AYI NEDJIMI Consultants

Guide de Sécurisation Active Directory Windows Server 2025

Catégorie : Guides Rouges Lecture : 3 min Publié le : 22/03/2026 Auteur : Ayi NEDJIMI

Guide de sécurisation Active Directory Windows Server 2025 : ANSSI, CIS, GPO, PKI, LAPS, PAM — 200 contrôles détaillés pour durcir votre AD.

Ce guide de référence francophone couvre la sécurisation complète d'**Active Directory Windows Server 2025** selon les recommandations **ANSSI**, **CIS Benchmarks** et les meilleures pratiques Microsoft. Rédigé par **Ayi NEDJIMI**, expert en sécurité offensive et défensive, il détaille plus de 200 contrôles de sécurité organisés en neuf domaines : durcissement des contrôleurs de domaine, politique de mots de passe et *Fine-Grained Password Policies (FGPP)*, déploiement de **LAPS**, sécurisation de la *Public Key Infrastructure (PKI)*, protection des délégations Kerberos, hardening des GPO, supervision avec l'audit de sécurité Windows, architecture **Tiering Model**, et réponse à incident. Chaque contrôle est accompagné de sa commande PowerShell de vérification, de son mapping MITRE ATT&CK, et de son niveau de priorité (critique, élevé, moyen).

Structure du Guide Sécurité Active Directory

Le guide est structuré en cinq chapitres progressifs, du durcissement des fondations jusqu'à la réponse à incident :

- **Chapitre 1 — Fondations et Durcissement DC** : SMB signing, LDAP signing, NTLMv2, Kerberos AES, élimination des protocoles legacy
- **Chapitre 2 — Gestion des Identités et des Accès** : FGPP, Protected Users, PAM, comptes de service, gMSA
- **Chapitre 3 — PKI et Délégations** : ADCS hardening, Certificate Templates, Kerberos Constrained Delegation, SPN
- **Chapitre 4 — Supervision et Détection** : Audit Policy, Event IDs critiques, SIEM, Microsoft Sentinel
- **Chapitre 5 — Réponse à Incident AD** : Isolation, krbtgt reset, forest recovery, forensics AD

Points Clés — Sécurisation Active Directory 2025

- Activez **SMB Signing obligatoire** sur tous les DC et serveurs membres — bloque les attaques NTLM Relay de type PetitPotam
- Déployez *LAPS (Local Administrator Password Solution)* sur 100% des machines pour éliminer les mots de passe locaux réutilisés
- Le double reset du compte **krbtgt** invalide tous les Golden Tickets — opération à réaliser après tout compromis suspecté
- Activez **Audit Account Logon** et **Audit Privilege Use** sur tous les DC — collectez les Event IDs 4624, 4625, 4648, 4768, 4769, 4771
- Bloquez l'utilisation de **RC4** et forcez **AES 256** pour Kerberos — élimine les attaques AS-REP Roasting et Kerberoasting sur les comptes sans SPN

Pourquoi sécuriser Active Directory est une priorité absolue en 2026 ?

Active Directory reste la cible numéro un des cyberattaquants : selon les derniers rapports Microsoft MDTI, plus de 95% des ransomwares déployés en entreprise impliquent une compromission AD au stade de la préparation. Les techniques comme le *DCSync*, les *Golden Ticket*, et les *Shadow Credentials* permettent à un attaquant de maintenir un accès persistant indétectable pendant des mois. Notre article sur les abus d'ACL Active Directory détaille ces vecteurs avec des PoC.

Windows Server 2025 introduit des fonctionnalités de sécurité majeures : **Credential Guard** amélioré, **Virtualization-Based Security** par défaut, et le nouveau modèle **IAM Conditional Access** natif. Ce guide couvre leur activation et leur configuration optimale.

Quelles sont les premières mesures à appliquer en urgence ?

Si vous devez prioriser vos actions, commencez par : (1) activer **LDAP signing et channel binding** sur tous les DCs — bloque les attaques LDAP relay ; (2) déployer **Microsoft LAPS v2** sur toutes les machines ; (3) placer les comptes Domain Admins dans le groupe **Protected Users** — désactive NTLM, DES, RC4 et la délégation Kerberos non contrainte. Ces trois mesures réduisent la surface d'attaque de 60% selon le Cybersecurity Assessment Tool Microsoft.

Pour les environnements ayant subi une compromission, consultez notre guide de forensics Windows et notre section sur le post-exploitation et la persistance pour comprendre les traces que les attaquants laissent dans AD.

Comment l'architecture Tiering Model complète-t-elle ce guide ?

La sécurisation technique d'AD (hardening, mots de passe, PKI) doit être complétée par une architecture de cloisonnement des privilèges. Le Guide Complet du Tiering Model Active Directory détaille la séparation Tier 0/1/2, le déploiement des **PAW** et l'architecture **ESAE**. Ces deux guides sont complémentaires et doivent être mis en œuvre conjointement pour une protection maximale.

Les référentiels officiels de l'ANSSI sur Active Directory et les CIS Benchmarks Windows Server constituent les sources normatives de ce guide.

Comment maintenir la sécurité AD dans la durée ?

La sécurité AD est un processus continu. Ce guide fournit un programme de revue trimestrielle : analyse des comptes dormants (>90 jours), vérification des délégations Kerberos, audit des Certificate Templates ADCS, et révision des appartenances aux groupes Domain Admins et Schema Admins. L'article sur l'exploitation ADCS couvre les vecteurs émergents liés aux certificats AD — un vecteur en forte croissance depuis 2023.

Pour les environnements hybrides Azure AD / Entra ID, consultez notre guide de détection des attaques Azure AD qui couvre la synchronisation des identités et les spécificités du cloud.

Sources et références : MITRE ATT&CK · ANSSI

Conclusion

Ce guide est mis à jour au rythme des nouvelles CVE et techniques d'attaque documentées par MITRE ATT&CK. La version PDF téléchargeable intègre les dernières mises à jour de mars 2026, incluant les recommandations post-ESXiArgs et les nouvelles techniques de contournement de **Credential Guard**.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr