Audit Active Directory : Méthode Complète et Outils Experts 2026

L'**audit Active Directory** est devenu l'une des missions de sécurité les plus critiques pour les organisations françaises. Active Directory (AD) est le cœur névralgique de l'infrastructure informatique de 95 % des entreprises : il gère les identités, les accès, les stratégies de groupe et les relations de confiance entre domaines. Quand il est compromis, c'est l'ensemble du système d'information qui tombe. Selon le rapport M-Trends 2025 de Mandiant, Active Directory est impliqué dans plus de 90 % des incidents de ransomware documentés. Les attaquants exploitent des vulnérabilités connues — délégations Kerberos non contraintes, templates ADCS mal configurés, ACLs permissives — pour escalader jusqu'à Domain Admin en quelques heures, parfois moins. Ce guide complet couvre la méthodologie d'un audit AD professionnel en 2026 : pourquoi l'audit est non négociable, les cinq piliers techniques à examiner, le comparatif des outils open source, une méthodologie en six étapes reproductibles, les spécificités PME, et les critères pour décider quand passer à un vrai pentest Active Directory.

Pourquoi auditer son Active Directory en 2026 ?

La surface d'attaque Active Directory n'a jamais été aussi large qu'en 2026. Trois tendances de fond expliquent cette explosion du risque :

L'héritage technique s'accumule

La plupart des AD en production ont entre 10 et 20 ans. Ils ont été déployés avec des configurations Windows Server 2003 ou 2008 jamais revues. Le schema AD est rétrocompatible par conception : une directive GPO créée sous Windows XP continue de s'appliquer aujourd'hui. Ce qui était acceptable en 2008 — délégation Kerberos non contrainte activée par défaut sur les

serveurs Exchange, comptes de service avec des mots de passe qui n'expirent jamais, templates ADCS copiés sans être sécurisés — est un vecteur d'attaque trivial en 2026.

Les attaques sur AD sont industrialisées

Des outils comme BloodHound ont démocratisé l'exploration des chemins d'attaque dans Active Directory. Ce qui nécessitait des semaines d'expertise manuelle se fait désormais en quelques minutes. Les groupes ransomware (LockBit, BlackCat, Cl0p) utilisent des playbooks standardisés : Kerberoasting → pass-the-hash → DCSync → déploiement masse. Sans audit régulier, ces chemins restent ouverts.

L'hybridation avec Entra ID crée de nouvelles surfaces

L'adoption massive de Microsoft 365 a conduit à des configurations hybrides où l'AD on-premises se synchronise avec Entra ID (Azure AD) via Azure AD Connect. Cette synchronisation crée des ponts d'escalade bidirectionnels : compromettre un compte synchronisé peut donner accès au tenant cloud, et inversement. Un audit AD en 2026 doit impérativement inclure le périmètre hybride.

La réglementation exige des preuves de contrôle

NIS 2 (transposée en France en 2024-2025), ISO 27001:2022 et SOC 2 exigent des contrôles d'accès documentés et testés. Un audit AD fournit la preuve concrète que les mesures de l'article 21 NIS 2 — gestion des accès, authentification forte, surveillance — sont effectivement appliquées. L'absence d'audit devient un risque de conformité autant qu'un risque technique.

Les 5 piliers d'un audit Active Directory complet

Un audit AD sérieux ne se limite pas à lancer PingCastle et lire le score. Il couvre cinq domaines techniques interdépendants :

1. Énumération des comptes et des privilèges

Le premier pilier cartographie qui a accès à quoi. Les questions clés : combien de comptes ont des droits Domain Admin ? Les comptes de service ont-ils des privilèges excessifs ? Des comptes orphelins (anciens employés, projets terminés) sont-ils toujours actifs ? Les indicateurs de risque typiques sont les comptes membres de Domain Admins sans justification documentée, les comptes avec AdminCount=1 hors des groupes protégés légitimes, et les comptes de service avec des droits d'administration locale sur des postes.

2. Analyse des ACLs et des délégations

Les Access Control Lists (ACLs) sur les objets Active Directory sont la source de la majorité des chemins d'escalade documentés par BloodHound. Un abus classique : un compte helpdesk avec le droit GenericWrite sur un compte admin peut modifier son attribut scriptPath et exécuter du code au prochain logon. Ces permissions s'accumulent au fil des ans, souvent par copie d'objets existants, sans nettoyage. L'audit manuel des ACLs sur les OUs sensibles (Domain Controllers, privileged accounts, GPO) est non négociable.

3. Configuration Kerberos et délégations

Trois configurations Kerberos à risque concentrent 60 % des chemins d'escalade observés en engagement :

Délégation non contrainte (Unconstrained Delegation) : tout service configuré avec cette option peut demander des tickets Kerberos au nom de n'importe quel utilisateur — y compris Domain Admins. Activer le monitor PrinterBug ou PetitPotam pour forcer l'authentification d'un DC permet l'extraction du TGT et le DCSync.

Délégation contrainte sans protection de protocole (S4U2Proxy) : exploitable pour l'usurpation d'identité si le compte service est compromis.

Kerberoasting : tout compte avec un SPN (Service Principal Name) peut être ciblé. Le TGS peut être cracké hors ligne. Les comptes de service avec des mots de passe anciens et faibles (<12 chars, non-complexes) tombent en quelques heures avec hashcat.

4. PKI et ADCS (Active Directory Certificate Services)

Le framework ESC (Enterprise Security Configuration) de SpecterOps a documenté 16 classes de vulnérabilités dans ADCS. Les trois plus fréquentes en audit :

ESC1 : template permettant à n'importe quel utilisateur authentifié de s'enregistrer et de spécifier un Subject Alternative Name arbitraire → impersonation de n'importe quel utilisateur, y compris Domain Admin

ESC4 : droits d'écriture sur un template ADCS → modification des propriétés pour déclencher ESC1

ESC8 : relay NTLM vers l'enrollment web ADCS → obtention d'un certificat de machine DC pour DCSync

Selon nos données d'engagement, 80 % des environnements en production ont au moins un template ADCS exploitable.

5. Group Policy Objects (GPO) et LAPS

Les GPO configurent la sécurité des postes et serveurs. L'audit vérifie : les scripts de démarrage ne contiennent pas de credentials en clair, les droits d'écriture sur les GPO sont restreints aux administrateurs légitimes, LAPS (Local Administrator Password Solution) est déployé et fonctionnel, les politiques de mot de passe sont conformes aux recommandations ANSSI (12 caractères minimum, complexité, durée de vie).

Outils d'audit Active Directory : comparatif 2026

Quatre outils open source couvrent l'essentiel d'un audit AD :

PingCastle — Score de risque instantané

PingCastle est l'outil d'entrée de gamme de l'audit AD. Il génère un rapport HTML avec un score de risque agrégé (0 = risque nul, 100 = risque maximum) et des findings classifiés par sévérité. Exécution :

```
PingCastle.exe --healthcheck --server dc01.domain.local --user auditeur --password "Audit2026!"
```

Output typique : score 65/100, finding critique "Unconstrained delegation enabled on 3 computers", finding high "Kerberoastable accounts: 12 with password older than 2 years". PingCastle est excellent pour un premier état des lieux rapide (30 minutes) mais ne remplace pas une analyse manuelle des chemins d'attaque. Il ne voit pas les ACLs custom ni les relations de confiance complexes.

BloodHound — Cartographie des chemins d'attaque

BloodHound est l'outil de référence pour visualiser les chemins d'escalade de privilèges dans Active Directory. La collection de données se fait avec SharpHound (Windows) ou BloodHound.py (Linux sans agent) :

```
# Collection depuis Linux
python3 bloodhound.py -u auditeur -p "Audit2026!" -d domain.local -dc dc01.domain.local -c All
```

Les requêtes Cypher pré-built identifient les chemins critiques : "Shortest path to Domain Admins", "Find Kerberoastable users with high-value targets in their path", "Find computers with Unconstrained Delegation". La version BloodHound CE (Community Edition) est gratuite et auto-hostable. BloodHound Enterprise ajoute la priorisation automatique et le suivi de remédiation.

Adalanche — Alternative open source

Adalanche (voir notre guide Adalanche) est une alternative à BloodHound entièrement open source. Il effectue la collecte et l'analyse sans dépendance Neo4j, avec une interface web intégrée. Particulièrement utile pour les environnements avec restrictions d'installation.

Certify / Certipy — Audit ADCS

Pour l'audit PKI/ADCS, Certipy (Python) est l'outil de référence :

```
certipy find -u auditeur@domain.local -p "Audit2026!" -dc-ip 192.168.1.1 -vulnerable -enabled
```

Il identifie automatiquement les templates ESC1 à ESC11 et génère un rapport avec le niveau de criticité. Voir aussi notre comparatif des 10 meilleurs outils d'audit AD.

Méthodologie d'audit Active Directory en 6 étapes

Étape 1 — Cadrage et préparation (J-7 à J-1)

Avant toute collecte, formalisez :

Convention d'audit signée par le responsable SI et la direction (obligation légale, art. 323-1 CP)

Périmètre exact : domaines, forêts, scope Entra ID inclus ou non

Fenêtre de maintenance ou règle de non-perturbation production

Compte d'audit fourni : utilisateur domain standard suffit pour la majorité des collectes

Contact d'urgence en cas de déclenchement d'alertes EDR

Étape 2 — Collecte passive (Jour 1, ~2h)

La collecte passive minimise l'impact sur le réseau. Lancez PingCastle depuis un poste joint au domaine, puis SharpHound avec la méthode DCOnly pour ne pas générer de trafic SMB massif vers les endpoints :

```
SharpHound.exe -c DCOnly --outputdirectory C:\audit\ --zipfilename bloodhound-passive.zip
```

DCOnly collecte les données de l'AD (comptes, groupes, ACLs, GPO) sans énumérer les sessions actives sur les postes — beaucoup moins bruyant.

Étape 3 — Collecte active (Jour 1, ~4h)

La collecte complète avec SharpHound All génère du bruit réseau mais donne une vue complète des sessions et des partages. Lancez-la en dehors des heures de pointe. Parallèlement, exécutez Certipy pour l'audit ADCS et collectez les exports LDAP pour l'analyse manuelle des ACLs :

```
ldapsearch -x -h dc01.domain.local -D "auditeur@domain.local" -w "Audit2026!" \
  -b "DC=domain,DC=local" "(objectClass=user)" \
  dn sAMAccountName userAccountControl adminCount memberOf pwdLastSet > users.ldif
```

Étape 4 — Analyse et identification des chemins critiques (Jour 2, ~6h)

Importez les données BloodHound dans Neo4j et exécutez les requêtes critiques. Analysez manuellement les ACLs sur les objets Tier 0 (DC, krbtgt, AdminSDHolder, ADCS Enterprise CA). Identifiez les comptes Kerberoastables avec des mots de passe anciens. Croisez les findings ADCS de Certipy avec les chemins BloodHound pour évaluer l'exploitabilité réelle. Voir notre guide PingCastle et BloodHound pour les requêtes Cypher à lancer en priorité.

Étape 5 — Validation et scoring (Jour 3, ~3h)

Priorisez les findings selon trois critères : facilité d'exploitation (compte domain standard suffit-il ?), impact (chemin direct vers Domain Admin ?), présence d'attaquants actifs (IoC détectés ?). Un finding ESC1 exploitable depuis n'importe quel compte authentifié est Critical. Un compte Kerberoastable avec mot de passe changé il y a 6 mois et complexe est Medium.

Étape 6 — Rapport et remédiation (Jour 4, ~4h)

Le rapport doit comporter :

Executive summary : score de risque global, top 3 findings critiques, impact business estimé

Findings techniques : description, preuve de concept (sans exploitation réelle), CVSS, recommandation, horizon de remédiation (immédiat / 30 jours / 90 jours)

Plan de remédiation priorisé : quick wins (désactiver LLMNR, activer SMB Signing), actions à moyen terme (migration gMSA, nettoyage ADCS), refonte à long terme (architecture Tier)

Annexes techniques : requêtes LDAP, exports BloodHound, rapport Certipy complet

---

Audit Active Directory pour PME : spécificités et budget

Les PME françaises font face à des contraintes spécifiques : budget limité, absence d'équipe sécurité dédiée, AD souvent administré par un généraliste. Ce contexte appelle une approche pragmatique.

Ce qu'un audit PME révèle systématiquement

Dans 9 engagements sur 10 en environnement PME (50 à 500 postes), nos auditeurs identifient :

Score PingCastle entre 55 et 75 sur 100

3 à 8 comptes avec délégation Kerberos non contrainte activée (héritage Exchange, serveurs d'impression)

1 à 3 templates ADCS exploitables (ESC1 ou ESC4)

10 à 30 comptes de service kerberoastables avec mots de passe anciens

LAPS absent ou déployé sur moins de 50 % du parc

GPO de sécurité basiques manquantes (pas de Credential Guard, LSASS Protection désactivée)

Tarifs d'un audit AD pour PME en 2026

Profil	Durée	Tarif HT
TPE/PME — 1 domaine, <200 postes	2–3 jours	2 000 – 3 500 €
PME — 1 domaine, 200–500 postes	3–5 jours	3 500 – 6 000 €
ETI — 2–3 domaines, 1 000–5 000 postes	5–8 jours	6 000 – 12 000 €
Audit + scope Entra ID hybride	+1–2 jours	+1 500 – 3 000 €

Ces tarifs incluent la collecte, l'analyse, le rapport détaillé et une session de restitution. Un audit trimestriel automatisé (PingCastle en self-service + revue mensuelle) peut compléter l'audit annuel approfondi pour maîtriser les coûts. Consultez aussi notre guide sur l'audit AD automatisé par agent IA pour les approches de monitoring continu.

Priorisation des remédiations pour PME

Si le budget de remédiation est contraint, concentrez-vous sur les quick wins qui neutralisent 60 % des vecteurs d'attaque courants :

Désactiver LLMNR et NBT-NS sur tous les postes (GPO, 30 min de travail)

Activer SMB Signing obligatoire sur tous les serveurs (GPO)

Supprimer les délégations Kerberos non contraintes sur les serveurs non-DC

Déployer LAPS sur tous les postes Windows

Désactiver ou sécuriser les templates ADCS vulnérables (ESC1 : désactiver l'enrollment pour "Authenticated Users")

Ces cinq actions prennent 2 à 3 jours de travail et éliminent les vecteurs exploités dans 80 % des compromissions PME documentées.

Quand faire un pentest Active Directory plutôt qu'un simple audit ?

La distinction est fondamentale : l'audit cartographie et évalue les vulnérabilités sans les exploiter. Le pentest Active Directory va jusqu'à la démonstration de compromission : DCSync réel, Golden Ticket émis, mouvement latéral documenté avec captures d'écran. Les deux missions sont complémentaires, pas substituables.

Choisissez l'audit AD quand :

Vous voulez un état des lieux de la surface d'attaque sans risque de perturbation

Vous avez un budget contenu (l'audit est moins coûteux qu'un pentest)

Vous devez répondre à une exigence de conformité (ISO 27001, NIS 2) nécessitant une documentation des contrôles

Vous souhaitez établir une baseline avant de lancer un programme de remédiation

C'est votre première démarche sécurité AD — l'audit donne la roadmap

Passez au pentest AD quand :

Vous avez déjà appliqué les recommandations d'un audit précédent et voulez tester l'efficacité des contrôles

Votre direction exige une preuve concrète de compromission pour justifier un budget sécurité

Vous êtes OIV ou OSE et devez démontrer la résistance aux attaques ciblées

Vous venez de subir un incident ou soupçonnez une compromission en cours

Vous préparez une migration vers Azure ou un projet de fusion/acquisition

À RETENIR

Un pentest AD inclut systématiquement une phase d'audit préalable. Si vous n'avez jamais audité votre AD, commencez par l'audit, appliquez les corrections évidentes, puis commandez le pentest pour valider la résistance résiduelle.

Prêt à passer à l'action ?

Nos experts certifiés (OSCP, CRTO, CRTE) réalisent audits et pentests Active Directory pour PME et ETI françaises. Rapport détaillé, session de restitution incluse, devis sous 24h.

Découvrir notre offre de pentest Active Directory →

FAQ — Questions fréquentes sur l'audit Active Directory

Quelle est la différence entre un audit AD et un pentest AD ?

L'audit AD identifie et documente les vulnérabilités sans les exploiter : il cartographie les chemins d'attaque potentiels, analyse les configurations à risque et produit un rapport de recommandations. Le pentest AD va plus loin : il démontre l'exploitabilité réelle en réalisant les attaques (Kerberoasting, DCSync, mouvement latéral) dans un cadre contractuel. L'audit est un diagnostic ; le pentest est un test de résistance. Pour une première démarche, commencez par l'audit.

Combien coûte un audit Active Directory pour une PME ?

Entre 2 000 et 6 000 € HT pour une PME de moins de 500 postes avec un domaine unique, selon la profondeur de l'analyse et l'inclusion ou non du périmètre Entra ID. Comptez 3–5 jours de travail effectif. Une ETI avec plusieurs domaines sera entre 6 000 et 12 000 € HT. Ces tarifs incluent rapport écrit et session de restitution.

PingCastle est-il suffisant pour auditer Active Directory ?

PingCastle est un excellent point de départ pour un état des lieux rapide (score de risque, findings classifiés). Mais il ne voit pas les chemins d'attaque complexes (ACLs custom, chemins BloodHound multi-sauts), ne couvre pas ADCS/PKI et ne peut pas analyser les sessions actives. Pour un audit complet, PingCastle doit être complété par BloodHound/Adalanche pour les chemins d'escalade et Certipy pour ADCS. Un auditeur humain reste indispensable pour l'interprétation contextuelle des findings.

À quelle fréquence auditer son Active Directory ?

Minimum une fois par an pour un audit approfondi. En complément, un scan PingCastle mensuel ou trimestriel permet de détecter les régressions entre deux audits (nouveaux comptes admin créés, délégations ajoutées, score PingCastle qui se dégrade). Les événements déclencheurs d'un audit ponctuel : départ d'un administrateur AD, projet de migration (Exchange, Azure AD Connect), incident de sécurité, fusion/acquisition.

Quels sont les signes qu'un Active Directory a été compromis ?

Les indicateurs les plus fiables : présence de tickets Kerberos avec durée de vie anormale (Golden Ticket = 10 ans), comptes créés en dehors des fenêtres de maintenance habituelles, accès au partage SYSVOL depuis des comptes non-admin, augmentation brutale des réplications DRS (signe de DCSync), événements 4769 en masse sur le DC (Kerberoasting en cours), event 4662 avec droits DS-Replication-Get-Changes sur des comptes non-DC. Si vous observez ces signaux, passez en mode incident response plutôt qu'audit.

Durcissement Active Directory post-audit : les actions prioritaires

L'audit sans remédiation n'a aucune valeur. Voici les actions de durcissement les plus impactantes, classées par horizon :

Actions immédiates (0 à 7 jours)

Désactiver les protocoles d'authentification obsolètes : NTLM v1, LM Hash et NTLMv2 sans restriction amplifient le risque de relay. Configurez les GPO Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options pour désactiver LM Hash et forcer NTLMv2 minimum. En parallèle, activez SMB Signing obligatoire sur les serveurs pour neutraliser les attaques de relay (Responder, NTLM relay via ADCS ESC8).

Sécuriser les comptes Tier 0 : Les comptes Domain Admin, Enterprise Admin et BUILTIN\Administrators ne doivent jamais être utilisés pour des tâches quotidiennes. Chaque compte Tier 0 doit avoir un mot de passe unique, généré aléatoirement (minimum 25 caractères), stocké dans un gestionnaire de secrets (CyberArk, HashiCorp Vault, ou au minimum BitWarden Enterprise). Activez Protected Users sur tous les comptes Tier 0 pour interdire les authentifications NTLM, Kerberos DES/RC4 et la délégation.

Actions à 30 jours

Migrer les comptes de service vers des gMSA : Les group Managed Service Accounts (gMSA) éliminent les mots de passe statiques des comptes de service. Windows gère automatiquement la rotation (tous les 30 jours par défaut). Plus de compte kerberoastable avec un mot de passe de 2015. La migration d'un service vers gMSA prend 30 minutes. Priorisez les services exposés (IIS, SQL Server, Exchange).

Corriger les templates ADCS : Pour chaque template ESC1 identifié, retirez le droit d'enrollment pour "Authenticated Users" ou "Domain Users" et remplacez-le par un groupe AD spécifique (ex : "PKI-Certificate-Enrollment-AppXYZ"). Auditez le "Manager Approval" et activez-le sur les templates permettant l'SAN arbitraire.

Actions à 90 jours

Implémenter le modèle en niveaux (Tier Model) : La recommandation fondamentale de Microsoft et de l'ANSSI est de segmenter l'administration AD en trois tiers : Tier 0 (contrôleurs de domaine, ADCS), Tier 1 (serveurs membres), Tier 2 (postes utilisateurs). Un compte Tier 2 ne

doit jamais pouvoir accéder à un système Tier 0. Cette segmentation se met en place via des GPO de restriction de connexion et des Authentication Policies/Silos Kerberos.

Ressources complémentaires

Guide méthodologique complet du pentest Active Directory (29 000 mots)

Top 10 des outils d'audit Active Directory

Audit AD avec PingCastle et BloodHound : guide pas à pas

Guide ANSSI — Recommandations de sécurité Active Directory

