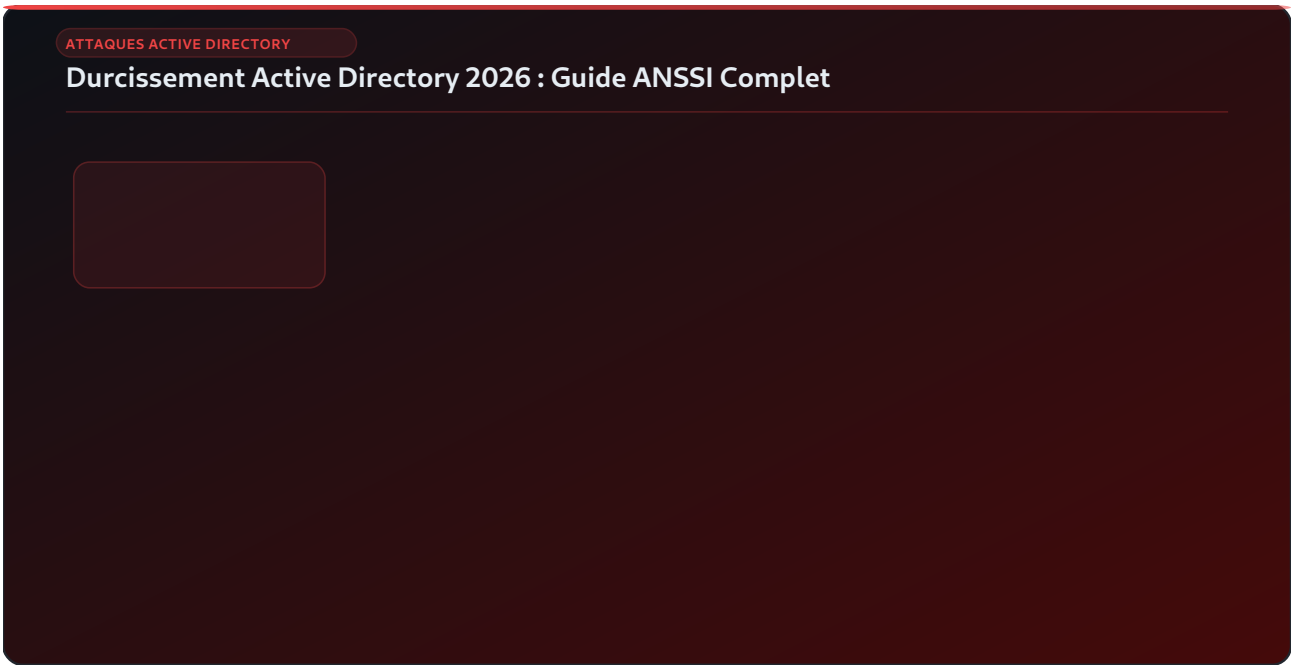
Durcissement Active Directory 2026 : Guide Complet ANSSI et Bonnes Pratiques

Guide complet de durcissement Active Directory 2026 : Tiering, LAPS v2, SMB Signing, désactivation RC4, ADCS hardening et recommandations ANSSI pour NIS 2.

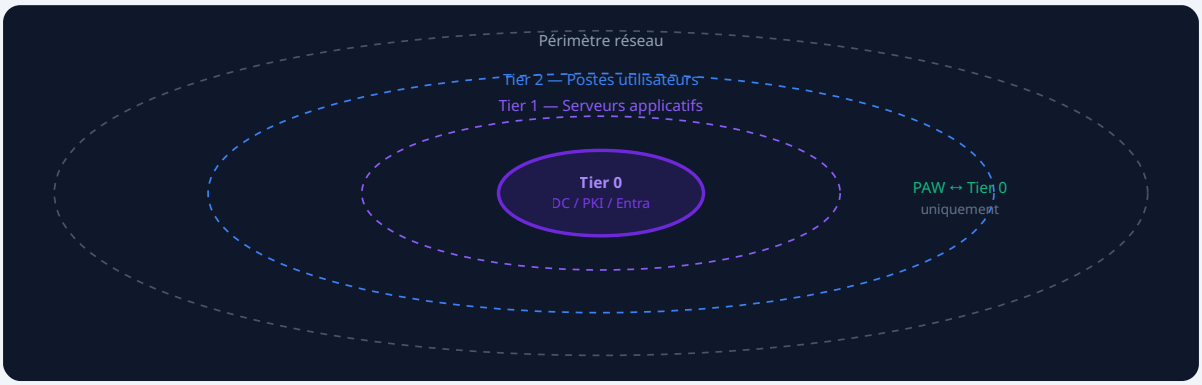
Le durcissement d'Active Directory reste en 2026 l'un des investissements sécurité les plus rentables qu'une organisation puisse réaliser. En tant que colonne vertébrale de l'authentification pour la quasi-totalité des entreprises françaises qui utilisent l'écosystème Microsoft, l'AD est systématiquement ciblé dans les phases post-exploitation de toute compromission sérieuse. L'ANSSI l'affirme sans ambiguïté dans son guide "Recommandations de sécurité pour Active Directory" : un AD mal configuré est un passe-partout pour l'ensemble du système d'information. Notre équipe a conduit plus de quarante audits AD en 2025-2026 pour des organisations françaises allant de la PME au grand groupe du CAC 40, et le constat est uniforme — les configurations par défaut de Windows Server, même récentes, laissent une surface d'attaque considérable que les attaquants exploitent de façon quasi-mécanique. Ce guide compile les mesures de durcissement les plus impactantes, priorisées selon leur efficacité observée en conditions réelles et leur compatibilité avec les exigences NIS 2, ISO 27001:2022 et les référentiels ANSSI. Chaque mesure est accompagnée de son impact opérationnel réel, car la sécurité sans exploitabilité terrain n'est que théorie : un durcissement qui bloque la production sera contourné par les équipes dans les semaines qui suivent, laissant l'organisation moins sécurisée qu'avant l'intervention.



Malgré des années de sensibilisation, les grandes attaques ransomware de 2025-2026 continuent de passer systématiquement par une compromission AD. Les groupes ALPHV/BlackCat, LockBit 4.0, et les nouveaux entrants comme RansomHub utilisent tous des techniques AD documentées : Kerberoasting, Pass-the-Hash, DCSync, Golden Ticket. La raison est simple : un AD compromis donne accès à tout le reste — messagerie, applications métier, backups, infrastructure cloud hybride. Durcir l'AD, c'est réduire la probabilité qu'une compromission initiale (phishing, exploitation de vulnérabilité) devienne une compromission totale du SI.

L'ANSSI a publié en 2024 une mise à jour majeure de ses recommandations AD intégrant les nouvelles techniques d'attaque comme **BadSuccessor**, **Shadow Credentials**, et les abus de **ADCS (Active Directory Certificate Services)**. Ces recommandations servent de base au référentiel de cet article et constituent le standard attendu lors d'audits de conformité NIS 2 pour les Opérateurs de Services Essentiels (OSE) et Fournisseurs de Services Numériques (FSN).

Architecture de défense AD en profondeur



Mesure 1 : Mise en Place du Modèle de Tiering AD

Le **modèle de tiering Active Directory** (Tier 0, Tier 1, Tier 2) est la mesure de durcissement architecturale la plus impactante disponible. Son principe : les administrateurs de Tier 0 (contrôleurs de domaine, PKI, ADFS, Entra Connect) ne doivent jamais s'authentifier sur des machines de Tier 1 (serveurs applicatifs) ou Tier 2 (postes utilisateurs), et réciproquement. Cette séparation empêche le mouvement latéral classique où un compte admin compromis sur un serveur de Tier 1 permet d'escalader vers les DC.

⚡ **Retour terrain**

Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles

(adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

La mise en œuvre technique passe par des *Authentication Policy Silos* (APS) dans Windows Server 2016+, qui permettent de restreindre cryptographiquement les comptes Tier 0 pour ne s'authentifier que sur des machines Tier 0. Ces silos sont complémentés par des GPO qui bloquent la connexion interactive des comptes Tier 0 sur des machines non-Tier 0. Le groupe **Protected Users** est activé pour tous les comptes Tier 0, désactivant RC4, DES, credential caching et délégations non contraintes.

```
 # Creer un Authentication Policy Silo pour Tier 0
New-ADAuthenticationPolicySilo -Name "Tier0-Silo" -Description "Silo Tier 0 - Comptes et ma
New-ADAuthenticationPolicy -Name "Tier0-User-Policy" -Description "Politique auth comptes T
    -UserAllowedToAuthenticateFrom "(Member of Tier0-Machines-Group)" `
    -Enforce

# Associer la politique au silo
Grant-ADAuthenticationPolicySiloAccess -Identity "Tier0-Silo" -Account "Tier0-User-Policy"

# Activer Protected Users pour comptes Tier 0
Get-ADGroupMember -Identity "Domain Admins" | ForEach-Object {
    Add-ADGroupMember -Identity "Protected Users" -Members $_
    Write-Host "Protected Users: $($_.SamAccountName)"
}
```

Mesure 2 : Durcissement Kerberos — Désactivation RC4 et Activation AES256

Kerberos est le protocole d'authentification central d'Active Directory, et sa configuration par défaut reste trop permissive en 2026. Le chiffrement RC4 (ARCFOUR), encore activé par défaut dans de nombreux environnements pour des raisons de compatibilité, est la cible principale des attaques **Kerberoasting** et **AS-REP Roasting** : les tickets chiffrés en RC4 se cassent en quelques heures avec Hashcat sur GPU, là où AES256 résisterait des siècles au même matériel.

La désactivation de RC4 dans Kerberos s'effectue via GPO (Computer Configuration → Windows Settings → Security Settings → Security Options → Network security: Configure encryption types allowed for Kerberos). Cependant, avant de désactiver RC4, il faut impérativement identifier les comptes de service et applications qui l'utilisent encore, au risque de casser l'authentification de systèmes critiques. L'outil `Get-ADUser -Filter {msDS-SupportedEncryptionTypes -band 4}` liste les comptes qui requièrent encore RC4.

```
 # Identifier les comptes utilisant encore RC4
# RC4 = bit 4 dans msDS-SupportedEncryptionTypes
Get-ADUser -Filter * -Properties msDS-SupportedEncryptionTypes,ServicePrincipalName |
    Where-Object {$_.'msDS-SupportedEncryptionTypes' -band 4 -or -not $_.'msDS-SupportedEnc
    Select-Object SamAccountName, ServicePrincipalName, 'msDS-SupportedEncryptionTypes' |
    Export-Csv /tmp/comptes-rc4.csv -NoTypeInformation

# Forcer AES256 sur un compte de service
Set-ADUser -Identity "svc-sqlprod" -KerberosEncryptionType AES256

# Ou via le parametre msDS-SupportedEncryptionTypes (24 = AES128+AES256)
Set-ADUser -Identity "svc-sqlprod" -Replace @{'msDS-SupportedEncryptionTypes'=24}
```

Mesure 3 : Éliminer les SPN sur les Comptes Utilisateurs (Anti-Kerberoasting)

Le Kerberoasting exploite le fait que tout utilisateur authentifié peut demander un ticket de service (TGS) pour n'importe quel SPN (Service Principal Name) enregistré dans l'AD, et ce ticket est chiffré avec le hash NT du mot de passe du compte associé au SPN. Si des comptes utilisateurs ont des SPN enregistrés (une mauvaise pratique hélas répandue), leurs tickets sont récupérables et cassables hors-ligne. La bonne pratique est de n'enregistrer des SPN que sur des *Managed Service Accounts (MSA)* ou *Group Managed Service Accounts (gMSA)*, dont les mots de passe de 240 caractères aléatoires sont gérés automatiquement par Windows et impossibles à casser.

La migration des comptes de service classiques vers des gMSA est une opération qui demande un inventaire préalable des applications utilisant ces comptes. Les gMSA sont supportés par la quasi-totalité des services Windows depuis Server 2012 R2, mais certaines applications tierces

nécessitent une configuration spécifique. L'investissement en temps est rentabilisé à chaque audit de sécurité : les auditeurs ciblent en priorité les SPN sur comptes utilisateurs, et leur absence change radicalement le profil de risque Kerberoasting.

```
 # Lister tous les SPNs sur comptes utilisateurs (cibles Kerberoasting)
Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName,Pass
    Select-Object SamAccountName, ServicePrincipalName, PasswordLastSet |
    Sort-Object PasswordLastSet

# Creer un gMSA en remplacement
New-ADServiceAccount -Name "gMSA-SqlProd" -DNSHostName "sqlprod.domain.local" `
    -PrincipalsAllowedToRetrieveManagedPassword "SQL-Servers-Group" `
    -ManagedPasswordIntervalInDays 30 `
    -KerberosEncryptionType AES256

# Tester sur le serveur cible
Test-ADServiceAccount -Identity gMSA-SqlProd
Install-ADServiceAccount -Identity gMSA-SqlProd
```

Mesure 4 : SMB Signing Obligatoire sur Tous les Systèmes

Le **SMB Signing** (signature des paquets SMB) est la défense principale contre les attaques NTLM Relay, où un attaquant intercepte une authentification NTLM et la relaie vers un autre serveur. Sans SMB Signing, cette attaque est triviale avec Responder + ntlmrelayx. La configuration par défaut de Windows Server active le SMB Signing sur les DC mais pas sur les serveurs membres ni les postes de travail, laissant la très grande majorité du parc exposé.

L'activation du SMB Signing mandatory sur l'ensemble du parc via GPO est une mesure de durcissement de premier ordre. L'impact opérationnel est minimal sur les environnements modernes (Windows 10+, Server 2016+) car SMB 3.1.1 gère la signature avec un impact performances négligeable (<1%). Sur les systèmes plus anciens avec SMB 1 ou 2, l'impact peut être plus marqué, mais ces systèmes devraient être migrés ou isolés de toute façon.

Mesure de durcissement	Risque neutralisé	Complexité	Impact ops
SMB Signing mandatory	NTLM Relay SMB	Faible (GPO)	Négligeable
LDAP Signing + Channel Binding	NTLM Relay LDAP	Faible	Faible
Désactivation RC4 Kerberos	Kerberoasting rapide	Moyenne	Moyen (compatibilité)
Tiering Model + Auth Silos	Lateral movement	Élevée	Élevé (formation)
Protected Users activé	Pass-the-Hash, délégation	Faible	Faible
Migration gMSA	Kerberoasting SPN users	Moyenne	Moyen (migration apps)
LAPS v2 déployé	Pass-the-Hash local admin	Faible	Faible
Désactivation LLMNR/NetBIOS	Responder poisoning	Faible	Négligeable

Mesure 5 : LDAP Signing et Channel Binding Token (CBT)

Parallèlement au SMB Signing, le **LDAP Signing** et le **Channel Binding Token (CBT)** sur les DC protègent contre les attaques NTLM Relay LDAP, utilisées notamment pour modifier des attributs AD sensibles comme `msDS-KeyCredentialLink` (Shadow Credentials) ou `msDS-AllowedToActOnBehalfOfOtherIdentity` (RBCD). Sans LDAP Signing, un attaquant peut relayer une authentification NTLM vers un DC LDAP et effectuer des modifications AD avec les droits du compte relayé.

La mise en œuvre est simple via GPO (Domain Controller Security Policy → LDAP server signing requirements → Require signing) mais nécessite de vérifier préalablement l'absence d'applications utilisant LDAP sans signing — ces applications doivent être migrées vers LDAPS ou configurées pour utiliser LDAP signing avant l'activation mandatory. L'ANSSI classe LDAP Signing comme mesure de durcissement de "priorité 1" dans ses recommandations AD 2024.

Mesure 6 : LAPS v2 — Randomisation des Mots de Passe Administrateurs Locaux

Le **Windows LAPS v2** (Local Administrator Password Solution), intégré nativement dans Windows Server 2022/2025 et Windows 11, résout le problème critique des mots de passe d'administrateur local identiques sur tous les postes — source de propagation massive du **Pass-the-Hash** dans les environnements traditionnels. Avec LAPS v2, chaque poste dispose d'un mot de passe administrateur local unique, généré aléatoirement, stocké chiffré dans AD ou Entra ID, et renouvelé automatiquement selon une politique configurable.

LAPS v2 apporte des améliorations significatives par rapport au LAPS v1 legacy : chiffrement du mot de passe dans AD (plus de stockage en clair), support de l'historique des mots de passe, intégration native sans agent supplémentaire, et support des comptes DSRM (Directory Services Restore Mode). Le déploiement se fait entièrement via GPO sur les environnements Windows 11 23H2+ et Server 2022/2025. Pour les systèmes plus anciens, LAPS v1 reste disponible mais l'objectif doit être la migration vers LAPS v2.

```
 # Configurer LAPS v2 via GPO (PowerShell)
# Prerequis: schema AD etendu pour LAPS v2
Update-LapsADSchema

# Definir les permissions sur les OUs
Set-LapsADComputerSelfPermission -Identity "OU=Workstations,DC=domain,DC=local"
Set-LapsADComputerSelfPermission -Identity "OU=Servers,DC=domain,DC=local"

# Permettre aux admins de lire les mots de passe
Set-LapsADReadPasswordPermission -Identity "OU=Workstations,DC=domain,DC=local" -AllowedPri
Set-LapsADReadPasswordPermission -Identity "OU=Servers,DC=domain,DC=local" -AllowedPrincipa

# Lire le mot de passe LAPS d'une machine
Get-LapsADPassword -Identity "PC-JOHN01" -AsPlainText
```

Mesure 7 : Désactivation de LLMNR et NetBIOS-ns

Les protocoles **LLMNR (Link-Local Multicast Name Resolution)** et **NetBIOS Name Service** sont des protocoles de résolution de noms hérités qui permettent l'empoisonnement de résolution par un attaquant sur le réseau local avec des outils comme Responder. Quand un poste Windows tente de résoudre un nom d'hôte qui n'existe pas dans DNS, il envoie une requête LLMNR/NetBIOS en broadcast — l'attaquant répond à sa place et capture le hash NTLM de l'authentification qui suit. Cette technique est triviale à mettre en œuvre et fonctionne sur tous les réseaux d'entreprise par défaut.

La désactivation de LLMNR et NetBIOS via GPO est une mesure à impact opérationnel quasi-nul dans les environnements avec DNS correctement configuré. Les seuls cas d'usage légitimes de LLMNR concernent des environnements domestiques ou de très petites structures sans DNS centralisé — des cas qui ne s'appliquent pas aux organisations ciblées par ce guide.

Pour LLMNR : Computer Configuration → Administrative Templates → Network → DNS Client → Turn Off Multicast Name Resolution → Enabled. Pour NetBIOS : via les paramètres avancés TCP/IP sur chaque interface (DHCP option 001 pour désactiver NetBIOS via DHCP option server, ou script PowerShell déployé via GPO). La combinaison LLMNR désactivé + NetBIOS désactivé + DNS bien configuré neutralise complètement Responder dans sa capacité à empoisonner les résolutions et capturer des authentifications NTLM sans interaction de l'attaquant au-delà de l'outil en écoute.

Mesure 8 : Audit et Revue des ACL Active Directory

Les **Access Control Lists (ACL)** Active Directory sont le talon d'Achille de nombreux environnements. Chaque objet AD (utilisateur, groupe, OU, GPO) possède une ACL définissant qui peut le lire, le modifier, ou lui déléguer des actions. Au fil des années, les ACL s'accumulent — délégations ponctuelles jamais nettoyées, droits octroyés lors d'un projet jamais révoqués, héritage mal maîtrisé. Des outils comme **BloodHound** et **PingCastle** exploitent exactement ces

ACL mal configurées pour identifier des chemins d'escalade de privilèges que l'administrateur AD ne soupçonne pas.

Notre anecdote terrain : lors d'un audit pour une ETI industrielle normande, PingCastle a révélé qu'un groupe "HelpDesk-IT" bénéficiait d'un droit `GenericWrite` sur l'objet du groupe "Domain Admins" — une délégation réalisée cinq ans plus tôt par un administrateur qui avait depuis quitté l'organisation, pour une raison inconnue de tous. Ce droit permettait à n'importe quel membre du helpdesk de s'ajouter aux Domain Admins sans intervention supplémentaire. La découverte n'était pas due à une technique sophistiquée, mais à l'absence de revue régulière des ACL.

```
 # Audit des ACL dangereuses sur les groupes privilegies
Import-Module ActiveDirectory

$dangerousRights = @("GenericWrite","GenericAll","WriteProperty","WriteDacl","WriteOwner","
$sensitiveGroups = @("Domain Admins","Enterprise Admins","Schema Admins","Group Policy Crea

foreach ($group in $sensitiveGroups) {
    $dn = (Get-ADGroup $group).DistinguishedName
    $acl = Get-Acl -Path "AD:\$dn"
    $acl.Access | Where-Object {
        $_.ActiveDirectoryRights -in $dangerousRights -and
        $_.IdentityReference -notmatch "^(NT AUTHORITY|BUILTIN|Domain Admins|Enterprise Adm
    } | ForEach-Object {
        Write-Warning "ACL RISQUE sur $group : $($_.IdentityReference) -> $($_.ActiveDirect
    }
}
```

Mesure 9 : Sécurisation des GPO et SYSVOL

Les **Group Policy Objects (GPO)** sont un vecteur d'attaque critique souvent négligé dans les audits AD. Une GPO mal sécurisée peut être modifiée par un attaquant pour déployer des scripts malveillants sur tout le parc ou créer des tâches planifiées backdoor. Les vulnérabilités les plus fréquentes concernent les GPO avec des droits d'écriture accordés à des comptes non-admin, les mots de passe dans les préférences GPO (Passwords in GPP — une pratique obsolète mais

encore présente dans certains environnements anciens), et les scripts de démarrage/connexion dans SYSVOL sans protection d'intégrité.

La protection du SYSVOL passe par l'activation de **DFSR (DFS Replication)** à la place de l'ancienne réplication FRS (obsolète depuis Server 2008 R2), et par la vérification que les permissions NTFS sur SYSVOL empêchent l'écriture par des comptes non-admins. Les GPP Passwords (présences dans les fichiers XML de SYSVOL) doivent être identifiées et supprimées — elles peuvent contenir des mots de passe chiffrés avec une clé publiquement connue depuis 2014.

Mesure 10 : Déploiement de Microsoft Defender for Identity (MDI)

Microsoft Defender for Identity (MDI), anciennement Azure ATP, est l'outil de détection dédié aux attaques AD. Déployé comme agent sur les DC, il analyse le trafic Kerberos, NTLM, LDAP et RPC en temps réel pour détecter les patterns d'attaque : Kerberoasting, DCSync, Pass-the-Hash, Golden Ticket, NTLM Relay, Reconnaissance LDAP. MDI est désormais intégré dans Microsoft Defender XDR et corrèle ses alertes avec les signaux Defender for Endpoint pour offrir une vision unifiée des incidents.

Pour les organisations sans budget Microsoft E5, les alternatives open source incluent **Zeek** + **Sigma** rules sur les logs AD, ou **Adalanche** pour l'analyse des chemins d'attaque. La configuration des logs Windows est un prérequis incontournable : les événements 4624 (logon), 4625 (échec logon), 4648 (explicit credential logon), 4662 (accès objet AD), 4740 (compte bloqué), et 5136 (modification objet AD) doivent être collectés et centralisés dans un SIEM.

Mesure 10b : Sigma Rules pour la Détection des Attaques AD

La mise en place de règles de détection dans le SIEM est le complément indispensable des mesures de durcissement préventif. Sans visibilité sur ce qui se passe dans l'AD, le défenseur est

aveugle même si les mesures de durcissement retardent l'attaquant. Les règles Sigma suivantes couvrent les techniques d'attaque AD les plus fréquentes et sont compatibles avec Elastic SIEM, Splunk, Microsoft Sentinel, et la plupart des SIEM du marché via le convertisseur sigma-cli.

```yaml
 # Sigma rule : Detection Kerberoasting
title: Kerberoasting - Service Ticket Request RC4
id: d8a9b28f-3c1e-4a2b-9f8c-6d7e5b4a3c2d
status: stable
description: Detect Kerberoasting via TGS requests with RC4 encryption (downgrade attack)
references:
  - https://attack.mitre.org/techniques/T1558/003/
tags:
  - attack.credential_access
  - attack.t1558.003
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4769
    TicketEncryptionType: '0x17'  # RC4-HMAC
    ServiceName|endswith: '$'
    ServiceName|contains|all:
      - krbtgt
  filter:
    AccountName|endswith: '$'
  condition: selection and not filter
falsepositives:
  - Legacy applications using RC4 Kerberos
level: high

---
# Sigma rule : DCSync Detection
title: DCSync - Replication Rights Used by Non-DC Account
id: b76d0a9e-4f2c-8b1d-3e7a-5c9f2d8b1e4a
status: stable
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4662
    Properties|contains:
      - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2'  # DS-Replication-Get-Changes
      - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2'  # DS-Replication-Get-Changes-All
  filter_dc:
    SubjectUserName|endswith: '$'
```

```
  condition: selection and not filter_dc
level: critical
```

Désactivation de l'Impression Spooler sur les DC (PrinterBug)

Le service **Print Spooler** sur les contrôleurs de domaine est le vecteur de la technique PrinterBug (aussi appelée MS-RPRN abuse), qui force une authentification NTLM entrante depuis un DC vers une machine contrôlée par l'attaquant. Cette authentification peut ensuite être relayée pour obtenir un TGT du DC (via NTLM relay vers LDAP avec délégation non contrainte) ou utilisée avec NTLM relay vers ADCS pour un ESC8. Le service Print Spooler est inutile sur un DC dans la très grande majorité des environnements d'entreprise : il n'y a aucune raison d'imprimer depuis un contrôleur de domaine.

La désactivation du Print Spooler sur les DC se fait via GPO (Computer Configuration → Windows Settings → System Services → Print Spooler → Disabled) ou PowerShell. C'est l'une des mesures les plus rapides à déployer avec un impact opérationnel nul sur les environnements où les DC ne gèrent pas directement des files d'impression (le cas standard dans les architectures modernes avec des serveurs d'impression dédiés). Le CERT-FR recommande explicitement cette désactivation depuis 2021 et son maintien en 2026 reste valide car des outils publics comme **printerbug.py** et **SpoolSample** continuent d'être intégrés dans les boîtes à outils des attaquants pour leur fiabilité éprouvée dans les phases de post-exploitation et de coercition d'authentification.

```powershell
 # Desactiver Print Spooler sur tous les DC
$dcs = Get-ADDomainController -Filter *
foreach ($dc in $dcs) {
    Invoke-Command -ComputerName $dc.HostName -ScriptBlock {
        Stop-Service -Name Spooler -Force
        Set-Service -Name Spooler -StartupType Disabled
        Write-Host "Spooler desactive sur: $env:COMPUTERNAME"
    }
}

# Verifier l'etat sur tous les DC
$dcs | ForEach-Object {
    $status = Invoke-Command -ComputerName $_.HostName -ScriptBlock {Get-Service Spooler |
    Write-Host "$($_.Name): Status=$($status.Status), StartType=$($status.StartType)"
}
```

Restriction du Protocole Netlogon et Protection PetitPotam

La vulnérabilité PetitPotam (CVE-2021-36942 et variantes) exploite le protocole MS-EFSRPC pour forcer l'authentification NTLM d'un DC sans authentification préalable de l'attaquant. Les patches Microsoft pour PetitPotam original ont été déployés, mais des variantes non patchées continuent d'exister car elles exploitent d'autres interfaces RPC qui permettent la même coercition d'authentification. La défense en profondeur contre PetitPotam et ses variantes comprend : désactivation du Web Enrollment ADCS non sécurisé, activation de l'EPA sur les services Web Enrollment, et restriction des interfaces RPC exposées.

La configuration du pare-feu Windows pour bloquer les appels RPC vers les interfaces spécifiques utilisées par PetitPotam est documentée dans le KB5005413. Des filtres RPC peuvent être configurés pour bloquer l'accès aux fonctions EfsRpcOpenFileRaw et ses variantes depuis des machines non autorisées. Cependant, la mesure la plus robuste reste l'activation de l'authentification sur toutes les interfaces ADCS (EPA + HTTPS) qui élimine la capacité de relay post-coercition.

Une autre technique de coercition documentée, **DFSCoerce**, exploite le protocole MS-DFSNM (Distributed File System Namespace Management Protocol) pour forcer l'authentification NTLM

d'un DC. DFSCoerce fonctionne même quand PetitPotam est patché, illustrant la résilience des techniques de coercition et la nécessité d'une défense en profondeur plutôt que de contre-mesures ciblées sur une seule technique. La désactivation du service DFS sur les DC qui ne l'utilisent pas activement est une mesure de réduction de surface d'attaque applicable immédiatement dans les environnements sans namespaces DFS sur les DC.

Hardening de l'Infrastructure DNS Active Directory

Le **DNS Active Directory** est un composant critique souvent négligé dans les audits de sécurité. Les zones DNS AD-intégrées, stockées directement dans Active Directory, sont répliquées sur tous les DC et constituent une cible de choix pour les attaques de type DNS poisoning ou exfiltration via DNS (DNS tunneling). Les mesures de durcissement DNS incluent la sécurisation des mises à jour dynamiques DNS (DNS Secure Update Only), la restriction des enregistrements DNS non authentifiés, et la surveillance des changements DNS anormaux.

Un vecteur d'attaque documenté en 2025 est le **DNS Admin DLL Injection** : les membres du groupe DNSAdmins peuvent configurer le serveur DNS pour charger une DLL arbitraire via `dnscmd /config /serverlevelplugindll`, permettant l'exécution de code avec les privilèges SYSTEM sur le DC hébergeant le service DNS (typiquement tous les DC). La mitigation est de restreindre l'appartenance au groupe DNSAdmins aux seuls administrateurs Tier 0 qui ont déjà ce niveau d'accès par d'autres vecteurs — mais l'audit de ce groupe est nécessaire pour identifier les membres non autorisés.

Contrôle des Trusts Active Directory : Sécuriser les Forêts Multiples

Les **trusts inter-forêts** Active Directory sont des vecteurs d'escalade de privilèges souvent sous-estimés dans les architectures multi-forêts complexes (fréquentes après des fusions-acquisitions). Un attaquant qui compromet une forêt avec un trust bidirectionnel vers une forêt cible peut

utiliser le **SID History** ou des tickets Kerberos inter-forêts pour escalader vers la forêt cible. La filtration SID (SID Filtering) et l'isolation via Selective Authentication sur les trusts sont les mesures de base pour limiter ce risque.

L'audit des trusts se réalise avec `Get-ADTrust -Filter *` et doit identifier tout trust non documenté, tout trust bidirectionnel avec des forêts externes non maîtrisées, et tout trust sans Selective Authentication activée. Dans les architectures post-acquisition, le durcissement des trusts est souvent la mesure de sécurité la plus impactante à court terme, car les deux forêts fusionnées ont rarement le même niveau de maturité sécurité AD.

Détection de l'Utilisation d'Outils d'Énumération AD (BloodHound, PingCastle)

Si les attaquants utilisent BloodHound et PingCastle pour cartographier votre AD, vous devriez les détecter. Ces outils génèrent des patterns de requêtes LDAP distinctifs : BloodHound effectue des requêtes massives et rapides sur tous les objets AD (comptes, groupes, ACL, GPO, sessions), tandis que PingCastle génère des requêtes ciblées sur les attributs de sécurité. La détection se base sur le volume et la régularité des requêtes LDAP depuis un compte non-DC, visible dans les logs 1644 (LDAP query statistics) et les événements de l'audit LDAP.

Microsoft Defender for Identity détecte nativement les phases d'énumération BloodHound avec des alertes "LDAP Reconnaissance" et "Account Enumeration Reconnaissance". Pour les environnements sans MDI, la configuration d'alertes SIEM sur les seuils de requêtes LDAP (par exemple : plus de 200 requêtes LDAP différentes depuis le même compte en moins de 5 minutes) permet de détecter ces comportements sans outil spécialisé. La difficulté est d'éviter les faux positifs générés par les outils d'administration légitimes — une baseline de comportement normal est nécessaire avant d'activer ces alertes en production.

Sécurisation du Processus LSASS et Protection des Credentials

Le processus **LSASS (Local Security Authority Subsystem Service)** est la cible principale des outils de credential dumping comme Mimikatz. Les credentials des utilisateurs authentifiés (hashes NTLM, tickets Kerberos, mots de passe en clair en mémoire pour certaines configurations) sont stockés dans la mémoire LSASS et accessibles aux processus avec des droits DEBUG. Trois couches de protection doivent être déployées en 2026 :

Credential Guard (Virtualization-Based Security) : isole les secrets d'authentification dans une VM légère (VBS/HVCI) inaccessible au système d'exploitation principal, même avec les droits SYSTEM. Compatible avec Windows 10/11 Pro et Enterprise, Server 2016+. C'est la protection la plus robuste contre Mimikatz et les outils similaires sur les machines Credential Guard activées.

PPL (Protected Process Light) pour LSASS : configure LSASS comme processus protégé (RunAsPPL), empêchant les outils sans driver kernel signé d'y accéder. Activable via une clé de registre (HKLM\SYSTEM\CurrentControlSet\Control\Lsa → RunAsPPL=1) ou via GPO Credential Guard. Moins robuste que Credential Guard mais compatible avec des systèmes ne supportant pas VBS.

Restriction de WDigest : s'assurer que WDigest est désactivé (valeur UseLogonCredential=0) pour empêcher le stockage de mots de passe en clair en mémoire LSASS. Normalement désactivé par défaut depuis Windows 8.1/Server 2012 R2, mais peut être réactivé par des applications héritées ou des GPO mal configurées.

Hardening de l'Infrastructure PKI et Renouvellement des Certificats DC

La **PKI (Public Key Infrastructure)** liée à Active Directory — via ADCS — est un composant de sécurité critique dont la gestion est souvent négligée jusqu'à ce qu'une alerte sécurité ou un renouvellement de certificat urgent le mette en lumière. Les certificats des DC (Domain Controller Authentication, Kerberos Authentication) expirent et doivent être renouvelés

proactivement. Un DC avec un certificat expiré peut présenter des problèmes d'authentification Kerberos sur les canaux nécessitant TLS (LDAPS, ADCS).

Le durcissement de la PKI ADCS comprend la restriction de l'accès à la CA (Certificate Authority) aux seuls admins Tier 0, la désactivation de l'interface Web Enrollment ADCS sur HTTP (HTTPS only avec EPA), l'audit et la correction des templates vulnérables (ESC1-ESC8 avec l'outil Certipy), et la mise en place d'une procédure de renouvellement proactif des certificats DC avec notification 60 jours avant expiration. La CA racine de l'entreprise doit être hors-ligne (offline Root CA) avec seulement les CA subordinates en ligne — une pratique standard de PKI mais souvent non respectée dans les déploiements ADCS rapides.

Mesure 11 : Désactivation des Protocoles d'Authentification Hérités

Les protocoles **NTLMv1** et **LM** (LAN Manager) sont des vecteurs d'attaque documentés depuis des décennies mais encore présents dans de nombreux environnements, parfois à l'insu des équipes IT. LM stocke les hashes de façon extrêmement vulnérable (division en deux moitiés de 7 caractères, cassables en quelques secondes). NTLMv1, bien que supérieur à LM, est vulnérable à des attaques de type "crack-me-if-you-can" avec des tables arc-en-ciel. La configuration GPO "Network security: LAN Manager authentication level" doit être positionnée sur "Send NTLMv2 response only. Refuse LM & NTLM" pour éliminer ces protocoles hérités.

La transition vers NTLMv2 exclusif, puis vers l'objectif final de **NTLMv2 restriction** avec préférence Kerberos, est documentée dans les guides ANSSI. Dans un environnement bien configuré avec Kerberos fonctionnel, NTLM ne devrait être utilisé que pour les workgroups, les authentifications locales, et quelques applications tierces non Kerberos-aware. L'objectif 2026 pour les organisations matures est de mesurer et réduire activement le ratio NTLM/Kerberos dans leurs logs d'authentification DC.

Mesure 12 : AdminSDHolder et la Chaîne des Comptes Protégés

L'objet **AdminSDHolder** dans Active Directory définit le gabarit de sécurité appliqué automatiquement (toutes les heures via SDProp) aux groupes et comptes protégés : Domain Admins, Enterprise Admins, Schema Admins, Account Operators, Backup Operators, Print Operators, Replication account, etc. Si les ACL de l'AdminSDHolder sont modifiées par un attaquant, il peut obtenir une persistance durable car SDProp écrase les ACL des objets protégés avec celles d'AdminSDHolder, propageant les droits malveillants de façon automatique et répétée.

La vérification régulière des ACL d'AdminSDHolder est donc une mesure de sécurité à part entière. Elle devrait s'effectuer mensuellement et être intégrée dans les procédures d'audit de sécurité AD. Tout droit inhabituel sur AdminSDHolder doit déclencher une investigation immédiate — il est rare qu'une modification légitime de cet objet soit effectuée, ce qui en fait un indicateur de compromission (IoC) à haute valeur.

Mesure 13 : Audit ADCS (Active Directory Certificate Services)

L'**Active Directory Certificate Services (ADCS)** est devenu l'un des vecteurs d'attaque les plus exploités en 2025-2026 depuis les travaux de SpecterOps sur les ESC (Escalation scenarios). Les misconfigrations ADCS les plus communes permettent à un attaquant d'obtenir un certificat qui lui donne les droits d'un Domain Admin (ESC1), de forger des certificats pour n'importe quel compte (ESC2/ESC3), ou d'exploiter le protocole NTLM Relay vers les services HTTP d'ADCS Web Enrollment (ESC8). L'outil **Certify** (SpecterOps) et **Certipy** (Python) permettent d'identifier rapidement ces misconfigrations.

Pour l'audit ADCS, les vérifications prioritaires sont : templates de certificats avec flag "CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT" combiné à des droits d'enrôlement larges (ESC1), templates avec Extended Key Usage trop permissives, présence de Web Enrollment HTTP (sans HTTPS, vulnérable au relay), et absence de HTTP EPA (Extended Protection for Authentication) sur les services Web Enrollment. L'ANSSI a intégré l'audit ADCS dans ses

recommandations 2024 suite à la multiplication des exploitations ESC en environnement de production.

```
 # Audit ADCS avec Certipy (depuis Linux)
# Installation
pip install certipy-ad

# Enumeration des templates vulnerables
certipy find -u 'user@domain.local' -p 'password' -dc-ip 192.168.1.10 -vulnerable

# Verification manuelle des templates avec enrollee supplies subject
# (indicateur ESC1 si enrollable par des utilisateurs standards)
Get-ADObject -SearchBase "CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Co
    -Filter * -Properties "msPKI-Certificate-Name-Flag","msPKI-Enrollment-Flag","msPKI-RA-S
    Where-Object {'msPKI-Certificate-Name-Flag' -band 1} |  # CT_FLAG_ENROLLEE_SUPPLIES_SUB
    Select-Object Name,'msPKI-Certificate-Name-Flag'
```

Mesure 14 : Hardening des Contrôleurs de Domaine

Les **contrôleurs de domaine (DC)** sont les actifs les plus critiques de l'infrastructure AD et doivent bénéficier du niveau de durcissement le plus élevé. Les mesures spécifiques aux DC incluent : installation minimale (Server Core sans interface graphique), aucune application tierce installée (pas d'antivirus "agent" lourd, de logiciel de monitoring avec agent système, ou d'application métier), accès RDP restreint aux seuls comptes Tier 0 via PAW dédié, et Windows Defender Credential Guard activé pour protéger les credentials LSA.

Le **DC Locator hardening** (KB5020276 et suivants) est une mesure récente à appliquer impérativement : il empêche la coercition d'authentification via des services qui localisent les DC (NetLogon, etc.), vecteur exploité par des techniques comme PetitPotam. L'activation du paramètre "RequireSeal" dans la configuration Netlogon est requise pour neutraliser les variantes de PetitPotam ciblant les canaux sécurisés Netlogon.

Mesure 15 : Restriction de la Délégation Kerberos

La **délégation Kerberos** permet à un service d'agir au nom d'un utilisateur auprès d'autres services. En trois variantes (non contrainte, contrainte, et basée sur les ressources), seule la délégation contrainte (Constrained Delegation) et RBCD (Resource-Based Constrained Delegation) devraient être utilisées dans un environnement durci. La délégation **non contrainte (Unconstrained Delegation)** est le vecteur d'attaque des techniques PrinterBug, PetitPotam et DFSCoerce : quand un utilisateur s'authentifie sur une machine avec Unconstrained Delegation, son TGT est stocké en mémoire sur cette machine et peut être volé.

L'audit des délégations non contraintes s'effectue avec `Get-ADComputer -Filter {TrustedForDelegation -eq $true}` — tout résultat autre que les DC légitimes est un risque potentiel. Les comptes avec délégation non contrainte doivent être migrés vers la délégation contrainte ou RBCD selon les besoins métier. Pour les comptes de service avec délégation, l'ajout au groupe Protected Users est incompatible (Protected Users désactive toute délégation Kerberos), une contrainte à prendre en compte dans la conception de l'architecture.

Gouvernance Continue : La Posture AD n'est Jamais Statique

Un des écueils les plus fréquents dans les projets de durcissement AD est de traiter le durcissement comme un projet avec une date de fin. La réalité est que la posture de sécurité AD se dégrade naturellement avec le temps : les délégations s'accumulent, les comptes de service prolifèrent, les applications héritées imposent des exceptions, et les équipes IT font des compromis sous pression opérationnelle. Le durcissement AD est un processus continu, pas un état final.

Pour maintenir le niveau de sécurité dans la durée, les organisations matures mettent en place trois mécanismes de gouvernance continue : des audits PingCastle trimestriels avec suivi du score dans le temps (un score qui se dégrade d'un trimestre à l'autre est un signal d'alerte), des tests d'intrusion internes red team semestriels spécifiquement focalisés sur les vecteurs AD, et une revue mensuelle des comptes privilégiés (Tier 0 et Tier 1) pour détecter les créations non

autorisées, les mots de passe non changés depuis plus de 90 jours, et les membres inattendus dans les groupes sensibles.

La documentation est également un facteur de gouvernance souvent négligé : sans cartographie à jour des délégations AD, des comptes de service et de leurs SPN, et des chemins d'accès privilégiés, toute nouvelle personne rejoignant l'équipe AD est condamnée à découvrir l'existant par tâtonnement — ou par les rapports BloodHound des attaquants. Maintenir un référentiel documenté de l'architecture AD est une mesure de sécurité à part entière, car elle permet des réponses à incident plus rapides et des décisions de durcissement plus informées.

Déploiement Progressif : Ordre de Priorité Recommandé par l'ANSSI

L'ANSSI recommande un déploiement progressif des mesures de durcissement AD, structuré en trois phases de 90 jours chacune pour les organisations débutant dans cette démarche :

Phase 1 — Actions immédiates (0-90 jours) : Activer Protected Users pour tous les comptes admin, activer SMB Signing mandatory, désactiver LLMNR/NetBIOS, déployer LAPS v2, auditer les SPN sur comptes utilisateurs et initier la migration gMSA, activer l'audit AD avancé (5136, 4662, 4624/4625/4648), déployer MDI en mode lecture seule pour établir une baseline de détection.

Phase 2 — Durcissement structurel (90-180 jours) : Concevoir et implémenter le modèle de tiering AD (au moins la séparation Tier 0 / reste), auditer et corriger les ACL Active Directory dangereuses, désactiver RC4 Kerberos après inventaire des dépendances, auditer ADCS et corriger les templates ESC vulnérables, activer LDAP Signing + CBT sur les DC, initier la restriction des délégations non contraintes.

Phase 3 — Maturité avancée (180-270 jours) : Déployer Authentication Policy Silos, implémenter PAW pour tous les admins Tier 0, compléter la migration gMSA pour tous les comptes de service, activer Credential Guard sur tous les postes admins, et mettre en place des tests red team AD trimestriels pour valider l'efficacité des mesures déployées.

Foire Aux Questions sur le Durcissement Active Directory

Par où commencer quand on n'a jamais durci son AD ?

La première action à mener est un audit de référence avec PingCastle (gratuit, génère un score de risque et une liste priorisée de vulnérabilités) ou BloodHound (open source, visualise les chemins d'attaque). Ces outils donnent en quelques heures une cartographie précise des risques prioritaires. Sans cette baseline, on risque d'investir dans des mesures de faible impact en ignorant des vulnérabilités critiques. Une fois l'audit réalisé, les mesures à impact/effort ratio le plus favorable sont : Protected Users pour les comptes admin, SMB Signing, désactivation LLMNR, et déploiement LAPS v2 — toutes réalisables en moins d'une semaine sans interruption de service.

Le durcissement AD est-il compatible avec les exigences NIS 2 ?

Oui, et NIS 2 l'exige implicitement via les mesures de l'article 21 sur la gestion des risques de cybersécurité. Les mesures de durcissement AD correspondent directement aux exigences NIS 2 de contrôle des accès (activation du MFA, gestion des droits d'accès, protection des comptes à hauts privilèges), de sécurité des réseaux (segmentation, contrôle des flux), et de gestion des incidents (capacité de détection et réponse via MDI et logs centralisés). Les entités NIS 2 auditées par l'ANSSI ou par des organismes d'audit accrédités doivent être en mesure de démontrer la mise en œuvre de ces mesures de durcissement AD.

Quels outils pour auditer régulièrement la posture AD sans budget important ?

Trois outils gratuits couvrent l'essentiel de l'audit AD continu : PingCastle (score de risque global, rapport complet, exécutable sans installation), BloodHound avec l'agent SharpHound (chemins d'attaque visuels, identification des comptes Kerberoastable, ACL dangereuses), et l'outil en ligne de commande PowerView du framework PowerSploit (énumération détaillée des délégations, SPN, trusts). Pour la surveillance continue, les événements Windows EventLog cités dans cet article (4662, 5136, 4740) collectés dans un SIEM open source comme Wazuh offrent une capacité de détection comparable à MDI pour un budget infrastructure uniquement.

Ressources Officielles pour le Durcissement AD

ANSSI — Guide de sécurité Active Directory 2024

MITRE ATT&CK TA0006 — Credential Access (techniques AD)

Liens Vers Nos Articles Techniques Complémentaires

Pour approfondir les aspects techniques abordés dans ce guide, consultez notre analyse de NTLM Relay 2026 avec les défenses SMB, HTTP et LDAP. Notre article sur BadSuccessor et les attaques Entra ID 2026 couvre les vecteurs cloud hybrides. Pour la gouvernance des identités avec un référentiel Zero Trust, notre guide Top 10 des attaques Active Directory est le complément naturel de ce guide de durcissement. Enfin, pour la mise en place d'une détection

SIEM adaptée aux attaques AD, notre analyse sur la détection des attaques Golden SAML et ADFS fournit les règles Sigma et KQL nécessaires.

À RETENIR

Points clés Durcissement Active Directory 2026

SMB Signing + LDAP Signing + CBT : les trois premiers durcissements à activer, impact nul sur les performances modernes

Protected Users pour tous les comptes admin : désactive RC4, credential cache, et délégations non contraintes en une opération

LAPS v2 natif sur Windows 11/Server 2022+ élimine la propagation Pass-the-Hash via admin local partagé

Migration gMSA pour les comptes de service avec SPN : rend le Kerberoasting cryptographiquement impossible

Audit ACL AD régulier avec PingCastle ou BloodHound : les chemins d'escalade cachés sont souvent hérités d'opérations passées

ADCS hardening : vérifier les templates ESC1-ESC8 avant tout déploiement — ADCS mal configuré vaut un DC compromis

Tiering Model : l'investissement architectural le plus durable pour briser les chaînes de mouvement latéral

PingCastle comme baseline : un score en amélioration continue est le meilleur indicateur de maturité AD à présenter à la direction