Authentication Policies et Authentication Silos : Guide Windows Server 2025

> Authentication Policies et Silos sous Windows Server 2025 : configurer, auditer et sécuriser l'accès Kerberos Tier 0. Guide expert avec PowerShell et GPO.

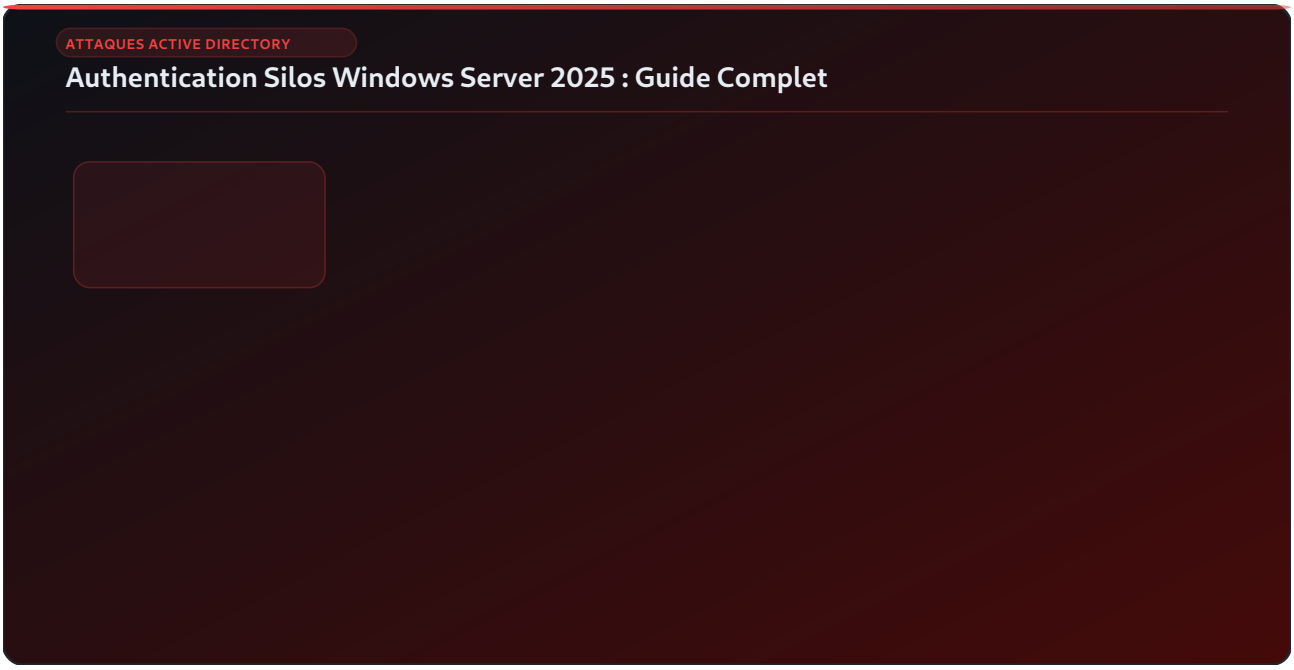
En 2026, la sécurisation des comptes à privilèges élevés dans les environnements Active Directory constitue l'une des priorités absolues pour les RSSI et architectes sécurité français. Les attaques ciblant les contrôleurs de domaine — Pass-the-Hash, Pass-the-Ticket, Golden Ticket — ne cessent de progresser, et les référentiels ANSSI comme le guide de l'hygiène informatique ou les recommandations NIS2 exigent désormais une isolation stricte des accès Tier 0. C'est précisément dans ce contexte que les **Authentication Policies** et les **Authentication Silos**, introduits avec Windows Server 2012 R2 et renforcés sous Windows Server 2025, s'imposent comme des mécanismes de défense incontournables. Ces deux fonctionnalités Kerberos permettent de restreindre de manière granulaire les comptes qui peuvent s'authentifier sur quels hôtes, réduisant considérablement la surface d'attaque en cas de compromission d'un poste de travail ou d'un serveur de niveau inférieur. Ce guide pratique, à destination des équipes sécurité des PME/ETI et des grandes organisations françaises, détaille l'architecture, le déploiement PowerShell, l'audit et les cas d'usage terrain, notamment dans les secteurs bancaire et de la défense.

📋 EN BREF

Points clés à retenir

- Les Authentication Silos isolent des groupes de comptes et d'hôtes dans des compartiments Kerberos étanches.
- Les Authentication Policies définissent les règles de durée de vie des tickets et les conditions d'accès associées à chaque Silo.

- Le niveau fonctionnel de domaine Windows Server 2012 R2 minimum est requis ; Windows Server 2025 apporte des améliorations notables sur le Kerberos Armoring (FAST).
- Le déploiement se fait intégralement via PowerShell ou la console ADAC, sans modification des GPO existantes.
- Les événements 4820 et 4821 permettent de monitorer les violations de politique en mode audit avant le passage en mode enforce.
- L'intégration avec Protected Users Group et LAPS constitue une défense en profondeur recommandée par l'ANSSI.



Avant d'entrer dans le vif du déploiement, il est essentiel de bien distinguer les deux objets Active Directory concernés, souvent confondus dans la documentation Microsoft.

1.1 Qu'est-ce qu'une Authentication Policy ?

Une **Authentication Policy** (objet AD de classe `msDS-AuthNPolicy`) est un conteneur de règles qui s'applique à des comptes utilisateurs, des comptes d'ordinateurs ou des comptes de service. Elle permet de définir :

La durée de vie du TGT (Ticket Granting Ticket) : valeur en minutes, distincte de la politique Kerberos globale du domaine.

Les conditions d'accès : expressions SDDL (Security Descriptor Definition Language) qui spécifient depuis quels hôtes un compte peut obtenir un TGT ou un ticket de service.

Le mode d'application : Audit (journalisation uniquement, aucun blocage) ou Enforce (blocage effectif des authentifications non conformes).

Une Authentication Policy peut exister de manière indépendante d'un Silo et être assignée directement à un compte. Cependant, l'usage le plus courant et le plus robuste est de l'associer à un Authentication Silo.

1.2 Qu'est-ce qu'un Authentication Silo ?

Un **Authentication Silo** (objet AD de classe `msDS-AuthNPolicySilo`) est un regroupement logique qui associe :

Des **comptes membres** (utilisateurs, ordinateurs, services managés) autorisés à appartenir à ce Silo.

Des **Authentication Policies** distinctes pour chaque type de compte (utilisateurs, ordinateurs, services).

Le Silo fonctionne comme un compartiment étanche : un compte membre d'un Silo ne peut s'authentifier que sur des hôtes également membres de ce Silo (selon la politique configurée). Si un attaquant compromet un poste de travail Tier 1, il ne pourra pas utiliser les credentials Tier 0 capturés pour s'authentifier sur un contrôleur de domaine, car ce dernier vérifiera l'appartenance au Silo et refusera le ticket.

1.3 Prérequis techniques

Le déploiement des Authentication Silos nécessite de vérifier plusieurs conditions préalables dans votre environnement :

Niveau fonctionnel de domaine : minimum Windows Server 2012 R2. Vérifiez avec `Get-ADDomain | Select DomainMode`.

Windows Server 2025 : apporte la prise en charge native du Kerberos Armoring (FAST) sur tous les rôles, une meilleure intégration avec les claims AD FS, et le support des groupes de sécurité dynamiques pour les silos.

Contrôleurs de domaine : tous les DC doivent tourner sous Windows Server 2012 R2 minimum pour honorer les politiques en mode Enforce.

Clients : les hôtes membres du Silo doivent supporter Kerberos Armoring (Windows 8.1/2012 R2+). Les clients plus anciens seront bloqués si la politique est en mode Enforce avec FAST requis.

Droits requis : membre de Domain Admins ou délégation explicite sur l'OU `CN=AuthN Policies,CN=AuthN Policy Configuration,CN=Services,CN=Configuration,DC=...`.

Pour vérifier votre niveau fonctionnel :

```
 # Vérification du niveau fonctionnel de domaine
Get-ADDomain | Select-Object Name, DomainMode, PDCEmulator

# Vérification que tous les DC supportent les Authentication Silos
Get-ADDomainController -Filter * | Select-Object Name, OperatingSystem, OperatingSystemVersion
```

---

2. Architecture Authentication Silos : Tiering AD et cloisonnement Kerberos

L'implémentation des Authentication Silos s'inscrit naturellement dans le modèle de tiering Active Directory recommandé par Microsoft et repris dans les guides de l'ANSSI. L'article Tiering Model AD : segmentation des privilèges détaille ce modèle en profondeur ; rappelons ici les grandes lignes applicables aux Silos.

⚡ **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.

2.1 Les trois niveaux (Tiers) et leurs Silos associés

Tier 0 — Plan de contrôle : contrôleurs de domaine, serveurs ADFS, PKI d'entreprise, systèmes de gestion des identités (PAM, CyberArk, BeyondTrust). Les comptes Tier 0 — Domain Admins, Enterprise Admins, Schema Admins — sont les cibles prioritaires de toute attaque APT. Un Silo Tier 0 garantit que ces comptes ne peuvent obtenir de TGT que depuis des Privileged Access Workstations (PAW) dédiées et ne peuvent s'authentifier que sur des systèmes Tier 0.

Tier 1 — Plan des serveurs : serveurs applicatifs, serveurs de fichiers, serveurs de base de données. Les administrateurs Tier 1 gèrent ces systèmes depuis des Jump Servers dédiés. Un Silo Tier 1 empêche ces comptes d'accéder aux ressources Tier 0.

Tier 2 — Plan des postes de travail : postes utilisateurs, terminaux mobiles gérés. Les helpdesk et techniciens de support opèrent à ce niveau. Un Silo Tier 2 limite leur périmètre aux seuls endpoints.

2.2 Mécanisme Kerberos sous-jacent : claims et DAC

Les Authentication Silos exploitent le mécanisme de **Dynamic Access Control (DAC)** et les **claims Kerberos** introduits avec Windows Server 2012. Lors de l'émission d'un TGT, le KDC (Key Distribution Center) inclut dans le PAC (Privilege Attribute Certificate) du ticket des informations sur le Silo d'appartenance du compte.

Lorsqu'un client demande un ticket de service (TGS), le serveur cible vérifie que le Silo du compte demandeur correspond à un Silo autorisé dans sa propre politique. Ce contrôle est effectué côté KDC, ce qui signifie qu'il n'est pas bypassable côté client — contrairement aux groupes de sécurité locaux qui peuvent être manipulés sur un poste compromis.

Les conditions d'accès sont exprimées en SDDL avec la syntaxe de claims AD :

```
 # Exemple de condition SDDL pour restreindre l'accès aux PAW Tier 0
# Seuls les membres du groupe "PAW-Tier0-Computers" peuvent initier une session
$condition = 'O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == "Silo-Tier0-DC"))'
```

2.3 Interaction avec le groupe Protected Users

Le groupe **Protected Users** (disponible depuis Windows Server 2012 R2) et les Authentication Silos sont complémentaires, non concurrents. Protected Users désactive NTLM, WDigest, CredSSP et limite la durée de vie des TGT à 4 heures sans renouvellement. Les Authentication Silos ajoutent une dimension géographique (restriction aux hôtes autorisés) que Protected Users n'offre pas.

La combinaison des deux constitue la défense en profondeur optimale pour les comptes Tier 0 :

Protected Users : supprime NTLM et les mécanismes de délégation dangereux.

Authentication Silo : restreint les hôtes depuis lesquels le compte peut s'authentifier.

LAPS : garantit l'unicité des mots de passe d'administration locale sur les PAW membres du Silo.

---

3. Déploiement pas à pas avec PowerShell

Le déploiement d'un Authentication Silo Tier 0 s'effectue en plusieurs étapes séquentielles. Nous détaillons ici le processus complet pour un environnement de production, avec les commandes de vérification à chaque étape.

3.1 Création du Silo Tier 0

```
 # Créer un Authentication Silo pour les comptes Tier 0
New-ADAuthenticationPolicySilo `
    -Name "Silo-Tier0-DC" `
    -Description "Silo isolé pour comptes Tier 0 — Contrôleurs de domaine et PAW" `
    -ProtectedAccounts "Domain Admins","Enterprise Admins","Schema Admins" `
    -Enforce $false  # Démarrer en mode Audit — passer à $true après validation

# Vérifier la création
Get-ADAuthenticationPolicySilo -Identity "Silo-Tier0-DC" | Format-List *
```

3.2 Création de l'Authentication Policy associée

```
 # Créer une Authentication Policy pour les utilisateurs Tier 0
New-ADAuthenticationPolicy `
    -Name "Policy-Tier0-Users" `
    -Description "Restriction Kerberos Tier 0 — TGT 240 min, hôtes PAW uniquement" `
    -UserTGTLifetimeMins 240 `
    -Enforce $false `
    -RollingNTLMSecret Enabled

# Créer la policy pour les ordinateurs Tier 0 (les DC eux-mêmes)
New-ADAuthenticationPolicy `
    -Name "Policy-Tier0-Computers" `
    -Description "Politique Kerberos pour DC et PAW Tier 0" `
    -ComputerTGTLifetimeMins 480 `
    -Enforce $false

# Créer la policy pour les comptes de service Tier 0
New-ADAuthenticationPolicy `
    -Name "Policy-Tier0-Services" `
    -Description "Politique pour comptes de service Tier 0 (gMSA)" `
    -ServiceAllowedToAuthenticateFrom "O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationS
    -Enforce $false
```

3.3 Association des politiques au Silo

```
 # Assigner les policies au Silo Tier 0
Set-ADAuthenticationPolicySilo `
    -Identity "Silo-Tier0-DC" `
    -UserAuthenticationPolicy "Policy-Tier0-Users" `
    -ComputerAuthenticationPolicy "Policy-Tier0-Computers" `
    -ServiceAuthenticationPolicy "Policy-Tier0-Services"

# Vérifier l'association
Get-ADAuthenticationPolicySilo -Identity "Silo-Tier0-DC" | `
    Select-Object Name, UserAuthenticationPolicy, ComputerAuthenticationPolicy, ServiceAuthentica
```

3.4 Assignation des comptes et hôtes au Silo

```
 # Assigner des comptes utilisateurs Tier 0 au Silo
$tier0Users = @("admindc01", "admindc02", "svc-backup-dc", "admin-pkiCA")

foreach ($user in $tier0Users) {
    Add-ADAccountToAuthenticationPolicySilo `
        -Identity $user `
        -AuthenticationPolicySilo "Silo-Tier0-DC"
    Write-Host "Compte $user ajouté au Silo-Tier0-DC" -ForegroundColor Green
}

# Assigner les contrôleurs de domaine et PAW au Silo
$tier0Computers = @("DC01$", "DC02$", "PAW-TIER0-01$", "PAW-TIER0-02$")

foreach ($computer in $tier0Computers) {
    Add-ADAccountToAuthenticationPolicySilo `
        -Identity $computer `
        -AuthenticationPolicySilo "Silo-Tier0-DC"
    Write-Host "Ordinateur $computer ajouté au Silo-Tier0-DC" -ForegroundColor Green
}

# Vérifier tous les membres du Silo
Get-ADAuthenticationPolicySilo -Identity "Silo-Tier0-DC" | `
    Select-Object -ExpandProperty Members
```

3.5 Définition des conditions d'accès (Access Control Expressions)

```
 # Définir la condition : seuls les membres du groupe PAW-Tier0 peuvent initier l'auth
# Cette expression SDDL vérifie que l'ordinateur source appartient au bon Silo
$userAccessCondition = @"
O:SYG:SYD:(XA;OICI;CR;;;WD;(@DEVICE.ad://ext/AuthenticationSilo == "Silo-Tier0-DC"))
"@

# Appliquer la condition sur la policy utilisateurs
Set-ADAuthenticationPolicy `
    -Identity "Policy-Tier0-Users" `
    -UserAllowedToAuthenticateFrom $userAccessCondition

# Vérifier les Silos actifs et leur état
Get-ADAuthenticationPolicySilo -Filter * | `
    Select-Object Name, Enforce, Description | `
    Format-Table -AutoSize
```

3.6 Passage en mode Enforce après validation

```
 # Après 2-4 semaines d'audit sans faux positifs, passer en mode Enforce
# D'abord sur la policy
Set-ADAuthenticationPolicy -Identity "Policy-Tier0-Users" -Enforce $true
Set-ADAuthenticationPolicy -Identity "Policy-Tier0-Computers" -Enforce $true

# Puis sur le Silo
Set-ADAuthenticationPolicySilo -Identity "Silo-Tier0-DC" -Enforce $true

Write-Host "Silo-Tier0-DC est maintenant en mode ENFORCE" -ForegroundColor Red
```

4. Audit et monitoring des Authentication Silos

Le monitoring est une étape critique, particulièrement pendant la phase de transition entre le mode Audit et le mode Enforce. L'hardening AD complet détaille les bonnes pratiques générales ; nous nous concentrons ici sur les événements spécifiques aux Authentication Silos.

4.1 Événements Windows à surveiller

Les contrôleurs de domaine génèrent des événements spécifiques lors des interactions avec les Authentication Silos. Voici les identifiants d'événements clés :

4769 — Ticket de service Kerberos demandé. Inclut des champs sur le compte cible et le résultat. Filtrer sur `Status: 0xC0000413` (KDC_ERR_POLICY) pour détecter les violations.

4820 — TGT refusé car le périphérique ne répond pas aux restrictions d'accès (mode Audit). Journalisé sur le KDC.

4821 — Ticket de service refusé car le périphérique ne répond pas aux restrictions (mode Audit).

4822 — NTLM bloqué par Authentication Policy (compte membre du Silo tentant NTLM).

4823 — NTLM requis mais non autorisé — combinaison avec Protected Users.

```
 # Requête des événements liés aux Authentication Silos sur les DC
# Événements 4820 et 4821 = violations de politique (mode audit)
Get-WinEvent -ComputerName "DC01" -FilterHashtable @{
    LogName   = 'Security'
    Id        = @(4820, 4821, 4822, 4823)
    StartTime = (Get-Date).AddDays(-7)
} | Select-Object TimeCreated, Id, Message | Format-Table -Wrap -AutoSize

# Filtrer les erreurs KDC_ERR_POLICY dans les événements 4769
Get-WinEvent -ComputerName "DC01" -FilterHashtable @{
    LogName   = 'Security'
    Id        = 4769
    StartTime = (Get-Date).AddDays(-1)
} | Where-Object { $_.Message -match "0xc0000413" } | `
    Select-Object TimeCreated, Message
```

4.2 Vérification PowerShell des politiques actives

```
 # Lister toutes les Authentication Policies avec leur état
Get-ADAuthenticationPolicy -Filter * | `
    Select-Object Name, Enforce, UserTGTLifetimeMins, Description | `
    Format-Table -AutoSize

# Lister tous les Silos avec leur état et membres
Get-ADAuthenticationPolicySilo -Filter * | `
    Select-Object Name, Enforce, Description | `
    Format-Table -AutoSize

# Vérifier les comptes membres d'un Silo spécifique
Get-ADUser -Filter {AuthenticationPolicySilo -eq "Silo-Tier0-DC"} | `
    Select-Object SamAccountName, DistinguishedName

# Vérifier la politique assignée à un compte spécifique
Get-ADUser -Identity "admindc01" -Properties AuthenticationPolicy, AuthenticationPolicySilo | `
    Select-Object SamAccountName, AuthenticationPolicy, AuthenticationPolicySilo
```

4.3 Script de rapport d'audit hebdomadaire

```
 # Script d'audit hebdomadaire — à placer dans une tâche planifiée sur le DC
$reportDate = Get-Date -Format "yyyy-MM-dd"
$reportPath = "C:\Audit\AuthSilos-$reportDate.html"

$violations = Get-WinEvent -ComputerName "DC01" -FilterHashtable @{
    LogName   = 'Security'
    Id        = @(4820, 4821, 4822)
    StartTime = (Get-Date).AddDays(-7)
} -ErrorAction SilentlyContinue

$silos = Get-ADAuthenticationPolicySilo -Filter * | `
    Select-Object Name, Enforce, Description

$report = @"
<html><body>
<h1>Rapport Audit Authentication Silos — $reportDate</h1>
<h2>Silos configurés</h2>
<p>Nombre de Silos : $($silos.Count)</p>
<h2>Violations détectées (7 derniers jours)</h2>
<p>Nombre d'événements : $($violations.Count)</p>
</body></html>
"@

$report | Out-File -FilePath $reportPath -Encoding UTF8
Write-Host "Rapport généré : $reportPath"
```

---

5. Kerberos Armoring (FAST) et intégration Windows Server 2025

Le **Kerberos Armoring**, ou FAST (Flexible Authentication Secure Tunneling), est un mécanisme qui chiffre les échanges Kerberos pré-authentification dans un tunnel TGT machine. Windows Server 2025 le prend en charge nativement sur toutes les topologies de domaine, y compris les forêts multi-sites — un apport majeur par rapport à 2019/2022.

5.1 Pourquoi le Kerberos Armoring est-il crucial pour les Silos ?

Sans Kerberos Armoring, les exchanges AS-REQ (demande de TGT) circulent en clair sur le réseau, permettant des attaques de type AS-REP Roasting. Avec FAST :

Les messages AS-REQ sont chiffrés avec le TGT machine de l'hôte client.

Le KDC peut vérifier l'identité de la machine avant même d'évaluer les credentials utilisateur.

Les **Authentication Silos peuvent ainsi valider l'appartenance de l'hôte au Silo** dès la phase d'obtention du TGT, et non uniquement lors de la demande de ticket de service.

5.2 Configuration du Kerberos Armoring via GPO

La configuration se fait via Group Policy, séparément sur les clients (ordinateurs du Silo) et sur les DC :

```
 # Chemin GPO pour activer le Kerberos Armoring côté client
# Computer Configuration > Policies > Administrative Templates >
# System > Kerberos > Kerberos client support for claims, compound authentication and Kerberos ar
# Valeur : Enabled

# Vérifier si le Kerberos Armoring est supporté sur un hôte
klist tgt
# La ligne "KDC: " indiquera si FAST est utilisé

# Sur le DC : vérifier la configuration KDC
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Kdc |
    Select-Object EnableKDCProxyServer, ClaimsCompoundAndPacEnabled

# Activer les claims et compound authentication sur le DC (si non fait via GPO)
Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Kdc `
    -Name "ClaimsCompoundAndPacEnabled" -Value 3 -Type DWORD
```

5.3 Nouveautés Windows Server 2025 pour les Authentication Silos

Windows Server 2025 introduit plusieurs améliorations significatives pour les Authentication Silos :

Support FAST sur les RODC : les Read-Only Domain Controllers peuvent désormais traiter les échanges FAST complets, utile pour les sites distants avec des comptes Tier 1 dans un Silo.

Intégration Azure AD Kerberos : les comptes hybrides (Azure AD + AD on-prem) peuvent être membres de Silos, permettant l'extension du tiering aux environnements cloud.

Diagnostic amélioré : le journal `Microsoft-Windows-Kerberos-Key-Distribution-Center/Operational` expose désormais les détails de validation des Silos, facilitant le troubleshooting.

Durée de vie des TGT configurable par Silo : dans les versions précédentes, la durée s'appliquait globalement ; 2025 permet une granularité par politique assignée au Silo.

---

6. Cas terrain France : intégration COMISO, NIS2 et secteurs sensibles

Les équipes de consulting AyiNedjimi interviennent régulièrement à Paris, Lyon et Bordeaux pour accompagner des organisations dans la mise en conformité NIS2 et l'application des recommandations ANSSI. Le déploiement des Authentication Silos est devenu un livrable standard dans nos missions RSSI externalisé pour les secteurs banque, défense et santé.

6.1 Contexte réglementaire NIS2 et ANSSI

La directive NIS2 (transposée en droit français par la loi du 17 octobre 2024) impose aux Entités Essentielles (EE) et Entités Importantes (EI) de mettre en œuvre des **mesures de gestion des risques** incluant le contrôle des accès à privilèges. L'ANSSI recommande explicitement dans son guide *"Recommandations pour l'administration sécurisée des systèmes d'information"* (PA-022) le cloisonnement des comptes d'administration via des mécanismes natifs Windows — dont font partie les Authentication Silos.

Pour un audit de conformité NIS2, les Authentication Silos apportent des preuves documentées et automatiquement vérifiables :

Les politiques AD sont modifiées uniquement via compte Admin avec journalisation (événement 5137 — modification d'objet AD).

Les tentatives de violation sont enregistrées (4820/4821) et peuvent être transmises au SIEM.

La configuration est centralisée dans AD, auditée par `Get-ADAuthenticationPolicy` et exportable en rapport.

6.2 Secteur bancaire : intégration avec CyberArk PAM

Dans les établissements bancaires français soumis à la supervision BCE/ACPR, la combinaison CyberArk PAM + Authentication Silos constitue une architecture cible fréquente. Le coffre CyberArk gère la rotation des mots de passe des comptes Tier 0, tandis que le Silo garantit que ces comptes ne peuvent s'authentifier qu'à partir des serveurs PSM (Privileged Session Manager) membres du Silo.

Les étapes d'intégration incluent :

Créer un Silo dédié `Silo-PAM-Vault` regroupant les comptes de service CyberArk et les serveurs PSM.

Configurer l'Authentication Policy avec une durée de TGT alignée sur la session PAM (généralement 60-120 minutes).

Exclure les comptes de service CyberArk du groupe Protected Users (incompatible avec certaines fonctions de rotation).

Activer l'audit en parallèle du déploiement CyberArk pour éviter les faux positifs lors de la migration.

6.3 Secteur défense : cloisonnement COMISO

Pour les organisations de défense françaises opérant des réseaux classifiés ou sous homologation RGS/LPM, le COMISO (Commandant de la Sécurité des Systèmes d'Information) exige une

traçabilité complète des accès administrateurs. Les Authentication Silos répondent à cette exigence en :

Empêchant tout accès admin depuis un poste non homologué (non membre du Silo).

Générant des traces Kerberos horodatées et signées numériquement dans les journaux DC.

Permettant la révocation immédiate d'un accès en retirant le compte du Silo, sans modification de mot de passe ni délai de propagation GPO.

Voir également notre article sur la rotation sécurisée du compte KRBTGT, étape complémentaire indispensable dans ces environnements.

7. Erreurs courantes et dépannage

Le déploiement des Authentication Silos génère des erreurs caractéristiques lors de la phase de validation. Voici les problèmes les plus fréquemment rencontrés en mission et leurs résolutions.

7.1 KDC_ERR_POLICY (0xC0000413) — Violation de politique

Cette erreur apparaît côté client lorsqu'un compte tente de s'authentifier depuis un hôte non autorisé par la politique. Elle est visible dans :

L'événement 4769 sur le DC avec Status `0xc0000413`.

L'événement 4820 ou 4821 selon le type de ticket demandé.

Côté client : message "L'accès est refusé" ou "Erreur d'authentification Kerberos".

```
 # Diagnostic : identifier l'hôte source de la violation
Get-WinEvent -ComputerName "DC01" -FilterHashtable @{
    LogName   = 'Security'
    Id        = 4769
    StartTime = (Get-Date).AddHours(-1)
} | Where-Object { $_.Message -match "0xc0000413" } | ForEach-Object {
    $event = [xml]$_.ToXml()
    [PSCustomObject]@{
        Time          = $_.TimeCreated
        Account       = $event.Event.EventData.Data | Where-Object {$_.Name -eq "TargetUserName"}
        ClientAddress = $event.Event.EventData.Data | Where-Object {$_.Name -eq "IpAddress"} | Se
        ServiceName   = $event.Event.EventData.Data | Where-Object {$_.Name -eq "ServiceName"} |
    }
}
```

7.2 Clients non compatibles avec FAST

Les postes Windows 7 / Windows Server 2008 R2 ne supportent pas Kerberos Armoring. Si votre Silo inclut des hôtes anciens :

Ne pas exiger FAST dans la GPO (*Fail Authentication Requests* doit rester à *Not Supported* pour ces machines).

Créer un Silo séparé sans exigence FAST pour les systèmes legacy.

Planifier la migration ou l'isolation réseau des systèmes non compatibles.

7.3 Comptes de service oubliés

Un oubli fréquent : les comptes de service non interactifs (services Windows, agents de supervision) qui s'authentifient sur des ressources Tier 0. Si ces comptes ne sont pas membres du Silo et que la politique est en Enforce, leurs authentifications seront bloquées.

```
 # Identifier les comptes de service qui accèdent aux ressources Tier 0
# en analysant les tickets Kerberos avant le passage en Enforce
Get-WinEvent -ComputerName "DC01" -FilterHashtable @{
    LogName   = 'Security'
    Id        = 4769
    StartTime = (Get-Date).AddDays(-30)
} | Where-Object { $_.Message -match "krbtgt|DC01\$|DC02\$" } | `
    ForEach-Object {
        $event = [xml]$_.ToXml()
        $event.Event.EventData.Data | Where-Object {$_.Name -eq "TargetUserName"} | `
            Select-Object -ExpandProperty '#text'
    } | Sort-Object -Unique
```

7.4 Gestion des exceptions temporaires

```
 # Retirer temporairement un compte du Silo pour opération de maintenance
# (sans supprimer la policy — le compte conserve son AuthenticationPolicy)
Remove-ADAccountFromAuthenticationPolicySilo `
    -Identity "admindc01" `
    -AuthenticationPolicySilo "Silo-Tier0-DC"

# Réintégrer après maintenance
Add-ADAccountToAuthenticationPolicySilo `
    -Identity "admindc01" `
    -AuthenticationPolicySilo "Silo-Tier0-DC"

# Désactiver temporairement le mode Enforce sur un Silo (break-glass)
Set-ADAuthenticationPolicySilo -Identity "Silo-Tier0-DC" -Enforce $false
Write-Warning "ATTENTION : Silo-Tier0-DC en mode AUDIT — remettre en Enforce sous 24h"
```

8. Checklist de mise en œuvre

Cette checklist synthétise les étapes clés pour un déploiement réussi des Authentication Silos dans un environnement de production. Elle s'inspire des recommandations Microsoft pour le durcissement AD et des guides ANSSI.

Pour les organisations utilisant ADFS comme STS fédéré, notre guide Durcissement ADFS : Hardening Windows Server 2025 couvre la sécurisation TLS, les endpoints, l'extranet lockout et la migration vers Microsoft Entra ID.

À RETENIR

Checklist Authentication Silos — Production

Phase 1 — Préparation (J-30)
Vérifier le niveau fonctionnel de domaine (minimum 2012 R2)

Inventorier tous les DC et vérifier leur version OS

Identifier et documenter tous les comptes Tier 0 (utilisateurs + services)

Identifier les hôtes PAW existants ou planifier leur déploiement

Vérifier la compatibilité FAST des clients (Win 8.1+ requis)

Activer l'audit Kerberos avancé sur tous les DC (GPO)

Configurer la collecte centralisée des événements 4769/4820/4821 dans le SIEM

Phase 2 — Déploiement en Audit (J-0 à J+30)
Créer le Silo Tier 0 en mode `Enforce $false`

Créer les Authentication Policies (utilisateurs, ordinateurs, services)

Assigner les policies au Silo

Ajouter progressivement les comptes et hôtes au Silo

Monitorer quotidiennement les événements 4820/4821

Traiter chaque violation d'audit (compte ou hôte oublié)

Documenter les exceptions légitimes identifiées

Phase 3 — Passage en Enforce (J+30)

Valider zéro violation non résolue sur les 7 derniers jours

Informer les équipes opérationnelles et le helpdesk

Préparer la procédure break-glass documentée

Passer les Authentication Policies en `Enforce $true`

Passer le Silo en `Enforce $true`

Monitorer en temps réel les 2 premières heures

Revue J+1 et J+7 post-enforcement

Phase 4 — Opérations courantes

Rapport d'audit hebdomadaire automatisé sur les événements Silo

Procédure de gestion des nouveaux comptes Tier 0 (onboarding)

Revue trimestrielle des membres des Silos

Test semestriel de la procédure break-glass

Intégration dans le processus de review Tiering AD

FAQ — Authentication Silos Windows Server 2025

Quelle est la différence entre Authentication Policy et Authentication Silo ?

Une **Authentication Policy** est un objet AD qui définit les règles Kerberos : durée de vie du TGT, conditions d'accès en SDDL, mode audit ou enforce. Un **Authentication Silo** est un conteneur qui regroupe des comptes (utilisateurs, ordinateurs, services) et leur associe des Authentication Policies spécifiques pour chaque type. Le Silo crée l'étanchéité entre groupes de comptes ; la Policy définit les règles qui s'appliquent dans ce compartiment. On peut avoir des Policies sans Silo (assignées directement à un compte), mais l'usage en Silo est la pratique recommandée pour le cloisonnement Tier 0.

Authentication Silos est-il compatible avec Windows Server 2019 ?

Oui, les Authentication Silos sont disponibles dès Windows Server 2012 R2 pour les contrôleurs de domaine. Windows Server 2019 les supporte pleinement. Cependant, Windows Server 2025 apporte des améliorations significatives : support FAST sur les RODC, meilleure intégration Azure AD Kerberos, journalisation opérationnelle enrichie et durée de TGT granulaire par politique. Si votre infrastructure est en 2019, vous bénéficiez des fonctionnalités de base des Silos, mais nous recommandons de planifier la migration vers 2025 pour les DC Tier 0 afin de profiter de ces apports.

Comment tester un Authentication Silo sans impact production ?

La méthode recommandée est le déploiement en trois étapes : (1) créer le Silo et les Policies avec `-Enforce $false`, ce qui génère des événements d'audit sans bloquer aucune authentification ; (2) surveiller les événements 4820 et 4821 pendant 2 à 4 semaines pour identifier tous les comptes et hôtes qui seraient bloqués en mode Enforce ; (3) corriger les configurations (ajouter les comptes/hôtes oubliés) puis passer en Enforce uniquement quand zéro violation non résolue n'est détectée sur 7 jours consécutifs. Vous pouvez également tester sur un domaine de lab avec un niveau fonctionnel 2012 R2 minimum avant le déploiement en production.

Quels événements Windows surveiller après déploiement ?

Les événements critiques à monitorer dans le journal Security des contrôleurs de domaine sont : **4820** (TGT refusé — violation de politique utilisateur), **4821** (ticket de service refusé), **4822** (NTLM bloqué par Authentication Policy), **4823** (NTLM requis mais non autorisé), et **4769** avec Status `0xC0000413` (erreur KDC_ERR_POLICY). En mode Audit, ces événements sont journalisés sans blocage. En mode Enforce, ils accompagnent un refus effectif. Configurez des alertes dans votre SIEM sur les événements 4820/4821/4822 pour être notifié en temps réel des tentatives d'accès non conformes.

Authentication Silos remplace-t-il Protected Users ?

Non, les deux mécanismes sont complémentaires. Le groupe **Protected Users** agit sur le protocole d'authentification : il désactive NTLM, WDigest et CredSSP pour les membres, et limite la durée des TGT à 4 heures non renouvelables. Les **Authentication Silos** agissent sur la topologie : ils définissent depuis quels hôtes un compte peut s'authentifier. Protected Users sécurise le "comment" de l'authentification ; les Silos sécurisent le "depuis où". La pratique optimale recommandée par l'ANSSI pour les comptes Tier 0 est d'utiliser les deux simultanément, en ajoutant LAPS sur les PAW membres du Silo pour couvrir la gestion des mots de passe locaux.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory

