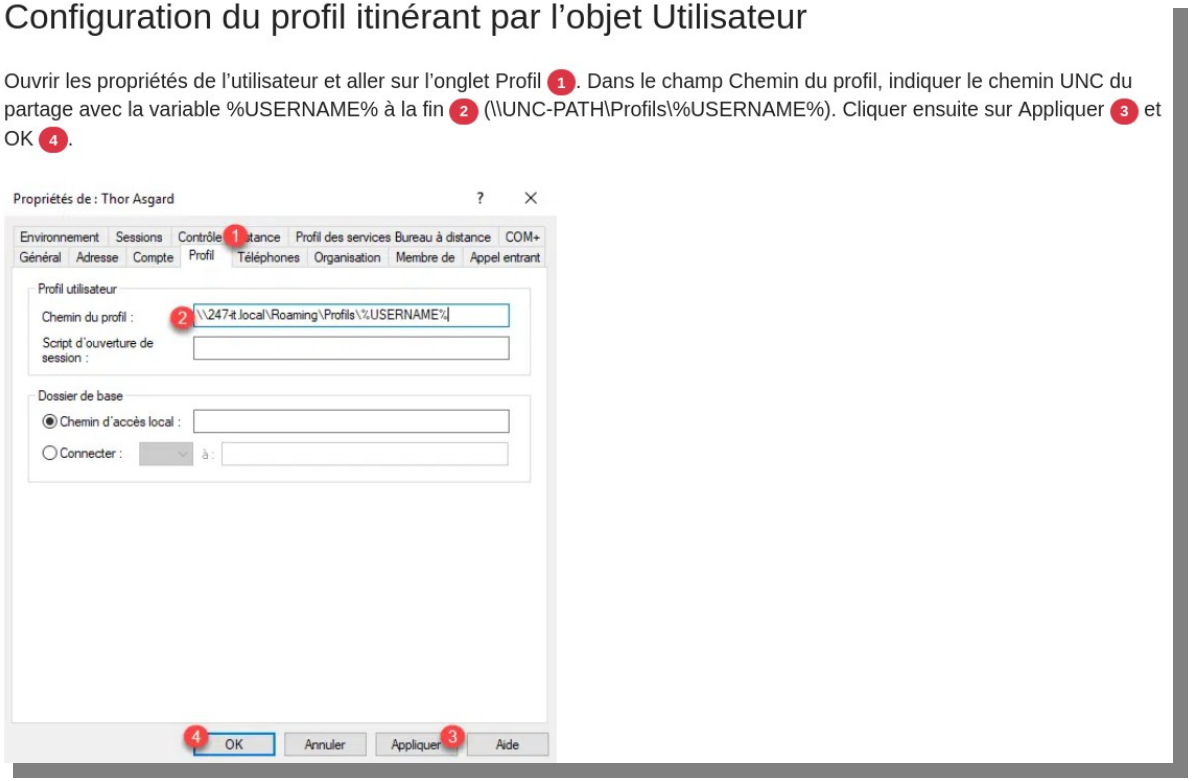
- Install-WindowsFeature -Name AD-Domain-Services
- Install-ADDSForest -DomainName entreprise.local



Configuration des Profils Itinérants

Objectif : permettre aux utilisateurs de retrouver leur environnement (fichiers, paramètres) quel que soit le poste utilisé.

- Créer un dossier partagé centralisé (\\srv-fichiers\profils$).
- Donner les droits NTFS nécessaires (utilisateur + administrateurs).
- Dans les propriétés du compte AD : "Profil", indiquer le chemin UNC.



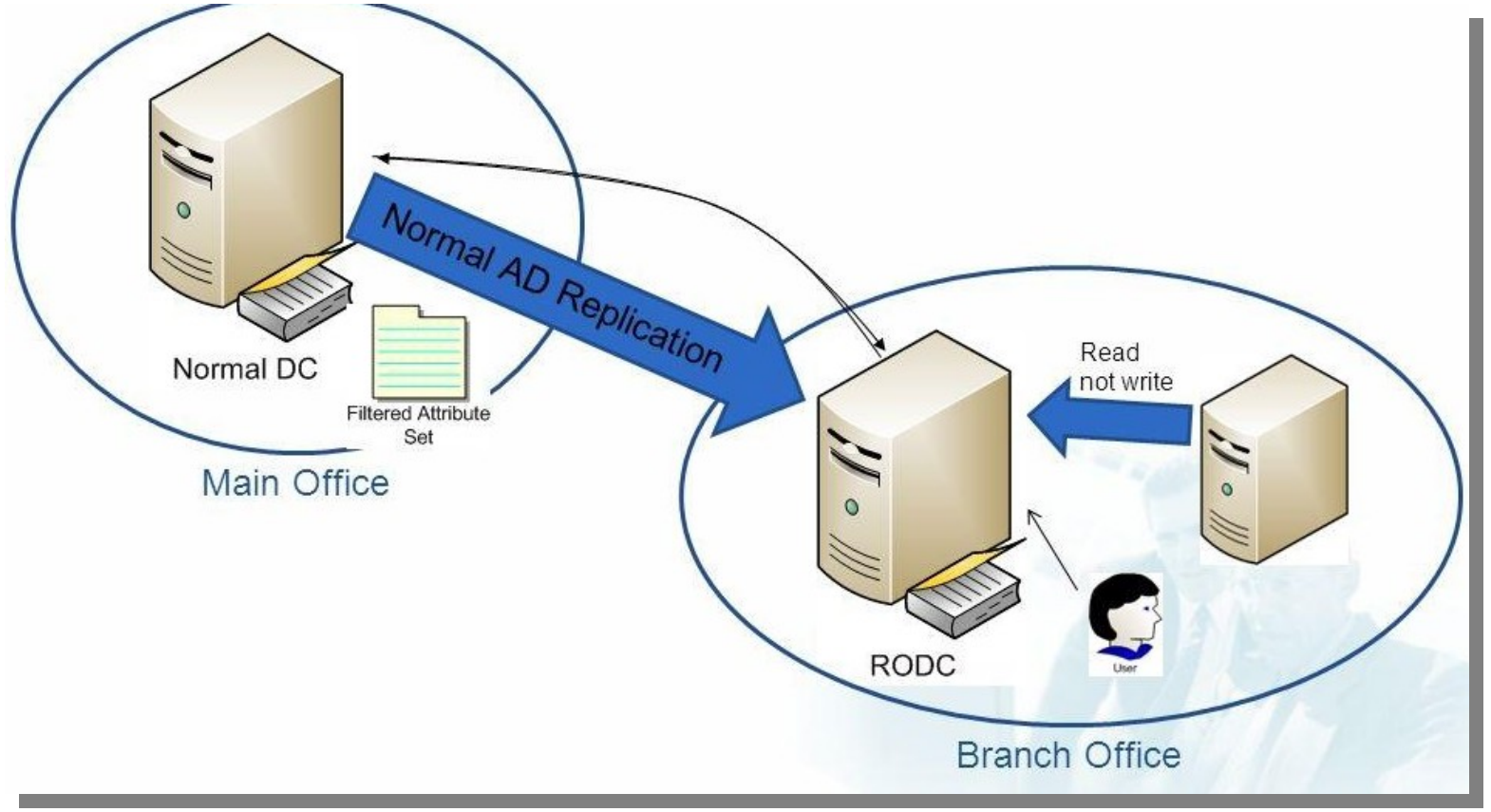
Avantages et Inconvénients des Profils Itinérants

- Avantages:
  - Mobilité utilisateur.
  - Centralisation et sauvegarde facile.
- Inconvénients:
  - Dépendance au réseau.
  - Latences de chargement si mal configuré.

RODC – Read-Only Domain Controller

- Le RODC est un contrôleur de domaine en lecture seule, utile dans les sites distants peu sécurisés.

* Ne stocke pas tous les mots de passe (filtrage).
* Lecture seule : aucune modification locale d’objets AD.
* Idéal pour sites distants ou peu fiables.



Configuration du RODC

- Ajouter un DC > cocher "Contrôleur en lecture seule".
- Choisir les comptes autorisés à se connecter localement.

Sécurité du RODC

- Réduit les risques en cas de vol ou compromis physique.
- Peut limiter la réplication des identifiants sensibles.

Plan de Continuité d’Activité (PCA) – Réplication AD

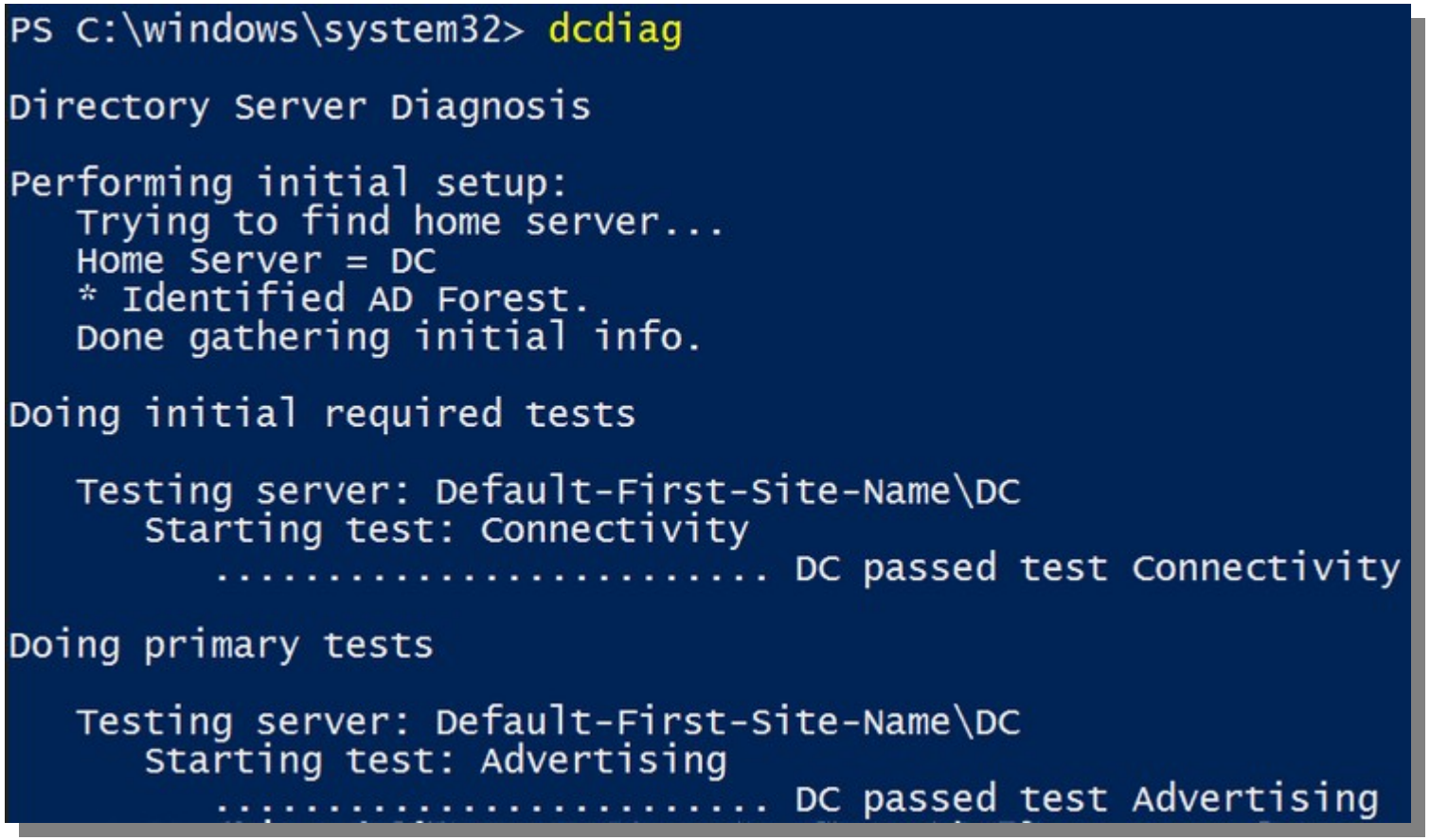
- AD utilise un modèle de réplication multimaitre entre les DC.
- Minimum 2 DC par domaine.
- Réplication planifiée via AD Sites and Services.
- Surveiller l’état de réplication avec `repadmin /replsummary`.

Avantages de la Réplication AD

- Résilience en cas de panne d’un DC.
- Répartition de charge (authentification, DNS...).
- Tolérance aux erreurs.

Outils Utiles pour la Réplication AD

- `repadmin`
- `dcdiag`
- `ntdsutil`
- Event Viewer.



Cybersécurité et Active Directory

- AD est une cible privilégiée pour les attaquants (escalade de privilèges, Golden Ticket, etc.).
- PRIVILÉGIER LE PRINCIPE DE MOINDRE PRIVILÈGE :
  - Éviter les comptes administrateurs permanents.
  - Utiliser l’élévation temporaire.
  - Compte personnel ≠ compte d’administration.
  - Isoler les ressources sensibles.
  - Admin Tiering (TIER 0 / TIER 1 / TIER 2)

Suivi des Modifications

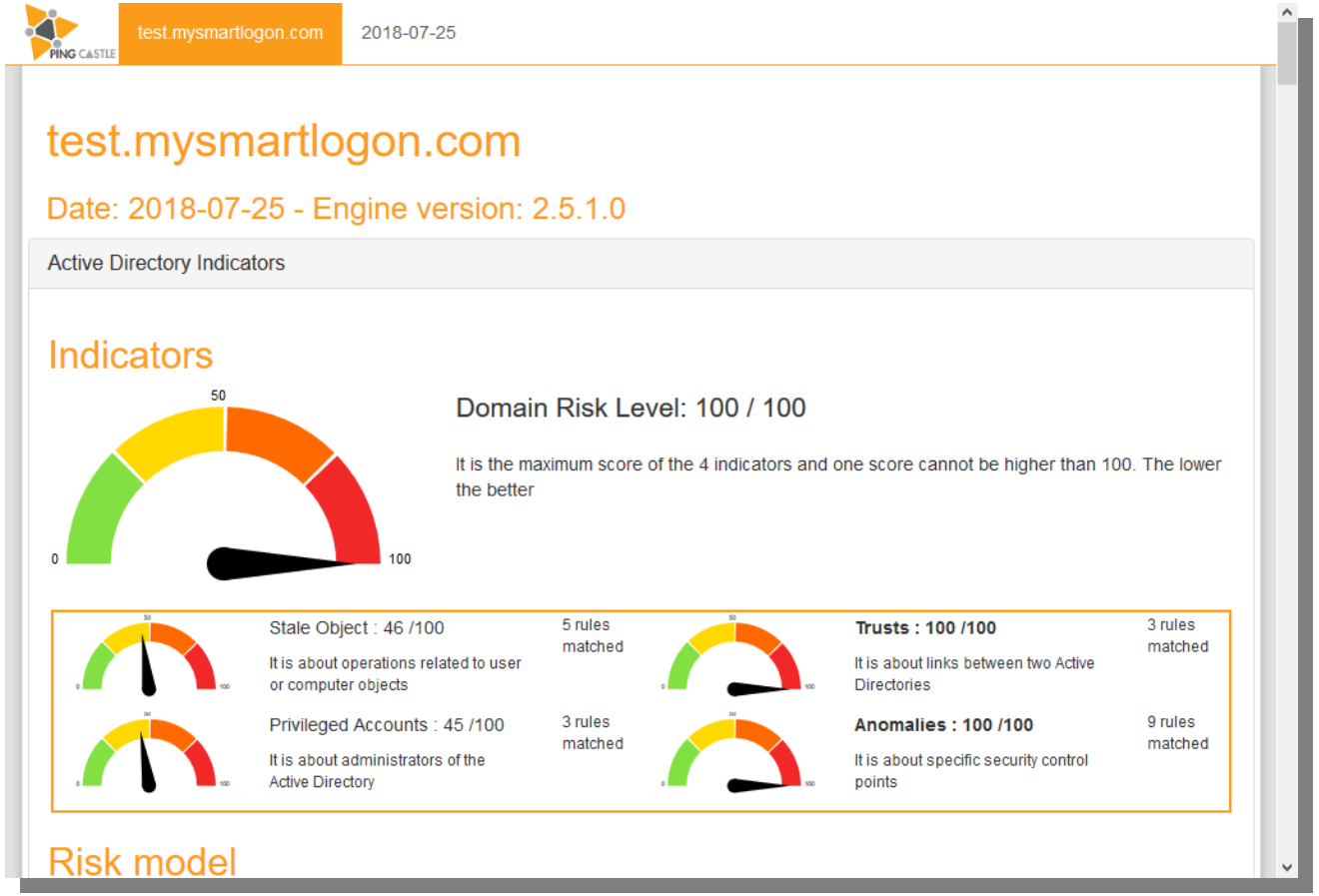
- Activer l’audit AD (activation des journaux de sécurité).
- Mettre en place un SIEM.

Utiliser des GPO pour Durcir les Postes et Serveurs

- Désactiver SMBv1, désactiver comptes invités, limiter les droits admin locaux.

Audit AD avec PingCastle

- PingCastle est un outil d’audit gratuit développé pour évaluer la sécurité d’un annuaire Active Directory.



Fonctionnalités de PingCastle

- Évaluation rapide de l’état de sécurité.
- Recommandations concrètes.
- Détection de comptes à privilèges, de trusts faibles, d’ouvertures réseau à risques.

Utilisation de PingCastle

- Télécharger PingCastle sur un poste joint au domaine.
- Exécuter : `PingCastle.exe --healthcheck --server mon-domaine.local`
- Un rapport HTML est généré avec un score global (critique/haut/moyen/bas).

Réponses Recommandées suite à l'Audit PingCastle

- Suivre les recommandations techniques.
- Mettre en œuvre un plan de remédiation.

Ressources Cyber

- Guide ANSSI "Active Directory : recommandations de sécurité"
- https://www.pingcastle.com/
- Microsoft Security Baselines

Conclusion

- Active Directory est le cœur d’un réseau Microsoft. Son bon fonctionnement et sa sécurité sont critiques. Avec les contrôleurs en lecture seule, la réplication, les profils itinérants et des audits réguliers comme PingCastle, une infrastructure AD peut être robuste, fiable et sécurisée.

FIN DU COURS