# LDAP Signing et LDAP Channel Binding : Durcissement Active Directory

> LDAP Signing et Channel Binding sous Active Directory : activer, auditer, tester et depanner. Protegez vos DC contre les attaques LDAP relay en 2026.

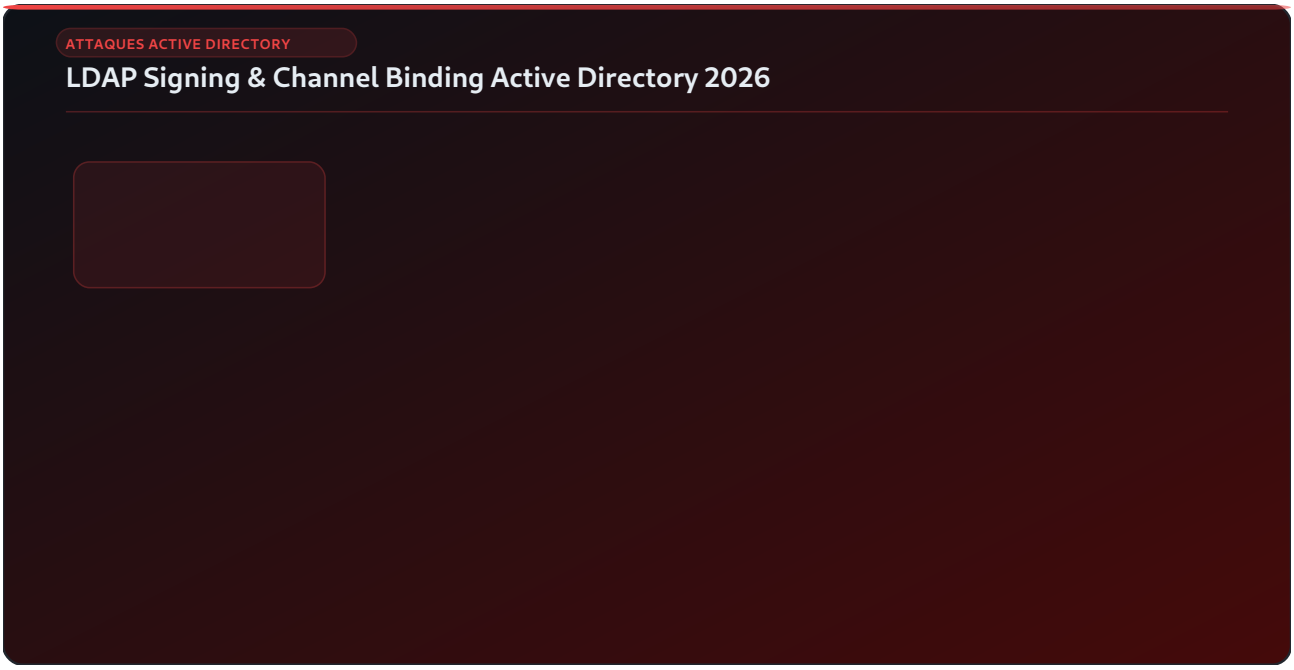
La sécurité du protocole LDAP (Lightweight Directory Access Protocol) est au cœur de la protection des infrastructures Active Directory en entreprise. Depuis la divulgation de la CVE-2017-8563, qui démontre comment un attaquant peut effectuer une élévation de privilèges via une attaque NTLM relay exploitant LDAP non signé, l'activation du LDAP Signing et du LDAP Channel Binding est devenue une priorité absolue pour les équipes sécurité. Pourtant, en 2026, de nombreuses organisations françaises — notamment dans les secteurs de la banque, de la santé et de l'industrie — n'ont toujours pas activé ces contrôles, craignant de casser des applications métier. Ce guide expert explique pourquoi ces deux mécanismes sont complémentaires et non interchangeables, comment les déployer sans interruption de service, comment auditer votre parc avant enforcement, et comment s'aligner sur les recommandations de l'ANSSI et les exigences de la directive NIS2 (article 21). Que vous soyez RSSI d'une PME industrielle de Normandie ou architecte sécurité d'un groupe bancaire parisien, ce guide vous donne les clés pour durcir vos contrôleurs de domaine contre les attaques LDAP relay modernes.

📋 EN BREF

**Points clés à retenir**

- LDAP non signé permet à un attaquant MitM de relayer des authentifications NTLM vers vos DC et créer des comptes privilégiés
- LDAP Signing protège l'intégrité des paquets LDAP ; Channel Binding lie l'authentification au canal TLS — les deux sont nécessaires
- Les événements 2886, 2887, 2888, 3039, 3040, 3041 permettent d'identifier les clients non compatibles avant enforcement

- Déployez en mode audit (Negotiate/When Supported) puis passez en enforcement après 2 à 4 semaines de surveillance
- LDAPS (port 636) est complémentaire mais ne remplace pas LDAP Signing pour les connexions intra-domaine
- L'ANSSI recommande explicitement ces deux contrôles dans son guide Active Directory 2023




### 1.1 Le protocole LDAP et ses faiblesses natives

LDAP est le protocole de communication principal entre les clients Windows et les contrôleurs de domaine Active Directory. Par défaut, LDAP v2 et LDAP v3 ne garantissent ni la confidentialité, ni l'intégrité des échanges. Un paquet LDAP en transit peut être lu, modifié, ou rejoué par un attaquant positionné sur le réseau. Sans signature cryptographique, rien n'empêche un acteur malveillant d'intercepter une requête LDAP légitime et d'y substituer des données

falsifiées — par exemple pour modifier les attributs d'un compte utilisateur ou ajouter un membre à un groupe privilégié.

Ce problème est amplifié dans les environnements qui utilisent encore NTLM (NT LAN Manager) comme mécanisme d'authentification, ce qui est le cas de la grande majorité des Active Directory en production en France. NTLM est un protocole challenge-response qui ne lie pas l'authentification à la session réseau : si un attaquant peut capturer le challenge NTLM d'un utilisateur, il peut le relayer vers un autre service — notamment LDAP sur les DC — pour s'authentifier en son nom.

### 1.2 Anatomie d'une attaque LDAP relay moderne

Une attaque LDAP relay classique se déroule en quatre étapes. L'attaquant, positionné sur le réseau interne (suite à un phishing, une compromission d'un poste de travail, ou un accès physique), déploie des outils comme Responder et ntlmrelayx de la suite Impacket.

**Étape 1 — Empoisonnement LLMNR/NBT-NS :** Responder écoute les requêtes de résolution de noms broadcast (LLMNR, NetBIOS, mDNS) et répond à la place du serveur légitime, forçant la victime à s'authentifier auprès de la machine de l'attaquant.

**Étape 2 — Capture du challenge NTLM :** La victime envoie ses credentials NTLM (hash NTLMv1 ou NTLMv2) à la machine de l'attaquant qui agit comme relai.

**Étape 3 — Relay vers LDAP sur le DC :** ntlmrelayx relaie immédiatement ce challenge vers le contrôleur de domaine via LDAP (port 389), en se faisant passer pour la victime.

**Étape 4 — Exploitation :** Si la victime est membre d'un groupe privilégié (Domain Admins, Account Operators, etc.), l'attaquant peut créer un nouveau compte, modifier des ACLs, ou activer la délégation Kerberos non contrainte — ouvrant la voie à une compromission totale du domaine.

```
 # Exemple d'attaque LDAP relay (à des fins de test en lab uniquement)
# Étape 1 : Démarrer Responder en mode analyse passive
sudo responder -I eth0 -A

# Étape 2 : Lancer ntlmrelayx vers le DC en ciblant LDAP
python3 ntlmrelayx.py -t ldap://dc01.domain.local --escalate-user compromised_user

# Sans LDAP Signing, ntlmrelayx peut :
# - Dumper les utilisateurs du domaine
# - Ajouter un utilisateur au groupe Domain Admins
# - Modifier les ACLs pour DCSync
```

Sans LDAP Signing, cette attaque fonctionne en quelques secondes. Avec LDAP Signing en mode **Require**, le DC rejette toute connexion LDAP non signée cryptographiquement — le relay échoue immédiatement car l'attaquant ne possède pas la clé de session nécessaire pour signer les paquets.

Pour approfondir les mécanismes d'attaque NTLM relay dans leur globalité, consultez notre article dédié : Attaques NTLM Relay 2026 : techniques et défenses.

---

## 2. LDAP Signing : fonctionnement et niveaux de configuration

### 2.1 Comment fonctionne la signature LDAP

Le LDAP Signing (ou signature LDAP) utilise le mécanisme SASL (Simple Authentication and Security Layer) pour garantir l'intégrité des paquets LDAP échangés entre un client et un serveur. Lorsqu'il est activé, chaque paquet LDAP est signé cryptographiquement via GSSAPI/Kerberos ou NTLM, permettant au récepteur de vérifier qu'il n'a pas été modifié en transit. La confidentialité n'est pas assurée par la signature seule (pour cela, il faut LDAPS ou LDAP avec STARTTLS), mais l'intégrité est garantie.

> ⚡ **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.

Le signing LDAP opère à deux niveaux indépendants :

**Côté serveur (DC)** : contrôlé par la clé de registre `LDAPServerIntegrity` sous `HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`

**Côté client** : contrôlé par la clé `LDAPClientIntegrity` sous `HKLM\SYSTEM\CurrentControlSet\Services\ldap`

### 2.2 Les trois niveaux de signing côté serveur

| Valeur | Nom | Comportement | Risque |
|---|---|---|---|
| **0** | None | Aucune signature requise ni proposée | Critique — relay trivial |
| **1** | Negotiate Signing | Signature si le client la supporte, connexion acceptée sinon (défaut Windows) | Moyen — relay possible contre clients legacy |
| **2** | Require Signing | Toute connexion LDAP non signée est refusée | Faible — relay LDAP bloqué |

La valeur par défaut depuis Windows Server 2019 est **1 (Negotiate)**, ce qui signifie que les clients qui ne demandent pas de signature peuvent encore se connecter sans signing — laissant une fenêtre d'attaque ouverte. Microsoft avait initialement prévu de passer la valeur par défaut à **2 (Require)** en mars 2020 (ADV190023), mais a repoussé ce changement en raison des impacts

sur les applications tierces. En 2026, ce passage en Require reste une action manuelle que les administrateurs doivent planifier.

### 2.3 Impact sur les clients legacy

Le principal obstacle à l'activation de LDAP Signing en mode Require est la présence de clients qui utilisent des connexions LDAP simple bind (sans SASL) ou des bibliothèques LDAP anciennes qui ne supportent pas la signature. Les catégories les plus fréquemment impactées dans les environnements français comprennent :

Anciennes versions de Java (pré-OpenJDK 11) avec JNDI LDAP sans TLS

Équipements réseau (switchs, imprimantes multifonctions) avec firmware ancien

Applications PHP utilisant `ldap_bind()` sans option LDAP_OPT_X_TLS

Certains scanners de documents Ricoh, Xerox, Canon avec firmware antérieur à 2018

Logiciels RH ou ERP développés en interne sans mise à jour depuis 2015

C'est pourquoi la phase d'audit préalable — décrite en section 6 — est absolument critique avant tout enforcement.

---

## 3. LDAP Channel Binding : protection contre le relay TLS

### 3.1 Le problème que Channel Binding résout

LDAP Signing protège les connexions LDAP non-TLS. Mais que se passe-t-il si un attaquant effectue un relay via LDAPS (LDAP sur TLS, port 636) ? Dans ce cas, la signature LDAP seule ne suffit pas, car la session TLS crée une encapsulation qui neutralise la vérification de signature au niveau SASL.

LDAP Channel Binding, basé sur le mécanisme **EPA (Extended Protection for Authentication)** défini dans la RFC 5056 et l'extension Microsoft MS-NLMP, lie cryptographiquement l'authentification NTLM ou Kerberos au canal TLS sous-jacent. Concrètement, lors d'une

connexion LDAPS, le client calcule un token qui incorpore le hash du certificat TLS du serveur (Channel Binding Token ou CBT). Ce token est inclus dans l'authentification GSSAPI.

Si un attaquant intercepte la connexion TLS et tente de la relayer vers un autre serveur, le certificat TLS change — donc le CBT ne correspond plus — et le DC rejette l'authentification. Le relay LDAP via TLS devient impossible.

### 3.2 Les trois niveaux de Channel Binding

| Valeur | Nom | Comportement |
|---|---|---|
| **0** | Never | Channel Binding ignoré (défaut pré-patch) |
| **1** | When supported | Channel Binding vérifié si le client l'envoie, connexion acceptée sinon (recommandé pour transition) |
| **2** | Always | Channel Binding obligatoire — toute connexion LDAPS sans CBT valide est rejetée |

La valeur **1 (When supported)** est le compromis recommandé pour la plupart des environnements en phase de transition. Elle bloque les attaques relay TLS contre les clients modernes tout en préservant la compatibilité avec les équipements legacy qui ne supportent pas encore EPA.

### 3.3 Prérequis : certificat TLS sur les DC

Channel Binding nécessite que vos contrôleurs de domaine disposent d'un certificat TLS valide pour les connexions LDAPS. Dans un environnement Active Directory, ce certificat est généralement émis par votre PKI d'entreprise (ADCS — Active Directory Certificate Services). Si vous n'avez pas encore de PKI interne, consultez notre guide complet : Architecture PKI entreprise avec ADCS.

## 4. Activation via GPO : guide étape par étape

### 4.1 LDAP Signing via GPO

La méthode recommandée pour déployer LDAP Signing sur tous vos contrôleurs de domaine est via une GPO liée à l'OU Domain Controllers. Cette approche garantit une configuration cohérente et tracée dans votre politique de sécurité.

**Chemin GPO pour LDAP Signing (côté serveur DC) :**

`Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → "Domain controller: LDAP server signing requirements"`

**Étapes de configuration :**

Ouvrez la **Group Policy Management Console** (gpmc.msc) sur un serveur membre ou depuis un poste d'administration avec RSAT

Naviguez vers **Forest → Domains → [votre domaine] → Domain Controllers**

Créez une nouvelle GPO : clic droit → **"Create a GPO in this domain, and Link it here..."** → nommez-la *DC-Security-LDAP-Hardening*

Éditez la GPO, naviguez vers le chemin indiqué ci-dessus

Double-cliquez sur **"Domain controller: LDAP server signing requirements"**

Sélectionnez **"Require signing"** pour l'enforcement complet, ou **"Negotiate signing"** en phase audit

Cliquez **OK** et fermez l'éditeur GPO

Forcez la mise à jour GPO sur les DC : `Invoke-GPUpdate -Computer dc01 -Force` ou attendez le prochain cycle de 5 minutes

**Chemin GPO pour LDAP Signing côté client (tous les postes du domaine) :**

`Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → "Network security: LDAP client signing requirements"`

Les valeurs disponibles pour le client sont identiques : **None**, **Negotiate signing**, **Require signing**. Configurez-le à **"Require signing"** après avoir validé la compatibilité de vos applications.

### 4.2 LDAP Channel Binding via GPO

À partir de Windows Server 2022 et via le KB4520412 sur Server 2016/2019, un paramètre GPO natif est disponible pour Channel Binding :

**Chemin GPO :**

`Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → "Domain controller: LDAP server channel binding token requirements"`

Les options disponibles sont :

**Never** — aucune vérification (déconseillé)

**When supported** — recommandé pour la transition

**Always** — enforcement strict (cible finale)

Si ce paramètre n'apparaît pas dans votre GPMC, vous devez importer les fichiers ADMX mis à jour. Téléchargez les *Administrative Templates (.admx)* pour Windows Server 2022 depuis le Microsoft Download Center et copiez-les dans `\\[domain]\SYSVOL\[domain]\Policies\PolicyDefinitions\`.

## 5. Activation via PowerShell et Registre

### 5.1 Vérification de l'état actuel

```
 # Vérifier le niveau de signing actuel sur les DC
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LDAPServerIntegrity" -ErrorAction SilentlyContinue
# 0 = None, 1 = Negotiate (défaut), 2 = Require
# Si la clé n'existe pas, la valeur effective est 1 (Negotiate)

# Vérifier Channel Binding
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LdapEnforceChannelBinding" -ErrorAction SilentlyContinue
# 0 = Never, 1 = When supported, 2 = Always
# Si absente, valeur effective = 0 (Never) sur serveurs non patchés

# Vérifier sur plusieurs DC en une commande
$DCs = (Get-ADDomainController -Filter *).HostName
foreach ($DC in $DCs) {
    $reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine', $DC)
    $key = $reg.OpenSubKey("SYSTEM\CurrentControlSet\Services\NTDS\Parameters")
    $signing = $key.GetValue("LDAPServerIntegrity", "NOT SET")
    $binding = $key.GetValue("LdapEnforceChannelBinding", "NOT SET")
    Write-Host "$DC - Signing: $signing | ChannelBinding: $binding"
}
```

### 5.2 Activation de LDAP Signing

```
 # Activer LDAP Signing en mode "Require" (valeur 2) sur le DC local
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LDAPServerIntegrity" -Value 2 -Type DWord

# Pour une transition progressive, utiliser Negotiate d'abord (valeur 1)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LDAPServerIntegrity" -Value 1 -Type DWord

# IMPORTANT : aucun redémarrage du service NTDS n'est nécessaire
# La modification prend effet immédiatement (hot-reload)

# Déployer sur tous les DC du domaine via PowerShell remoting
$DCs = (Get-ADDomainController -Filter *).HostName
Invoke-Command -ComputerName $DCs -ScriptBlock {
    Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
        -Name "LDAPServerIntegrity" -Value 2 -Type DWord
    Write-Host "$(hostname) : LDAP Signing set to Require"
} -Credential (Get-Credential)
```

### 5.3 Activation de LDAP Channel Binding

```
 # Activer LDAP Channel Binding en mode "When supported" (valeur 1)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LdapEnforceChannelBinding" -Value 1 -Type DWord
# 0 = Never, 1 = When supported (recommandé), 2 = Always

# Mode enforcement strict "Always" (valeur 2) - après validation complète
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LdapEnforceChannelBinding" -Value 2 -Type DWord

# Déployer sur tous les DC
$DCs = (Get-ADDomainController -Filter *).HostName
Invoke-Command -ComputerName $DCs -ScriptBlock {
    Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
        -Name "LdapEnforceChannelBinding" -Value 1 -Type DWord
    Write-Host "$(hostname) : Channel Binding set to When Supported"
} -Credential (Get-Credential)
```

### 5.4 Test de connexion LDAP signée

```
 # Test de connexion LDAP avec signing activé
$conn = New-Object System.DirectoryServices.DirectoryEntry(
    "LDAP://dc01.domain.local",
    "domain\testuser",
    "P@ssword!"
)
$conn.AuthenticationType = [System.DirectoryServices.AuthenticationTypes]::Signing

try {
    $null = $conn.NativeObject
    Write-Host "Connexion LDAP signée : SUCCÈS" -ForegroundColor Green
} catch {
    Write-Host "Connexion LDAP signée : ÉCHEC - $_" -ForegroundColor Red
}

# Test avec ldp.exe (outil GUI intégré Windows)
# Lancez ldp.exe → Connection → Connect (dc01, port 389)
# Puis Connection → Bind → Choisir "Simple Bind" pour tester le rejet
# Si Require Signing est actif, le simple bind doit échouer avec erreur 8 (LDAP_AUTH_METHOD_NOT_S
```

## 6. Audit avant activation : identifier les clients non compatibles

### 6.1 Les événements Windows à surveiller

Avant d'activer LDAP Signing en mode Require, il est impératif d'identifier tous les clients qui effectuent des connexions LDAP non signées. Windows Server génère des événements d'audit spécifiques dans le journal **Directory Service** (Observateur d'événements → Journaux des applications et des services → Microsoft → Windows → ActiveDirectory_DomainService → Operational).

| Event ID | Signification | Action requise |
|---|---|---|
| **2886** | Le DC n'impose pas le signing LDAP — avertissement de sécurité généré au démarrage | Activer le signing pour faire disparaître cet événement |
| **2887** | Résumé périodique du nombre de connexions non signées dans les dernières 24h | Identifier les sources et les corriger avant enforcement |
| **2888** | Résumé des tentatives de simple bind rejetées (après enforcement) | Surveiller après activation de Require pour détecter les clients cassés |
| **3039** | Client LDAP sans Channel Binding Token (CBT) lors d'une connexion TLS | Identifier les clients pour mise à jour ou configuration EPA |
| **3040** | Client LDAP avec CBT incorrect lors d'une connexion TLS | Indique potentiellement un relay en cours ou un client buggé |
| **3041** | Résumé des échecs Channel Binding dans les dernières 24h | Surveiller en continu après activation |

### 6.2 Collecte et analyse des événements par PowerShell

```
 # Vérifier les événements d'audit sur le DC local
Get-WinEvent -FilterHashtable @{
    LogName = 'Directory Service'
    Id = 2886, 2887, 2888, 3039, 3040, 3041
} -MaxEvents 100 |
    Select-Object TimeCreated, Id, Message |
    Format-Table -AutoSize -Wrap

# Extraire les adresses IP des clients non signés depuis l'événement 2887
Get-WinEvent -FilterHashtable @{LogName='Directory Service'; Id=2887} |
    ForEach-Object {
        if ($_.Message -match "client IP address : (.+)") {
            [PSCustomObject]@{
                Date    = $_.TimeCreated
                EventID = $_.Id
                Client  = $matches[1]
            }
        }
    } | Group-Object Client | Sort-Object Count -Descending |
    Select-Object Count, Name | Format-Table

# Collecter sur tous les DC du domaine
$DCs = (Get-ADDomainController -Filter *).HostName
$allEvents = foreach ($DC in $DCs) {
    Get-WinEvent -ComputerName $DC -FilterHashtable @{
        LogName = 'Directory Service'
        Id = 2886, 2887, 2888, 3039, 3040, 3041
        StartTime = (Get-Date).AddDays(-7)
    } -ErrorAction SilentlyContinue |
    Select-Object @{N='DC';E={$DC}}, TimeCreated, Id, Message
}
$allEvents | Export-Csv -Path "C:\Audit\LDAP-Signing-Audit.csv" -NoTypeInformation -Encoding UTF8
```

### 6.3 Activer la journalisation détaillée LDAP (diagnostic logging)

```
 # Activer la journalisation LDAP Interface Events (niveau 2 = basique, 5 = verbose)
# ATTENTION : niveau 5 génère beaucoup de logs — utiliser en courte durée uniquement
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" `
    -Name "16 LDAP Interface Events" -Value 2 -Type DWord

# Vérifier les connexions simple bind non sécurisées
# Elles apparaissent dans l'Event Log avec l'adresse IP source du client

# Désactiver après audit (revenir à 0)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics" `
    -Name "16 LDAP Interface Events" -Value 0 -Type DWord
```

Pour une stratégie de durcissement AD globale incluant la gestion des comptes de service et des délégations Kerberos, référez-vous à notre guide : Sécuriser Active Directory : le guide définitif.

---

## 7. Plan de déploiement progressif en production française

### 7.1 Les quatre phases de déploiement

Un déploiement réussi de LDAP Signing et Channel Binding en production nécessite une approche en quatre phases. Cette méthodologie est particulièrement adaptée aux environnements français qui combinent souvent des applications métier critiques (ERP, SIRH, GED) avec des contraintes de disponibilité fortes.

**Phase 1 — Inventaire et audit (semaines 1-2) :**

Activer la journalisation LDAP (diagnostic level 2) sur tous les DC

Collecter les événements 2887 et 3039 pendant 7 à 14 jours

Identifier toutes les sources de connexions LDAP non signées (IP, application, service)

Cartographier les applications tierces utilisant LDAP (voir section 10)

**Phase 2 — Mode Negotiate / When Supported (semaines 3-4) :**

Configurer LDAP Signing à **1 (Negotiate)** sur les DC si ce n'est pas déjà le cas

Configurer Channel Binding à **1 (When supported)**

Continuer la surveillance des événements

Corriger ou mettre à jour les clients identifiés en phase 1

**Phase 3 — Enforcement progressif (semaines 5-8) :**

Commencer par les DC de test ou les sites secondaires

Passer LDAP Signing à **2 (Require)** sur un DC à la fois

Surveiller les événements 2888 (connexions rejetées) pendant 48h

Si zéro événement, passer au DC suivant

En cas d'incident, rollback immédiat via GPO ou registry

**Phase 4 — Full enforcement et Channel Binding Always (semaine 9+) :**

Tous les DC en mode **Require** pour Signing

Passer Channel Binding de **1 (When supported)** à **2 (Always)** après validation LDAPS complète

Supprimer la journalisation verbose (revenir à diagnostic level 0)

Documenter la configuration dans votre CMDB et politique de sécurité

### 7.2 Rollback d'urgence

```
 # Rollback immédiat en cas d'incident (revenir à Negotiate)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LDAPServerIntegrity" -Value 1 -Type DWord

# Si la GPO bloque le rollback registry, créer une GPO d'override en priorité haute
# GPO: "DC-EMERGENCY-LDAP-Signing-Off" liée en premier sur l'OU Domain Controllers
# Valeur: Negotiate signing (pour ne pas couper totalement)
```

Pour les recommandations officielles Microsoft sur le durcissement AD, consultez : [Recommandations Microsoft pour le durcissement Active Directory].

# 8. LDAPS : LDAP over TLS port 636

## 8.1 LDAPS vs LDAP Signing : complémentarité, pas substitution

Une confusion fréquente dans les équipes IT consiste à croire que LDAPS (LDAP sur TLS, port 636) remplace LDAP Signing. En réalité, ces deux mécanismes protègent contre des menaces différentes et doivent être déployés ensemble pour une protection complète.

| Critère | LDAP Signing (port 389) | LDAPS (port 636) |
|---|---|---|
| Intégrité | Oui (SASL signing) | Oui (TLS) |
| Confidentialité | Non | Oui (chiffrement TLS) |
| Protection relay | Oui (avec Channel Binding) | Partielle (sans Channel Binding) |
| Prérequis certificat | Non (pour signing seul) | Oui (PKI obligatoire) |
| Port | 389 (TCP/UDP) | 636 (TCP) |
| Compatibilité legacy | Bonne | Nécessite mise à jour client |

## 8.2 Configuration LDAPS sur les contrôleurs de domaine

LDAPS est automatiquement disponible sur les DC lorsqu'un certificat TLS est installé dans le magasin *Personal* du compte *Computer*. Le certificat doit satisfaire aux conditions suivantes :

Le Subject ou Subject Alternative Name contient le FQDN du DC

Le certificat a l'Enhanced Key Usage (EKU) Server Authentication (OID 1.3.6.1.5.5.7.3.1)

La chaîne de certification est approuvée par les clients

Le certificat n'est pas expiré

```
 # Vérifier si LDAPS fonctionne sur le DC local
$conn = New-Object System.DirectoryServices.DirectoryEntry("LDAPS://dc01.domain.local:636")
try {
    $null = $conn.NativeObject
    Write-Host "LDAPS : OPÉRATIONNEL" -ForegroundColor Green
} catch {
    Write-Host "LDAPS : NON DISPONIBLE - $_" -ForegroundColor Red
}

# Tester LDAPS depuis la ligne de commande
# openssl s_client -connect dc01.domain.local:636 -showcerts

# Lister les certificats installés sur le DC pouvant activer LDAPS
Get-ChildItem -Path Cert:\LocalMachine\My |
    Where-Object { $_.EnhancedKeyUsageList -match "Server Authentication" } |
    Select-Object Subject, NotAfter, Thumbprint
```

### 8.3 Forcer LDAPS uniquement (désactiver LDAP non-TLS)

Pour les environnements haute sécurité (secteur financier, opérateurs d'importance vitale), il est possible de désactiver complètement LDAP non chiffré sur les DC :

```
 # Désactiver les connexions LDAP non-TLS (port 389) — ATTENTION : impact majeur possible
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
    -Name "LDAPServerDisallow" -Value 1 -Type DWord

# Cette opération bloque également LDAP avec SASL signing sur port 389
# N'effectuer qu'après validation complète de la migration vers LDAPS
```

## 9. Impact sur les applications tierces

### 9.1 Veeam Backup et Replication

Veeam utilise LDAP pour la découverte des contrôleurs de domaine et l'authentification lors de la configuration de jobs de sauvegarde. Les versions récentes (v12+) supportent nativement LDAP Signing. Pour les versions antérieures :

Mettre à jour Veeam vers la version 12 minimum

Vérifier que le compte de service Veeam utilise Kerberos (pas NTLM) pour l'authentification AD

Tester la connexion après activation : Admin Console → Credentials → Verify

### 9.2 Microsoft SCCM / Configuration Manager

SCCM utilise intensivement LDAP pour la découverte des ressources AD (ordinateurs, utilisateurs, groupes). La méthode AD System Discovery et AD User Discovery peuvent être affectées si elles utilisent des connexions LDAP non signées.

Vérifier la version SCCM : Current Branch 2203+ supporte LDAP Signing

Dans Administration → Discovery Methods → Active Directory System Discovery : s'assurer que le compte de découverte utilise les protocoles modernes

Surveiller les événements SCCM après enforcement : distmgr.log, adsgdis.log

### 9.3 Network Policy Server (NPS) et authentification RADIUS

NPS utilise LDAP pour valider les appartenances aux groupes lors de l'authentification RADIUS (VPN, WiFi 802.1X). Après activation de LDAP Signing :

NPS sur Windows Server 2016+ supporte LDAP Signing nativement

Vérifier les logs NPS : Observateur d'événements → Windows Logs → Security (Event 6273 pour les échecs d'authentification NAS)

Tester avec un compte de test avant enforcement pour les flux WiFi et VPN critiques

### 9.4 VPN et équipements réseau

Les équipements VPN (Cisco ASA/FTD, Palo Alto, Fortinet FortiGate, Check Point) utilisent LDAP pour l'authentification des utilisateurs. Le niveau de support LDAP Signing varie selon le fournisseur et la version firmware :

**Cisco ASA 9.14+** : Supporte LDAP over SSL (LDAPS, port 636) — migrer vers LDAPS plutôt que LDAP Signing

**Palo Alto PAN-OS 10.1+** : Profil LDAP avec option "Require SSL/TLS" disponible

**Fortinet FortiOS 7.x** : Supporte LDAPS mais pas LDAP Signing SASL — migrer vers port 636

**Copieurs réseau (Ricoh, Xerox, Canon)** : Vérifier firmware — souvent nécessite mise à jour ou migration vers LDAPS

### 9.5 Applications Java et frameworks d'authentification

Les applications utilisant JNDI (Java Naming and Directory Interface) pour LDAP peuvent être impactées. Depuis Java 8u181, JNDI désactive par défaut les connexions LDAP simple bind non sécurisées. Pour les applications Java en production :

```
 # Vérifier la configuration LDAP Java de l'application
# Chercher dans les propriétés de connexion LDAP :
# java.naming.security.authentication = "simple" (problématique sans TLS)
# java.naming.security.authentication = "GSSAPI" (Kerberos, compatible signing)

# Pour les applications Spring/Spring Security LDAP :
# spring.ldap.base=dc=domain,dc=local
# spring.ldap.urls=ldaps://dc01.domain.local:636  (migrer vers LDAPS)
# spring.ldap.username=cn=ldapbind,ou=service,dc=domain,dc=local
```

La relation entre NTLM relay sur LDAP et les attaques Pass-the-Hash est directe : une fois qu'un attaquant a compromis un compte via relay, il peut effectuer du Pass-the-Hash. Consultez notre analyse : Pass-the-Hash : anatomie de l'attaque NTLM.

## 10. Checklist ANSSI/NIS2 : conformité et gouvernance

### 10.1 Alignement ANSSI Guide Active Directory 2023

L'ANSSI publie depuis 2021 un guide de référence pour la sécurisation des Active Directory, mis à jour en 2023. Ce guide classe le LDAP Signing et le Channel Binding parmi les mesures de **niveau 1 (indispensable)**, soit la priorité maximale. Les organisations françaises soumises à la réglementation NIS2 (secteurs énergie, transport, banque, santé, eau, infrastructure numérique et bien d'autres depuis octobre 2024) ont une obligation réglementaire d'implémenter ces contrôles au titre de l'article 21 (mesures de gestion des risques).

### 10.2 Checklist complète de conformité

Le déploiement de LDAPS repose sur une PKI robuste. Notre guide ADCS Offline Root CA : Architecture PKI Sécurisée Windows Server 2025 détaille la mise en place d'une hiérarchie à deux niveaux, la gestion des templates et la protection contre les attaques ESC1-ESC8.

Au-delà du chiffrement LDAP, Windows Server 2025 introduit également SMB over QUIC, qui permet d'exposer les partages fichiers sur internet avec TLS 1.3 intégré, sans VPN — une alternative moderne pour le télétravail sécurisé.

**À RETENIR**

**Checklist LDAP Signing et Channel Binding — ANSSI/NIS2**

[ ] Inventaire complet des clients LDAP réalisé (événements 2887 analysés sur min. 7 jours)

[ ] Toutes les applications tierces testées en environnement de pré-production

[ ] LDAP Signing configuré à **Require (2)** sur tous les DC via GPO

[ ] LDAP Client Signing configuré à **Require** sur tous les postes du domaine

[ ] Channel Binding configuré à **When supported (1)** minimum sur tous les DC

[ ] Certificats TLS valides installés sur tous les DC (prérequis Channel Binding et LDAPS)

> [ ] LDAPS (port 636) testé et fonctionnel pour les applications qui le requièrent
>
> [ ] Journalisation des événements LDAP activée et intégrée dans le SIEM
>
> [ ] Plan de rollback documenté et testé
>
> [ ] Configuration documentée dans la politique de sécurité AD et la CMDB
>
> [ ] Revue trimestrielle planifiée pour vérifier la non-régression
>
> [ ] Preuve de conformité disponible pour l'audit NIS2 (capture GPO, export registry)

### 10.3 Export de preuves pour audit de conformité

```
 # Générer un rapport de conformité LDAP Signing pour audit
$report = @()
$DCs = (Get-ADDomainController -Filter *).HostName

foreach ($DC in $DCs) {
    $signing = Invoke-Command -ComputerName $DC -ScriptBlock {
        (Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
            -Name LDAPServerIntegrity -ErrorAction SilentlyContinue).LDAPServerIntegrity
    }
    $binding = Invoke-Command -ComputerName $DC -ScriptBlock {
        (Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
            -Name LdapEnforceChannelBinding -ErrorAction SilentlyContinue).LdapEnforceChannelBind
    }
    $report += [PSCustomObject]@{
        DC             = $DC
        SigningLevel   = switch($signing) { 0{"None"} 1{"Negotiate"} 2{"Require"} default{"Unknow
        BindingLevel   = switch($binding) { 0{"Never"} 1{"When Supported"} 2{"Always"} default{"U
        Compliant      = ($signing -eq 2 -and $binding -ge 1)
        Date           = Get-Date -Format "yyyy-MM-dd HH:mm"
    }
}

$report | Export-Csv "C:\Audit\LDAP-Compliance-$(Get-Date -Format 'yyyyMMdd').csv" -NoTypeInforma
$report | Format-Table -AutoSize
```

Pour une vision complète du durcissement Active Directory incluant les délégations Kerberos, les ACLs et les comptes de service, consultez notre guide de référence : [Guide définitif de sécurisation Active Directory].

# FAQ — LDAP Signing et Channel Binding

## LDAP Signing peut-il casser des applications tierces ?

Oui, si ces applications utilisent des connexions LDAP simple bind sans SASL signing. C'est particulièrement fréquent avec des équipements réseau anciens (copieurs, switchs), des applications Java non mises à jour, ou des logiciels développés en interne avant 2015. La phase d'audit préalable — analyse des événements 2886, 2887, 2888 — est indispensable pour identifier et corriger ces applications avant l'enforcement. Dans la grande majorité des cas, une mise à jour firmware ou une migration vers LDAPS résout le problème.

## Quelle est la différence entre LDAP Signing et LDAPS ?

LDAP Signing garantit l'intégrité des paquets LDAP sur le port standard 389 en utilisant SASL — les données ne sont pas chiffrées mais ne peuvent pas être modifiées en transit. LDAPS (port 636) encapsule LDAP dans TLS, garantissant à la fois l'intégrité et la confidentialité (chiffrement). Les deux sont complémentaires : LDAP Signing avec Channel Binding protège contre le relay NTLM, tandis que LDAPS protège également la confidentialité des données LDAP (mots de passe, attributs sensibles) contre l'écoute passive.

## Comment identifier les clients LDAP non signés avant enforcement ?

Activez la journalisation LDAP sur vos DC (Set-ItemProperty "16 LDAP Interface Events" -Value 2) et surveillez les événements ID 2887 dans le journal "Directory Service". L'événement 2887 liste le nombre de connexions LDAP non signées par heure avec les adresses IP source. Collectez ces données pendant minimum 7 jours ouvrés (incluant des week-ends pour les tâches planifiées) avant de passer en enforcement. L'outil Get-WinEvent avec filtrage sur les ID 2887 permet d'exporter facilement ces informations vers CSV pour analyse.

### Faut-il activer LDAP Signing et Channel Binding ensemble ?

Oui, les deux mécanismes sont complémentaires et protègent contre des vecteurs d'attaque différents. LDAP Signing (port 389) bloque les relay NTLM sur les connexions LDAP non-TLS. Channel Binding bloque les relay sur les connexions LDAPS (TLS, port 636). Un attaquant qui ne peut pas relay sur le port 389 peut tenter de relay via LDAPS si Channel Binding n'est pas activé. Déployez les deux simultanément, en commençant par le mode "Negotiate/When supported" puis en passant à l'enforcement complet.

### LDAP Channel Binding est-il requis par NIS2 en France ?

NIS2 (directive UE 2022/2555, transposée en France par ordonnance d'octobre 2024) exige à l'article 21 la mise en oeuvre de "mesures appropriées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information". L'ANSSI, dans son guide Active Directory 2023 et ses recommandations sectorielles, classe explicitement LDAP Signing et Channel Binding parmi les mesures de niveau 1 (indispensable). Pour les entités essentielles et importantes soumises à NIS2, ne pas activer ces contrôles constitue une non-conformité documentée, potentiellement sanctionnable lors d'un audit NIS2 par l'ANSSI. La réponse est donc oui — Channel Binding est attendu dans le cadre NIS2.

## Références et documentation


Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory