Active Directory Tiering Model 2026 : Architecture Zero Trust en 3 Niveaux

L'Active Directory Tiering Model, ou modèle d'administration par niveaux, représente en 2026 la pierre angulaire de toute stratégie de sécurité Zero Trust pour les environnements Microsoft Windows d'entreprise. Face à la sophistication croissante des attaques ciblant Active Directory — mouvement latéral, Pass-the-Hash, NTLM Relay, abus de délégation Kerberos, exploitation des chemins BloodHound — les organisations qui maintiennent une architecture à plat, sans séparation des privilèges, sont systématiquement compromises lors des exercices Red Team en quelques dizaines de minutes à peine. Le principe fondamental du Tiering Model est simple mais d'une efficacité redoutable : segmenter les ressources, les comptes et les postes d'administration en trois niveaux d'isolement étanches (Tier 0, Tier 1, Tier 2), de sorte qu'une compromission d'un niveau inférieur ne puisse jamais escalader vers un niveau supérieur grâce à une combinaison de restrictions GPO, de comptes dédiés et de postes durcis. Recommandé par Microsoft dans son Enterprise Access Model, par l'ANSSI dans ses guides de sécurisation Active Directory, et par le CISA dans ses directives de durcissement des environnements gouvernementaux, le Tiering Model active directory est devenu un prérequis pour toute organisation souhaitant atteindre un niveau de maturité SSI sérieux et démontrable. Ce guide pratique détaille l'architecture complète, les modalités d'implémentation étape par étape, les erreurs à éviter et les outils permettant de valider votre déploiement en 2026.

Points essentiels à retenir

Le Tiering Model divise Active Directory en 3 couches étanches : Tier 0 (DC et identité), Tier 1 (serveurs applicatifs), Tier 2 (postes utilisateurs)

Chaque niveau dispose de ses propres comptes d'administration dédiés, jamais partagés entre niveaux, avec des mots de passe distincts

Les Privileged Access Workstations (PAW) sont des postes dédiés et durcis permettant l'administration sécurisée de chaque tier

Les GPO de restriction d'authentification bloquent techniquement les tentatives d'utilisation de comptes Tier 0 sur des machines Tier 1 et 2

Microsoft a renommé son modèle "Enterprise Access Model" en 2021, mais la terminologie Tier 0/1/2 reste dominante dans l'industrie

L'ANSSI et le CISA classent ce modèle comme recommandation de sécurité de premier rang pour toute organisation

Pourquoi le modèle d'administration traditionnel est-il dangereux ?

Dans la majorité des organisations sans Tiering Model, les administrateurs IT utilisent un unique compte à privilèges élevés — souvent membre du groupe Domain Admins — pour toutes leurs tâches : administration des contrôleurs de domaine, maintenance des serveurs applicatifs, dépannage des postes utilisateurs, navigation sur Internet et lecture des e-mails depuis ce même compte. Cette approche "à plat" crée une surface d'attaque colossale qui rend toute compromission partielle immédiatement fatale pour l'ensemble du domaine.

Prenons un scénario type reproduit quotidiennement lors des exercices Red Team : un administrateur utilise son compte Domain Admin pour se connecter en RDP sur un serveur applicatif afin de déployer une mise à jour. Ce serveur est compromis via une vulnérabilité applicative non patchée. L'attaquant dumpe les credentials en mémoire via Mimikatz — et récupère directement les credentials du Domain Admin. En 30 secondes, il possède l'ensemble du domaine Active Directory. Ce scénario trivial est la raison d'être du Tiering Model, qui aurait dans ce cas limité la compromission au seul niveau du serveur applicatif Tier 1.

Comme démontré dans nos analyses des attaques NTLM Relay sur Active Directory et des chemins d'attaque BloodHound, la compromission latérale dans un AD non-segmenté est triviale pour un attaquant disposant d'un simple pied de nez dans le réseau interne, même sans droits particuliers au départ.

Architecture du Tiering Model : les 3 niveaux en détail

Le modèle Microsoft Enterprise Access Model (anciennement ESAE, ou Red Forest) définit trois tiers d'administration, chacun correspondant à un périmètre de confiance distinct avec des actifs, des comptes et des postes d'administration propres. L'isolation entre ces trois niveaux est à la fois logique (GPO, groupes de sécurité) et physique (réseaux séparés, PAW dédiées).

Tier 0 : La Couronne Jewels — Contrôleurs de Domaine et Infrastructure d'Identité

Le Tier 0 représente les actifs les plus critiques de l'organisation, ceux dont la compromission entraîne la perte de contrôle totale et permanente du domaine Active Directory. Ce niveau comprend les contrôleurs de domaine (DC), les services AD FS (authentification fédérée), les services AD CS (Certificate Authority et PKI), Azure AD Connect (synchronisation identités hybrides), les solutions de gestion des identités privilégiées (PAM, PIM, CyberArk, Beyondtrust), les systèmes de sauvegarde des DC, et les serveurs DNS autoritaires intégrés à Active Directory.

Les comptes Tier 0 sont réservés exclusivement à l'administration de ces actifs. Ils ne doivent jamais être utilisés pour se connecter à un serveur Tier 1 ou Tier 2. Les comptes T0 typiques sont les membres de Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator Owners, et tout compte disposant de droits DCSync, de réplication AD, ou de l'accès aux clés de sauvegarde DSRM (Directory Services Restore Mode).

Tier 1 : Serveurs Applicatifs, Middleware et Infrastructure

Le Tier 1 englobe l'ensemble des serveurs membres du domaine hébergeant des applications et services métier, mais sans rôle d'infrastructure d'identité proprement dite. Ce niveau comprend les serveurs de fichiers et d'impression, les serveurs web et d'applications (IIS, Apache, JBoss), les serveurs de bases de données (SQL Server, Oracle, PostgreSQL), les serveurs Exchange et SharePoint, les serveurs de virtualisation (VMware vCenter, Hyper-V hosts, qui sont eux-mêmes Tier 0 si des DC y tournent), les serveurs de monitoring et de gestion (WSUS, SCCM, MECM, Ansible, Puppet), et les serveurs d'accès distant (VPN concentrators, Remote Desktop Services).

Les comptes Tier 1 peuvent administrer les serveurs T1 mais ne doivent jamais avoir de droits sur les actifs Tier 0. Si un compte T1 est compromis, l'attaquant peut impacter les applications métier et potentiellement accéder à des données sensibles, mais ne peut pas directement compromettre les contrôleurs de domaine.

Tier 2 : Postes de Travail, Appareils Mobiles et Utilisateurs Finaux

Le Tier 2 correspond aux postes de travail des utilisateurs finaux, aux laptops, aux appareils mobiles et aux environnements VDI. Ce niveau comprend les postes de travail Windows 10 et 11, les laptops et appareils BYOD gérés par MDM, les kiosques et terminaux industriels, les appareils mobiles sous gestion Intune, et les environnements VDI (Virtual Desktop Infrastructure). Les comptes Tier 2 (helpdesk niveau 1 et 2, support technique) peuvent gérer les postes utilisateurs mais n'ont aucun droit sur les serveurs Tier 1 ni sur les DC Tier 0.

Privileged Access Workstations (PAW) : les postes durcis par tier

Le concept de PAW est indissociable du Tiering Model. Sans PAW, les restrictions de comptes sont contournables si un administrateur Tier 0 utilise son compte T0 depuis un poste Tier 2 compromis. Une Privileged Access Workstation est un poste de travail physique ou virtuel dédié à l'administration d'un tier spécifique, durci selon les recommandations Microsoft et l'ANSSI, et isolé du réseau de production général.

Qu'est-ce qu'une PAW et pourquoi est-elle indispensable ?

L'idée fondamentale des PAW est simple : si un administrateur Tier 0 utilise son poste habituel, sur lequel il navigue sur Internet, lit ses emails professionnels et personnels, et gère ses applications quotidiennes, pour administrer les contrôleurs de domaine, ce poste constitue un vecteur de compromission majeur pour le Tier 0. Une PAW est un poste dont l'unique raison d'être est l'administration d'un périmètre défini et dont toute utilisation autre est techniquement impossible par configuration. Une PAW Tier 0 comprend une isolation réseau stricte via VLAN

dédié avec filtrage entrant et sortant ne laissant passer que les flux AD nécessaires, un OS Windows 11 Enterprise durci avec mises à jour forcées et AppLocker ou WDAC activé en mode whitelist, BitLocker avec TPM et PIN, Credential Guard et Device Guard activés, absence de navigateur grand public ou navigateur sandboxé en mode strict, et MFA obligatoire pour tout accès à la PAW elle-même.

PAW physiques vs PAW virtuelles : architecture recommandée

Deux architectures de PAW sont possibles, chacune avec ses avantages. Les PAW physiques dédiées offrent la meilleure isolation car l'hyperviseur potentiellement compromis ne peut pas intercepter les communications d'une machine physique, mais elles ont un coût plus élevé en acquisition et en gestion. Les PAW virtuelles, hébergées sur un hyperviseur dédié et isolé, sont plus flexibles et moins coûteuses, mais leur sécurité dépend entièrement de celle de l'hyperviseur qui doit lui-même être classé Tier 0 si des DC y tournent. Microsoft propose une architecture "PAW légère" via Windows Sandbox ou Microsoft Defender Application Guard pour les organisations ne pouvant pas déployer des PAW dédiées dans un premier temps.

Implémentation GPO : les restrictions d'authentification entre tiers

Le mécanisme technique central du Tiering Model est la restriction des authentifications via les objets de stratégie de groupe (GPO). Sans ces restrictions techniques, même avec des comptes séparés et des PAW dédiées, un administrateur Tier 0 pourrait délibérément ou par erreur utiliser son compte T0 sur une machine Tier 1, invalidant l'ensemble du modèle de sécurité.

Authentication Policy Silos : la solution moderne et recommandée

Introduits avec Windows Server 2012 R2 et le niveau fonctionnel de domaine correspondant, les Authentication Policy Silos permettent de définir de manière centralisée et cryptographiquement imposée quels comptes peuvent s'authentifier sur quelles machines. C'est la méthode la plus

robuste car elle est appliquée par le contrôleur de domaine lui-même plutôt que par une GPO qui pourrait être contournée localement.

```
 # PowerShell - Créer un Authentication Policy Silo pour Tier 0
New-ADAuthenticationPolicySilo -Name "Tier0AdminSilo" -Enforce $true

# Créer une Authentication Policy pour les comptes T0
New-ADAuthenticationPolicy -Name "Tier0Policy" `
  -UserAllowedToAuthenticateFrom "O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo ==
  -Enforce $true

# Assigner la politique au silo
Set-ADAuthenticationPolicySilo -Identity "Tier0AdminSilo" `
  -UserAuthenticationPolicy "Tier0Policy"

# Ajouter un compte admin T0 au silo
Add-ADAccountToAuthenticationPolicySilo -Identity "admin-tier0" `
  -AuthenticationPolicySilo "Tier0AdminSilo"
```

Approche GPO classique par groupes de sécurité

Pour les environnements sans niveau fonctionnel Windows Server 2012 R2 ou par préférence opérationnelle, les restrictions via les droits utilisateur dans les GPO fonctionnent efficacement. On crée des GPO liées aux OU contenant les machines de chaque tier, avec des droits "Deny log on locally", "Deny log on through Remote Desktop Services" et "Deny access to this computer from the network" appliqués aux groupes d'administration des tiers supérieurs. Ainsi, un compte Domain Admin du Tier 0 se verra refuser toute tentative de connexion sur une machine Tier 1 ou Tier 2 au niveau GPO, même s'il tente de le faire intentionnellement.

Structure OU recommandée pour le Tiering Model

La mise en œuvre technique du Tiering Model repose sur une structure d'Unités Organisationnelles (OU) reflétant les trois tiers et permettant l'application de GPO distinctes à

chaque couche. Voici la structure recommandée par Microsoft et l'ANSSI dans son guide de sécurisation Active Directory ANSSI-BP-028.

```
Domaine.local
├── Tier0
│   ├── Accounts          (comptes admins T0 dédiés)
│   ├── Groups            (groupes T0 : Domain Admins, etc.)
│   ├── Service Accounts  (comptes de service T0)
│   └── Devices           (PAW Tier 0)
├── Tier1
│   ├── Accounts          (comptes admins serveurs)
│   ├── Groups
│   ├── Service Accounts
│   ├── Devices           (PAW Tier 1)
│   └── Servers           (OU des serveurs membres)
├── Tier2
│   ├── Accounts          (comptes helpdesk et support T2)
│   ├── Groups
│   ├── Service Accounts
│   ├── Devices           (PAW Tier 2 et postes support)
│   └── Workstations      (OU des postes utilisateurs)
└── Users                 (comptes utilisateurs standards non-admins)
```

Cette structure OU permet d'appliquer des GPO distinctes à chaque tier et de déléguer les droits d'administration de manière granulaire. Les comptes de service doivent impérativement être classifiés dans le tier correspondant au système qu'ils administrent : un service account qui tourne sur un DC est automatiquement Tier 0, peu importe ses droits formels dans l'annuaire, car un attaquant compromettant le service pourrait rebondir vers les secrets du DC.

Implémentation pas à pas : migration vers le Tiering Model

La migration d'un environnement existant vers un Tiering Model est un projet structurant de plusieurs semaines à plusieurs mois selon la taille et la complexité de l'organisation. Voici la roadmap recommandée, compatible avec un environnement Active Directory standard d'entreprise.

Phase 1 : Audit et inventaire (semaines 1-2)

Avant de déployer quoi que ce soit, un inventaire complet et exhaustif est indispensable. Il faut lister tous les comptes à privilèges actuels (membres de Domain Admins, Enterprise Admins, Administrators locaux des DC), identifier tous les comptes de service et leurs droits AD réels vs droits formels, cartographier les chemins d'authentification existants pour déterminer quels comptes se connectent sur quelles machines, identifier les applications legacy nécessitant des droits élevés, et auditer la composition actuelle de l'infrastructure DC et des actifs Tier 0. L'outil BloodHound avec le collecteur SharpHound est particulièrement utile pour cette phase, en révélant les chemins de privilege escalation existants et les comptes non-classifiés disposant de droits Tier 0 sans que personne ne le sache.

Phase 2 : Création des OU, groupes et comptes dédiés (semaines 3-4)

Créer la structure OU décrite ci-dessus, puis pour chaque administrateur nécessitant des accès à plusieurs tiers, créer les comptes dédiés correspondants avec des mots de passe distincts gérés via un gestionnaire de mots de passe ou une solution PAM (CyberArk, Beyondtrust, Delinea). Définir une convention de nommage claire et appliquée uniformément : prenom.nom pour le compte utilisateur standard, prenom.nom-t1 pour le compte Tier 1, prenom.nom-t0 pour le compte Tier 0. Créer les groupes de sécurité PAW-Tier0-Admins, PAW-Tier1-Admins, PAW-Tier2-Admins qui serviront dans les GPO de restriction.

Phase 3 : Déploiement des GPO de restriction (semaines 5-6)

Tester chaque GPO en mode Audit avant l'application en mode Enforce pour identifier les éventuels blocages opérationnels. Les GPO prioritaires sont : Restrict-T0-Admins-From-T1-T2 (Deny logon pour PAW-Tier0-Admins sur toutes les machines non-Tier 0), Restrict-T1-T2-From-T0 (Deny logon pour PAW-Tier1-Admins et PAW-Tier2-Admins sur les DC), PAW-T0-Hardening (AppLocker, Credential Guard, réseau restreint sur PAW Tier 0), et Protected-Users-T0 (appliquer le groupe "Protected Users" de l'AD aux comptes Tier 0 pour bloquer NTLMv1, NTLMv2 et la délégation non-contrainte).

Phase 4 : Déploiement des PAW et formation des équipes (semaines 7-10)

Les PAW peuvent être déployées via SCCM, MECM ou Intune avec un profil de configuration durci et un script PowerShell d'initialisation. Microsoft fournit le PAW Deployment Guide officiel avec des scripts de configuration automatisée. La formation des équipes IT au changement d'habitudes opérationnelles est souvent la partie la plus difficile de cette phase — les administrateurs habitués à tout faire depuis un seul poste et un seul compte doivent adopter une discipline stricte de commutation entre leurs différents environnements d'administration.

Phase 5 : Validation continue par script PowerShell (semaine 11+)

Utiliser un script PowerShell d'audit AD automatisé pour valider régulièrement l'intégrité du Tiering Model. Ce script doit vérifier qu'aucun compte T0 n'apparaît dans les logs d'accès de machines T1 et T2, que la composition des groupes sensibles n'a pas été modifiée sans procédure de changement, que les PAW sont toujours dans les OU dédiées et appliquent bien les GPO de durcissement, et qu'aucun nouveau compte de service avec des droits T0 n'a été créé sans classification appropriée.

Tableau comparatif : Modèle plat vs Tiering Model

Critère de sécurité	Modèle plat (sans tiers)	Active Directory Tiering Model
Compromission d'un poste Tier 2	Accès Domain Admin si credentials en cache mémoire	Limité au Tier 2, aucune escalade vers Tier 0 possible
Compromission d'un serveur Tier 1	Accès potentiel à tous les actifs du domaine	Limité aux actifs Tier 1 uniquement
Attaque NTLM Relay depuis Tier 2	Relay vers DC possible, compromission domaine directe	Relay bloqué par restrictions d'authentification GPO
Pass-the-Hash depuis un poste Tier 2	Hash Domain Admin potentiellement en cache sur le poste	Aucun hash Tier 0 jamais stocké en cache sur machines T2
Détection Red Team	Compromission domaine en 10-30 minutes	Temps de compromission multiplié par 10 au minimum
Complexité opérationnelle	Faible (un seul compte admin par personne)	Élevée (2 à 3 comptes admin par personne selon les tiers)
Coût de déploiement	Nul (situation héritée)	Significatif (PAW, formation, migration sur plusieurs mois)
Conformité ANSSI BP-028	Non conforme	Conforme recommandation de niveau 1
Conformité CISA SCuBA	Non conforme	Conforme directives d'administration privilégiée

À RETENIR

À retenir : Active Directory Tiering Model 2026

3 tiers étanches : Tier 0 (DC et infrastructure d'identité) → Tier 1 (serveurs applicatifs) → Tier 2 (postes utilisateurs), avec comptes dédiés distincts pour chaque niveau

La règle absolue : un compte Tier 0 ne s'authentifie jamais sur une machine Tier 1 ou Tier 2 — les GPO de restriction et les Authentication Policy Silos imposent cela techniquement

PAW obligatoires pour l'administration Tier 0 : poste physique ou VM dédiée, isolée réseau, durcie selon les recommandations Microsoft

Authentication Policy Silos disponibles depuis Windows Server 2012 R2 : mécanisme le plus robuste car imposé par le DC, pas contournable par une GPO locale

Migration progressive : commencer par isoler le Tier 0 et créer les comptes dédiés, avant de déployer les PAW et les restrictions Tier 1 et Tier 2

BloodHound est indispensable pour l'audit initial : révèle les comptes implicitement Tier 0 et les chemins d'escalade non-documentés dans l'annuaire

Surveillance continue obligatoire : les Event ID 4624 sur les DC avec authentifications de comptes non-T0 constituent un signal d'alarme critique à monitorer en temps réel

Questions fréquentes sur l'Active Directory Tiering Model

Combien de comptes d'administration un administrateur doit-il avoir dans un Tiering Model ?

Dans un Tiering Model complet, chaque administrateur dispose d'autant de comptes dédiés que de tiers qu'il administre, plus son compte utilisateur standard pour la productivité quotidienne. Un administrateur ayant des responsabilités sur les DC (Tier 0) et les serveurs applicatifs (Tier 1) disposera de trois comptes distincts : prenom.nom pour la messagerie et la navigation, prenom.nom-t1 pour l'administration des serveurs Tier 1, et prenom.nom-t0 pour l'administration des contrôleurs de domaine. Ces trois comptes ont des mots de passe entièrement différents gérés idéalement via une solution PAM, sont stockés dans des OU distinctes, et les droits de chacun sont strictement limités à leur périmètre tier respectif. Il ne doit jamais exister de chemin permettant d'utiliser le compte T0 depuis un poste ou une session liée au périmètre T2.

Le Tiering Model est-il compatible avec un environnement Azure AD hybride ?

Oui, et Microsoft a précisément étendu le Tiering Model aux environnements hybrides dans son Enterprise Access Model de 2021. Dans un contexte hybride Azure AD Connect, le Tier 0 inclut à la fois les contrôleurs de domaine on-premises ET les rôles Azure AD les plus privilégiés (Global Administrator, Privileged Role Administrator, Security Administrator, le compte Azure AD Connect Sync Account). Les PAW Tier 0 doivent être en mesure d'administrer aussi bien les DC locaux que le portail Azure AD et Entra ID. Les comptes cloud-only membres de rôles Azure AD sensibles sont traités comme des identités Tier 0 même si elles n'ont pas d'équivalent on-premises. La gestion des identités Tier 0 hybrides dans Microsoft Entra PIM (Privileged Identity Management) avec activation just-in-time est la meilleure pratique recommandée pour 2026.

Quels sont les principaux pièges à éviter lors de la migration vers un Tiering Model ?

Les écueils les plus fréquents lors d'une migration vers le Tiering Model Active Directory sont au nombre de cinq. Premièrement, les comptes de service oubliés : des service accounts avec des droits excessifs découverts seulement après la mise en place des restrictions GPO, causant des pannes applicatives difficiles à diagnostiquer en urgence. Deuxièmement, les administrateurs qui contournent le modèle en utilisant leurs comptes T0 sur des machines T1 "juste une fois" par facilité, d'où l'importance des restrictions techniques plutôt que procédurales. Troisièmement, les applications legacy nécessitant des droits Domain Admin pour fonctionner, qui doivent être migrées, isolées dans un périmètre dédié, ou remplacées. Quatrièmement, les systèmes de sauvegarde des DC qui requièrent des droits T0 mais sont gérés depuis des serveurs T1 — le serveur de backup des DC doit impérativement être classé Tier 0. Cinquièmement, la formation insuffisante et l'accompagnement au changement des équipes IT, qui est souvent le facteur limitant principal d'un déploiement réussi.

Comment valider que le Tiering Model est correctement implémenté et maintenu dans la durée ?

La validation passe par plusieurs axes complémentaires et doit être un processus continu, pas un exercice ponctuel. En premier lieu, un test d'intrusion interne ciblé Red Team simulant une compromission d'un poste T2 ou d'un serveur T1 : si l'escalade vers T0 est possible, le modèle présente une brèche qui doit être corrigée immédiatement. En second lieu, un audit technique

BloodHound mensuel pour identifier les chemins de privilege escalation nouveaux créés par des changements de configuration non contrôlés. En troisième lieu, la vérification systématique des logs : les Event ID 4624 sur les DC ne doivent montrer aucune authentification de comptes non-T0 ; chaque exception doit déclencher une alerte et une investigation. Enfin, un script PowerShell d'audit automatisé hebdomadaire vérifiant la composition des groupes sensibles, les membres des Authentication Policy Silos, et l'application effective des GPO de restriction sur toutes les machines des trois tiers. Ce type de gouvernance continue s'inscrit dans une démarche globale de surveillance de la santé Active Directory par scripts automatisés.