AYI NEDJIMI Consultants

Guide Complet du Tiering Model Active Directory 2026

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

Implémentez le Tiering Model Active Directory 2026 : PAW, ESAE, niveaux 0/1/2, GPO de verrouillage et supervision des déplacements latéraux.

Le **Tiering Model Active Directory** est l'architecture de référence définie par Microsoft pour sécuriser un environnement AD contre les attaques modernes. Ce grand guide de référence — rédigé par **Ayi NEDJIMI**, expert en cybersécurité offensive et défensive — couvre intégralement les trois niveaux de privilège (Tier 0, Tier 1, Tier 2), la mise en place des *Privileged Access Workstations (PAW)*, l'architecture *ESAE (Enhanced Security Admin Environment)*, les Group Policy Objects de verrouillage, et la surveillance comportementale des comptes à privilèges. Avec plus de 120 contrôles détaillés, des schémas d'architecture et des scripts PowerShell prêts à l'emploi, ce guide vous accompagne de l'audit initial jusqu'à la mise en production d'une architecture Tiering robuste conforme aux recommandations **ANSSI**, **Microsoft** et **CIS**.

Structure du Guide Tiering Model

Ce guide est organisé en cinq chapitres progressifs qui couvrent l'intégralité du déploiement Tiering Model dans un environnement Active Directory :

- **Chapitre 1 — Fondamentaux du Tiering Model** : principes de séparation des privilèges, Tier 0/1/2, surfaces d'attaque
- **Chapitre 2 — Architecture PAW et ESAE** : déploiement des stations d'administration sécurisées, forest ESAE, délégation minimale
- **Chapitre 3 — GPO et politiques de verrouillage** : User Rights Assignment, credential guard, Protected Users, LAPS
- **Chapitre 4 — Supervision et détection** : Event IDs critiques, alertes SIEM, honeytokens, baselining comportemental
- **Chapitre 5 — Cas pratiques et remédiation** : migration d'un AD legacy, scénarios d'escalade, post-mortem d'incidents

Points Clés — Tiering Model Active Directory

- Le Tier 0 contient les contrôleurs de domaine, PKI, ADFS — aucun compte d'un autre tier ne doit s'y connecter
- Les **PAW** sont obligatoires pour administrer les ressources Tier 0 ; utiliser un PC standard est une faute de sécurité critique
- L'activation du groupe **Protected Users** pour tous les comptes admin bloque les attaques Pass-the-Hash et Pass-the-Ticket
- LAPS doit être déployé sur *tous* les postes Tier 1 et Tier 2 pour éliminer les mots de passe locaux réutilisés
- La détection repose sur les Event IDs 4624/4625/4648/4768/4769 : tout accès Tier 0 depuis un Tier 1/2 doit déclencher une alerte immédiate

Pourquoi le Tiering Model est-il indispensable en 2026 ?

Les attaques ciblant **Active Directory** ont augmenté de 42% en 2025. Les techniques comme le *Pass-the-Hash*, le *Kerberoasting*, les attaques **DCSync** et les **Golden Ticket** exploitent directement l'absence de séparation des privilèges. Sans Tiering Model, un attaquant qui compromet un simple poste utilisateur peut potentiellement atteindre les contrôleurs de domaine en quelques mouvements latéraux. Notre article sur les abus ACL Active Directory illustre comment cette escalade se produit en pratique.

La directive **NIS2**, applicable depuis octobre 2024, impose aux opérateurs d'importance vitale de mettre en place des mesures de gestion des accès privilégiés. Le Tiering Model répond directement à cette obligation. Consultez notre guide sur la conformité NIS2 pour l'articulation réglementaire complète.

Quels sont les prérequis pour déployer le Tiering Model ?

Le déploiement du Tiering Model nécessite un inventaire complet de votre Active Directory existant : comptes de service, délégations, GPO héritées, et accès inter-domaines. Notre Guide de Sécurisation Active Directory Windows Server 2025 contient les checklists d'audit préliminaire. Vous aurez besoin d'au minimum Windows Server 2019 sur les contrôleurs de domaine pour bénéficier des fonctionnalités **Credential Guard** et **Protected Users** complètes.

Sur le plan organisationnel, prévoyez 3 à 6 mois pour un déploiement complet dans un environnement de taille intermédiaire (500 à 2000 utilisateurs). Une approche progressive — en commençant par le Tier 0 — permet de sécuriser les actifs critiques rapidement tout en minimisant l'impact opérationnel.

Comment gérer les comptes de service dans l'architecture Tiering ?

Les *Managed Service Accounts (gMSA)* sont la réponse de Microsoft à la problématique des comptes de service dans un contexte Tiering. Ils permettent la rotation automatique des mots de passe sans intervention manuelle, et leur portée peut être limitée à des machines spécifiques. Tout compte de service ayant des droits sur des ressources Tier 0 doit être classifié Tier 0 lui-même, indépendamment de où il s'exécute.

L'article RBCD — Resource-Based Constrained Delegation détaille les vecteurs d'attaque spécifiques aux délégations Kerberos, souvent exploités pour contourner les contrôles Tiering lorsqu'ils sont mal configurés. Les références externes comme le guide ANSSI sur l'administration sécurisée et la matrice MITRE ATT&CK — Privilege Escalation complètent ce guide.

Comment auditer la conformité de votre Tiering Model ?

L'audit d'un Tiering Model existant s'effectue en trois axes : vérification des appartenances aux groupes Tier 0, analyse des connexions inter-tiers dans les logs de sécurité, et test des délégations Kerberos. Notre guide sur l'exploitation des certificats AD (ADCS) couvre également les vecteurs d'escalade de privilège liés à la PKI, souvent oubliés dans les audits Tiering.

Les scripts PowerShell fournis dans ce guide permettent de générer automatiquement un rapport de conformité Tiering en moins de 30 minutes sur un domaine de 1000 utilisateurs.

Sources et références : MITRE ATT&CK · ANSSI

Conclusion

Ce guide est mis à jour régulièrement pour intégrer les nouvelles techniques d'attaque et les évolutions des recommandations ANSSI et Microsoft. Vous pouvez également **télécharger la version PDF** pour une consultation hors ligne ou une diffusion interne à votre équipe.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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