Durcissement Active Directory 2026 : Checklist ANSSI et Meilleures Pratiques

Le durcissement Active Directory selon les recommandations ANSSI est devenu en 2026 une priorité absolue pour toute organisation disposant d'un parc Windows de taille significative. Active Directory reste la cible numéro un des attaquants sophistiqués : 95 % des intrusions réussies dans les grandes entreprises françaises transitent par un compte ou un service AD compromis, selon les retours d'incidents traités par l'ANSSI. Les guides de l'Agence nationale de la sécurité des systèmes d'information — notamment le PA-022 dédié à la sécurisation d'Active Directory et l'ANSSI-BP-072 sur les mesures de sécurité essentielles — constituent aujourd'hui le référentiel incontournable pour toute équipe sécurité. Ce guide complet vous présente une checklist opérationnelle de durcissement AD 2026 : gestion des comptes privilégiés selon le modèle en tiers, activation du SMB Signing, déploiement de LAPS, politiques de mots de passe affinées, politiques d'audit, et détection des chemins d'attaque BloodHound. Chaque mesure est associée à sa commande PowerShell, son niveau de priorité ANSSI, et ses indicateurs de vérification. Que vous soyez RSSI, administrateur système ou consultant en sécurité offensive, cette ressource vous permettra d'évaluer et de renforcer concrètement la posture de sécurité de votre annuaire Windows.

Résumé exécutif

Référentiels : ANSSI PA-022 (sécurisation AD) et ANSSI-BP-072 (mesures essentielles), complétés par les CIS Benchmarks Microsoft Windows Server

Modèle en tiers : séparation Tier 0 (contrôleurs de domaine), Tier 1 (serveurs membres), Tier 2 (postes utilisateurs) — socle de tout hardening AD

SMB Signing obligatoire : bloque les attaques NTLM relay sur l'ensemble du parc

LAPS : rotation automatique des mots de passe administrateur local, élimine le mouvement latéral par réutilisation de credentials

Fine-Grained Password Policies : appliquer des politiques différenciées par groupe (comptes privilegiés, service accounts)

Audit policies avancées : activer les 9 catégories d'audit recommandées par l'ANSSI pour une détection efficace

BloodHound : analyse régulière des chemins d'attaque pour identifier les délégations dangereuses et les ACLs abusives

Pourquoi l'ANSSI fait d'Active Directory sa priorité de 2026

L'ANSSI publie régulièrement des rapports de menaces qui convergent vers le même constat : Active Directory est systématiquement présent dans les chaînes d'attaque des groupes APT ciblant la France. Le guide PA-022 "Recommandations de sécurité relatives à Active Directory" identifie les vecteurs d'attaque les plus exploités — Kerberoasting, DCSync, Golden Ticket, Pass-the-Hash — et propose des contre-mesures précises et priorisées. L'ANSSI-BP-072, quant à lui, définit les mesures de sécurité dites "essentielles" applicables à tout système d'information, avec une section spécifique aux annuaires. Ces deux documents forment le socle normatif du durcissement AD en France, avant même les recommandations CIS ou DISA STIG. En 2026, les exigences NIS 2 renforcent ce cadre : les entités essentielles et importantes doivent documenter leurs mesures de durcissement et être en mesure de les justifier lors d'audits. Ne pas avoir appliqué les recommandations ANSSI sur l'AD constitue désormais une non-conformité NIS 2 caractérisée.

Le modèle en tiers : fondation du durcissement AD

Le modèle de délégation en tiers (Tiering Model) est la mesure architecturale la plus importante recommandée par l'ANSSI. Il consiste à segmenter l'administration en trois niveaux d'isolation étanches :

Tier 0 — Contrôleurs de domaine, PKI d'entreprise, ADFS, Azure AD Connect, solutions de sauvegarde de l'AD. Seuls les comptes Tier 0 peuvent administrer ces systèmes. Ces comptes ne doivent jamais se connecter à des postes Tier 1 ou Tier 2.

Tier 1 — Serveurs membres (fichiers, applicatifs, bases de données, infrastructure). Les comptes Tier 1 administrent ces serveurs mais n'ont aucun privilège sur le Tier 0.

Tier 2 — Postes de travail et équipements utilisateurs. Les comptes Tier 2 (helpdesk, support) ne peuvent administrer que les postes, jamais les serveurs ou les DC.

La mise en oeuvre technique passe par des **Authentication Silos** et des **Authentication Policies** Kerberos (Windows Server 2012 R2+), qui interdisent à un compte Tier 0 de s'authentifier sur un poste Tier 2, même si l'attaquant tente de forcer cette connexion. On configure également des GPO de restrictions de logon :

```
 # Vérification des groupes à hauts privilèges - Tier 0
Get-ADGroupMember -Identity "Domain Admins" -Recursive | Select-Object Name, SamAccountName
Get-ADGroupMember -Identity "Schema Admins" -Recursive | Select-Object Name, SamAccountName
Get-ADGroupMember -Identity "Enterprise Admins" -Recursive | Select-Object Name, SamAccountName

# Les groupes Tier 0 ne doivent contenir que des comptes dédiés, jamais des comptes utilisateurs
# Nombre recommandé par l'ANSSI : moins de 5 membres permanents dans Domain Admins
```

Gestion des comptes privilégiés selon l'ANSSI

L'ANSSI recommande plusieurs principes fondamentaux pour les comptes d'administration :

Comptes dédiés et cloisonnés

Chaque administrateur dispose d'au moins deux comptes : un compte nominatif standard pour les tâches quotidiennes (messagerie, navigation), et un compte d'administration dédié sans accès à Internet ni à la messagerie. Les comptes de service doivent être distincts des comptes humains et utiliser des Managed Service Accounts (MSA) ou Group Managed Service Accounts (gMSA) pour une rotation automatique du mot de passe.

```
 # Créer un gMSA - rotation automatique du mot de passe (30 jours par défaut)
New-ADServiceAccount -Name "svc-sql-prod" -DNSHostName "sql01.domaine.local" `
    -PrincipalsAllowedToRetrieveManagedPassword "SQL_Servers" `
    -ManagedPasswordIntervalInDays 30

# Vérifier les comptes avec SPN (cibles Kerberoasting)
Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName |
    Select-Object Name, SamAccountName, ServicePrincipalName |
    Where-Object { $_.SamAccountName -notlike "krbtgt*" }
```

Comptes Kerberos protégés : Protected Users

Le groupe **Protected Users** (Windows Server 2012 R2+) renforce automatiquement la protection des comptes membres :

Authentification uniquement via Kerberos (NTLM, Digest, CredSSP interdits)

Tickets Kerberos limités à 4 heures (non renouvelables)

Pas de délégation Kerberos possible

Credentials non mis en cache sur les machines locales

```
 # Ajouter tous les comptes Domain Admins au groupe Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members (
    Get-ADGroupMember "Domain Admins" -Recursive | Where-Object objectClass -eq "user"
)

# Vérifier que les comptes de service critiques sont dans Protected Users
Get-ADGroupMember -Identity "Protected Users" | Select-Object Name, SamAccountName
```

SMB Signing : bloquer les attaques NTLM Relay

Le SMB Signing (signature des messages SMB) est l'une des mesures les plus efficaces contre les attaques de type NTLM Relay et Pass-the-Hash. Sans signature SMB, un attaquant positionné en Man-in-the-Middle peut relayer des authentifications NTLM pour accéder à des partages ou exécuter du code à distance. L'ANSSI recommande d'activer le SMB Signing en mode "Required" sur tous les contrôleurs de domaine ET sur tous les serveurs membres.

```
 # Vérifier l'état actuel du SMB Signing (à exécuter sur chaque serveur)
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature, EnableSecuritySignature

# GPO recommandée ANSSI - Computer Configuration > Windows Settings > Security Settings
# > Local Policies > Security Options :
# - Microsoft network server: Digitally sign communications (always) = Enabled
# - Microsoft network client: Digitally sign communications (always) = Enabled

# PowerShell pour audit rapide du parc
$computers = Get-ADComputer -Filter * -Properties DNSHostName | Select-Object -ExpandProperty DNSH
foreach ($c in $computers) {
    try {
        $smb = Get-SmbServerConfiguration -CimSession $c -ErrorAction Stop
        [PSCustomObject]@{
            Computer = $c
            RequireSignature = $smb.RequireSecuritySignature
        }
    } catch { [PSCustomObject]@{ Computer = $c; RequireSignature = "Unreachable" } }
}
```

LAPS : rotation des mots de passe administrateur local

La réutilisation du même mot de passe administrateur local sur l'ensemble du parc Windows est l'une des principales causes de propagation d'attaques ransomware. **LAPS (Local Administrator Password Solution)**, dans sa version moderne Windows LAPS (intégrée à Windows 11 22H2 et Server 2025), génère et stocke un mot de passe aléatoire unique par machine dans Active Directory. L'ANSSI recommande LAPS comme mesure prioritaire dans PA-022. En 2026,

Windows LAPS remplace définitivement le LAPS legacy et apporte le chiffrement natif des mots de passe en AD.

```
 # Activer Windows LAPS via Group Policy
# Computer Configuration > Administrative Templates > System > LAPS
# - Enable Local Administrator Password Management = Enabled
# - Password Settings : 24 chars minimum, complexity max, rotation 30 jours
# - Do not allow password expiration time longer than required by policy = Enabled
# - Configure size of encrypted password history : 3

# Vérifier le déploiement LAPS
Import-Module LAPS
Get-LapsADPassword -Identity "WORKSTATION01" -AsPlainText

# Audit : machines sans LAPS déployé
Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwdExpirationTime |
    Where-Object { $_."ms-Mcs-AdmPwdExpirationTime" -eq $null } |
    Select-Object Name, OperatingSystem | Sort-Object Name
```

Fine-Grained Password Policies : politiques différenciées

Les **Fine-Grained Password Policies** (FGPP), disponibles depuis Windows Server 2008, permettent d'appliquer des politiques de mots de passe distinctes par groupe ou utilisateur, indépendamment de la Default Domain Policy. L'ANSSI recommande d'appliquer des politiques plus strictes aux comptes privilégiés tout en gardant une politique raisonnable pour les utilisateurs standard.

Type de compte	Longueur min.	Complexité	Durée max.	Historique	Priorité PSO
Comptes Tier 0 (DA, EA)	20 caractères	Oui + passphrases	90 jours	24	1 (plus haute)
Comptes Tier 1 (admins serveurs)	16 caractères	Oui	90 jours	12	10
Comptes de service (non-gMSA)	30 caractères	Oui	365 jours	5	5
Utilisateurs standard	12 caractères	Oui	180 jours	6	50 (par défaut)

```
 # Créer un PSO (Password Settings Object) pour les Domain Admins
New-ADFineGrainedPasswordPolicy -Name "PSO-Tier0-Admins" `
    -Precedence 1 `
    -MinPasswordLength 20 `
    -PasswordHistoryCount 24 `
    -MaxPasswordAge "90.00:00:00" `
    -MinPasswordAge "1.00:00:00" `
    -LockoutThreshold 3 `
    -LockoutDuration "00:30:00" `
    -LockoutObservationWindow "00:30:00" `
    -ComplexityEnabled $true `
    -ReversibleEncryptionEnabled $false

# Appliquer le PSO au groupe Domain Admins
Add-ADFineGrainedPasswordPolicySubject -Identity "PSO-Tier0-Admins" -Subjects "Domain Admins"

# Vérifier les PSO appliqués
Get-ADUserResultantPasswordPolicy -Identity "adminDA01"
```

Audit Policies avancées recommandées par l'ANSSI

La détection des attaques sur Active Directory repose sur une collecte d'événements exhaustive. L'ANSSI définit dans PA-022 les catégories d'audit avancées à activer. Ces politiques doivent être configurées via **Advanced Audit Policy Configuration** (non via les Legacy Audit Policies) pour éviter les conflits. Voici la checklist complète :

Catégorie d'audit	Sous-catégorie	Paramètre ANSSI	Événements clés
Account Logon	Credential Validation	Success + Failure	4776 (NTLM)
Account Logon	Kerberos Authentication	Success + Failure	4768, 4769, 4771
Account Management	User Account Management	Success + Failure	4720, 4725, 4728, 4732
DS Access	Directory Service Access	Success + Failure	4662 (DCSync: GUID DRSUAPI)
DS Access	Directory Service Changes	Success	5136, 5137, 5141
Logon/Logoff	Logon	Success + Failure	4624, 4625, 4648
Object Access	SAM	Success + Failure	4661 (énumération SAM)
Policy Change	Audit Policy Change	Success + Failure	4719
Privilege Use	Sensitive Privilege Use	Success + Failure	4673, 4674 (SeDebugPrivilege)

```
 # Configurer les audit policies via auditpol (à déployer via GPO sur les DCs)
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Service Ticket Operations" /success:enable /failure:enable
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Access" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Changes" /success:enable
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable

# Vérifier la configuration
auditpol /get /category:* | findstr /i "success failure"
```

Délégation Kerberos : identifier et corriger les délégations dangereuses

La délégation Kerberos non contrainte (Unconstrained Delegation) est l'une des vulnérabilités les plus exploitées lors de tests d'intrusion sur Active Directory. Elle permet à un service compromis d'usurper l'identité de n'importe quel utilisateur connecté, y compris les comptes Domain Admin. L'ANSSI recommande de supprimer toutes les délégations non contraintes sauf sur les contrôleurs de domaine.

```
 # Lister les serveurs avec délégation non contrainte (hors DCs) - CRITIQUE
Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation,DNSHostNa
    Where-Object { $_.Name -notlike "*DC*" } |
    Select-Object Name, DNSHostName

# Lister les utilisateurs avec délégation non contrainte
Get-ADUser -Filter {TrustedForDelegation -eq $true} -Properties TrustedForDelegation |
    Select-Object Name, SamAccountName

# Désactiver la délégation non contrainte sur un serveur
Set-ADComputer -Identity "SERVER01" -TrustedForDelegation $false

# Lister les délégations contraintes (S4U2Proxy) - vérifier les SPNs autorisés
Get-ADComputer -Filter {msDS-AllowedToDelegateTo -ne "$null"} `
    -Properties msDS-AllowedToDelegateTo | Select-Object Name, msDS-AllowedToDelegateTo

# Identifier les comptes avec délégation Resource-Based Constrained (RBCD) - vecteur d'attaque
Get-ADComputer -Filter * -Properties PrincipalsAllowedToDelegateToAccount |
    Where-Object { $_.PrincipalsAllowedToDelegateToAccount -ne $null } |
    Select-Object Name, PrincipalsAllowedToDelegateToAccount
```

Détection BloodHound : cartographier les chemins d'attaque

BloodHound est l'outil de référence pour la cartographie des chemins d'attaque dans Active Directory. Son usage défensif — lancé régulièrement par l'équipe sécurité — permet d'identifier les ACLs dangereuses, les groupes imbriqués à risque et les chemins vers Domain Admin avant les attaquants. L'ANSSI recommande explicitement une analyse BloodHound lors de tout audit de sécurité AD et encourage les équipes défensives à intégrer cet outil dans leur cycle de supervision.

```
 # Analyse des requêtes Cypher clés dans BloodHound Community Edition
# 1. Chemins vers Domain Admin depuis n'importe quel utilisateur authentifié
MATCH p=shortestPath((u:User)-[*1..]->(g:Group {name:"DOMAIN ADMINS@DOMAINE.LOCAL"}))
RETURN p LIMIT 25

# 2. Utilisateurs avec GenericAll sur des objets critiques
MATCH (n)-[r:GenericAll]->(m:Group)
WHERE m.name CONTAINS "ADMINS"
RETURN n.name, m.name

# 3. Comptes avec DCSync rights (GetChangesAll)
MATCH (n)-[r:GetChangesAll]->(d:Domain) RETURN n.name, r, d.name

# 4. Sessions administratives sur des machines non-Tier 0
MATCH (u:User)-[r:HasSession]->(c:Computer)
WHERE u.admincount = true AND NOT c.name CONTAINS "DC"
RETURN u.name, c.name
```

Durcissement LDAP signing et Channel Binding

Deux mesures complémentaires souvent négligées mais explicitement recommandées par l'ANSSI : le **LDAP Signing** et le **LDAP Channel Binding**, qui protègent contre les attaques LDAP Relay (variante des NTLM Relay ciblant le port 389).

```
 # LDAP Signing - GPO sur les DCs
# Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Optior
# "Domain controller: LDAP server signing requirements" = Require signing

# LDAP Channel Binding - Registry (Server 2022+ et Windows 10 20H1+)
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LdapEnforceChannelBinding" -Value 2 -Type DWord
# Valeur 2 = Always require channel binding

# Désactiver NTLMv1 sur tout le domaine
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" `
    -Name "LmCompatibilityLevel" -Value 5 -Type DWord
# Valeur 5 = Send NTLMv2 response only, refuse LM and NTLM
```

Checklist ANSSI : les 20 mesures prioritaires

Cette checklist synthétise les recommandations prioritaires des guides ANSSI PA-022 et ANSSI-BP-072, classées par priorité opérationnelle pour un déploiement progressif.

Priorité critique (à déployer en premier)

Activer SMB Signing en mode Required sur tous les DCs et serveurs membres

Vider les groupes Domain Admins / Enterprise Admins (comptes dédiés uniquement)

Supprimer toutes les délégations Kerberos non contraintes hors DCs

Déployer LAPS (Windows LAPS) sur 100% du parc

Désactiver NTLMv1 (LmCompatibilityLevel = 5)

Priorité haute

Implémenter le modèle en tiers avec Authentication Silos

Ajouter les comptes DA/EA dans Protected Users

Configurer FGPP : PSO spécifique par niveau de privilège

Activer LDAP Signing + Channel Binding sur les DCs

Activer toutes les Advanced Audit Policies recommandées ANSSI

Priorité standard

Migrer tous les comptes de service vers gMSA

Désactiver les comptes inactifs (supérieur à 90 jours) et supprimer les orphelins

Retirer les droits d'administration locale généralisés (GPO restricted groups)

Activer le chiffrement AES-256 pour Kerberos (désactiver DES et RC4)

Sécuriser le compte krbtgt (rotation bi-annuelle du mot de passe)

Auditer les ACLs dangereuses (GenericAll, WriteDACL, WriteOwner) via BloodHound

Configurer PowerShell Constrained Language Mode pour les postes utilisateurs

Activer Windows Defender Credential Guard sur les postes Tier 2

Configurer les Authentication Policies pour restricter les logons par tier

Mettre en place un honeypot AD (compte canari avec alerte sur 4624/4768)

Lien avec les tests d'intrusion AD

Le durcissement Active Directory ne se conçoit pas en isolation. Un audit de santé PowerShell régulier permet de maintenir la posture de sécurité dans le temps et de détecter les dérives de configuration. La réalisation de tests d'intrusion internes — avec des outils comme BloodHound, Impacket ou CrackMapExec — permet de valider l'efficacité des mesures de durcissement. L'ANSSI recommande de coupler le hardening à un programme de détection et réponse aux incidents, notamment via la mise en place d'un SIEM collectant les événements Windows définis dans les audit policies. Pour les attaques AD les plus sophistiquées, la compréhension des vecteurs comme le Pass-the-Hash ou l'exploitation de l'annuaire via les mécanismes fondamentaux d'Active Directory est indispensable pour prioriser les mesures de protection.

Les guides CISA Active Directory Security complètent utilement les recommandations ANSSI avec des cas d'usage nord-américains et des indicateurs de compromission (IOC) supplémentaires.

À RETENIR

Points clés à retenir

L'ANSSI PA-022 est le référentiel français de référence pour le durcissement AD — obligatoire dans le cadre de NIS 2

Le modèle en tiers est la mesure architecturale la plus impactante : il casse la propagation latérale entre niveaux d'administration

SMB Signing Required élimine 80% des vecteurs NTLM Relay — mesure simple, impact majeur

LAPS supprime le risque de réutilisation des mots de passe administrateur local sur le parc Windows

Protected Users + Authentication Policies = barrière technique contre le Pass-the-Hash pour les comptes privilégiés

BloodHound en mode défensif : analysez vos chemins d'attaque avant les pentesteurs

Audit policies avancées : sans logs, pas de détection — activer a minima les 9 catégories ANSSI

La rotation bi-annuelle du mot de passe **krbtgt** invalide tous les Golden Tickets en circulation

FAQ — Durcissement Active Directory ANSSI 2026

Quelle est la différence entre l'ANSSI PA-022 et l'ANSSI-BP-072 pour le durcissement AD ?

L'ANSSI PA-022 est un guide dédié exclusivement à la sécurisation d'Active Directory : il couvre en détail les vecteurs d'attaque AD (Kerberoasting, DCSync, délégations), les mesures de hardening spécifiques et les recommandations opérationnelles. L'ANSSI-BP-072 (Recommandations de sécurité relatives aux systèmes d'information) est un guide plus généraliste qui inclut des bonnes pratiques sur les annuaires comme l'une de ses nombreuses thématiques. En pratique, PA-022 est la référence technique à suivre pour le hardening AD, tandis que BP-072 fournit le cadre global de gouvernance de la sécurité SI.

Comment prioriser les mesures de durcissement AD quand les ressources sont limitées ?

L'ANSSI recommande une approche en trois vagues. Première vague (impact maximum, effort modéré) : SMB Signing, vidage des groupes Domain Admins, désactivation de NTLMv1, déploiement LAPS. Ces quatre mesures bloquent les vecteurs les plus courants des ransomwares. Deuxième vague : modèle en tiers, Protected Users, FGPP, LDAP Signing. Troisième vague : gMSA, Credential Guard, Authentication Policies, analyse BloodHound régulière. Cette priorisation permet d'atteindre 80% de la protection avec 30% de l'effort total.

LAPS legacy ou Windows LAPS : lequel déployer en 2026 ?

Windows LAPS (intégré nativement depuis Windows 11 22H2 et Windows Server 2022 avec la mise à jour d'avril 2023) doit être privilégié en 2026. Il apporte le chiffrement AES-256 des mots de passe directement dans Active Directory ou Azure AD, une meilleure intégration PowerShell, la gestion de l'historique des mots de passe chiffrés, et la prise en charge native des comptes locaux arbitraires (pas seulement le compte "Administrator"). Le LAPS legacy (basé sur l'extension CSE) est toujours fonctionnel mais ne reçoit plus de mises à jour majeures. Microsoft recommande officiellement la migration vers Windows LAPS.

Comment détecter une attaque DCSync en cours sur Active Directory ?

Une attaque DCSync génère l'événement Windows 4662 avec le GUID d'objet correspondant aux droits GetChanges et GetChangesAll. Pour détecter cela, configurez l'audit "Directory Service Access" sur Success+Failure, puis créez une règle SIEM qui alerte sur l'événement 4662 généré depuis une adresse IP qui n'est pas un contrôleur de domaine. Des outils comme Microsoft Defender for Identity (MDI) ou le module BloodHound Enterprise détectent automatiquement ces patterns.

Sécurisation des contrôleurs de domaine : mesures complémentaires

Les contrôleurs de domaine (DC) sont les actifs les plus critiques de l'infrastructure Active Directory. Leur compromission équivaut à la compromission totale du domaine. Au-delà des mesures de durcissement génériques, l'ANSSI recommande un ensemble de protections spécifiques aux DC :

Réduction de la surface d'attaque des DCs

Rôle Server Core : déployer les DC en mode Server Core (sans interface graphique) réduit drastiquement la surface d'attaque et les vecteurs de mise à jour

Pas d'applications tierces sur les DCs : aucun logiciel de monitoring, antivirus tiers (utiliser Windows Defender intégré), aucun agent de déploiement non validé

Accès physique et hyperviseur : les DC virtuels nécessitent une protection de l'hyperviseur au niveau Tier 0 — le compte vCenter/Hyper-V qui gère les DCs est de niveau Tier 0

Sauvegardes chiffrées offline : les sauvegardes AD (état système) doivent être chiffrées, stockées hors réseau, et testées régulièrement avec une restauration simulée

```
 # Vérifier que Windows Defender est actif et à jour sur les DCs
Get-MpComputerStatus | Select-Object AMServiceEnabled, AntispywareEnabled,
    AntivirusEnabled, RealTimeProtectionEnabled, NISEnabled

# Vérifier les connexions ouvertes sur les DCs (baseline puis surveillance des anomalies)
netstat -an | findstr "ESTABLISHED" | findstr /v "127.0.0.1"

# Lister les services en écoute sur les DCs - réduire au strict nécessaire
Get-NetTCPConnection -State Listen | Select-Object LocalPort, OwningProcess |
    ForEach-Object { $p = Get-Process -Id $_.OwningProcess -ErrorAction SilentlyContinue;
    [PSCustomObject]@{Port=$_.LocalPort; Process=$p.Name} } | Sort-Object Port
```

Rotation du compte krbtgt : neutraliser les Golden Tickets

Le compte **krbtgt** est le compte de service utilisé par le Key Distribution Center (KDC) Kerberos pour signer tous les tickets du domaine. Un attaquant qui parvient à extraire le hash NTLM de ce compte peut forger des Golden Tickets — des tickets Kerberos valables pour n'importe quel service, pour n'importe quel utilisateur, avec une durée de vie arbitraire. La rotation régulière du mot de passe krbtgt invalide tous les Golden Tickets en circulation.

```
 # Rotation du mot de passe krbtgt (procédure ANSSI recommandée)
# IMPORTANT : La rotation doit être effectuée 2 fois avec un délai de replication entre les deux
# Car la valeur précédente est conservée pour permettre la décryption des tickets en cours

# Étape 1 : Première rotation
$krbtgt = Get-ADUser krbtgt
Set-ADAccountPassword -Identity $krbtgt -Reset `
    -NewPassword (ConvertTo-SecureString -AsPlainText `
    ([System.Web.Security.Membership]::GeneratePassword(128, 32)) -Force)

# Attendre la réplication AD complète (au moins 10 minutes)
# Vérifier la réplication : repadmin /replsummary

# Étape 2 : Deuxième rotation (invalide définitivement les Golden Tickets)
Set-ADAccountPassword -Identity $krbtgt -Reset `
    -NewPassword (ConvertTo-SecureString -AsPlainText `
    ([System.Web.Security.Membership]::GeneratePassword(128, 32)) -Force)

# Vérifier la date de dernière rotation
Get-ADUser krbtgt -Properties PasswordLastSet | Select-Object PasswordLastSet
```

L'ANSSI recommande une rotation bi-annuelle du compte krbtgt, et systématiquement après tout incident de sécurité impliquant un accès suspect aux DC. Le script New-KrbtgtKeys.ps1 (disponible sur le GitHub Microsoft) automatise cette procédure de rotation double avec les vérifications de réplication.

Intégration avec Microsoft Defender for Identity (MDI)

Microsoft Defender for Identity (anciennement Azure ATP) est la solution de détection d'intrusions spécifique à Active Directory recommandée pour compléter le durcissement. MDI analyse le trafic réseau vers les DC via un capteur léger, corrèle les comportements avec la threat intelligence Microsoft, et alerte sur les patterns d'attaque AD en temps réel : Kerberoasting, Pass-the-Hash, DCSync, Golden/Silver Tickets, reconnaissance BloodHound. Sa configuration optimale intègre MDI avec Microsoft Sentinel pour une réponse automatisée.

```
 # Vérifier l'installation du capteur MDI sur les DCs
Get-Service AATPSensor -ComputerName DC01 | Select-Object Status, StartType

# Les alertes MDI clés à activer (priorité haute) :
# - Suspected identity theft (pass-the-hash)
# - Suspected DCSync attack (replication of directory services)
# - Malicious request of Data Protection API master key
# - Suspected Golden Ticket usage (encryption downgrade)
# - Suspected skeleton key attack (encryption downgrade)
# - Reconnaissance using LDAP queries
```