Durcissement ADFS : Guide de Hardening Windows Server 2025 — 2026

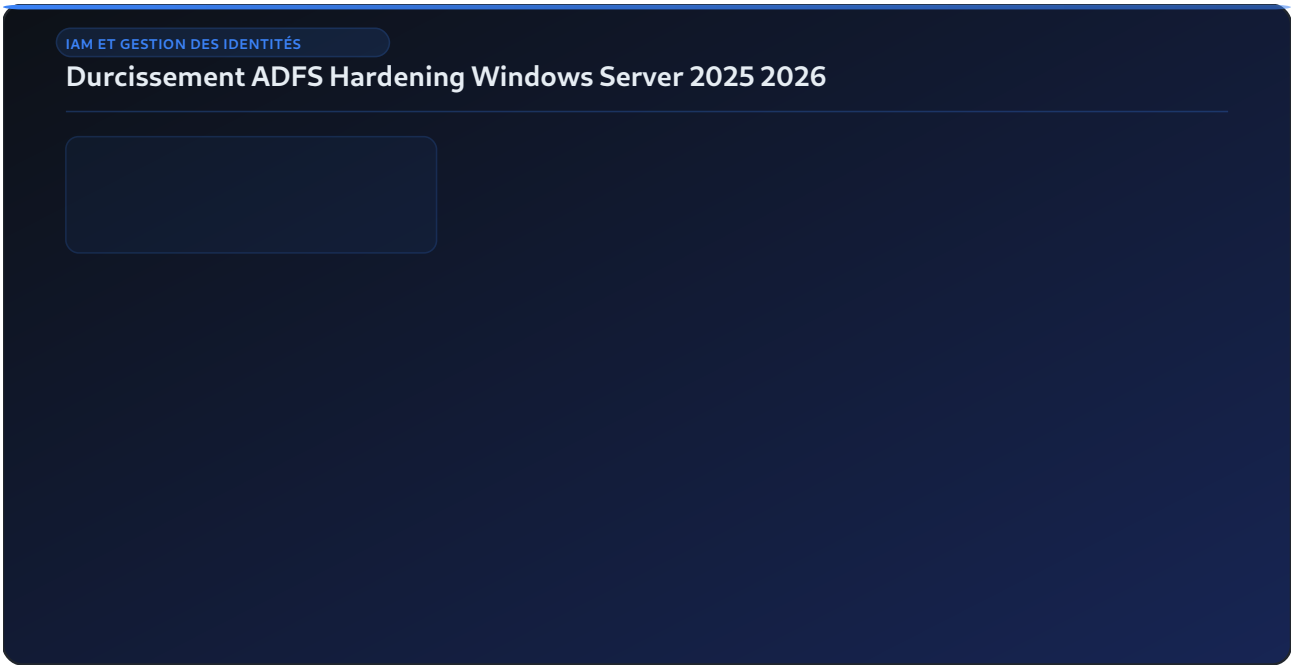
Guide complet durcissement ADFS Windows Server 2025 : TLS, endpoints, Extranet Lockout, MFA, claim rules, monitoring SIEM et conformité NIS 2 DORA.

📋 EN BREF

- ADFS reste déployé dans des milliers d'organisations françaises et européennes malgré la recommandation de Microsoft de migrer vers Entra ID — son durcissement est donc critique en 2026.
- Désactiver IdpInitiatedSignOn.aspx et tous les endpoints ADFS non nécessaires réduit drastiquement la surface d'attaque exposée au WAP et à Internet.
- L'Extranet Lockout ADFS (Soft + Hard) doit être activé dès le déploiement pour bloquer les attaques par force brute sur les comptes exposés en fédération.
- Les claim rules ADFS mal configurées permettent des élévations de privilèges invisibles — un audit trimestriel est indispensable pour les OES soumis à NIS 2 et DORA.
- La migration vers Entra ID doit être planifiée stratégiquement par phases, en commençant par les applications avec le plus faible risque de régression.

Active Directory Federation Services (ADFS) est au cœur de l'infrastructure d'authentification fédérée de milliers d'organisations françaises et européennes — administrations, banques, assurances, industriels soumis à DORA ou NIS 2. Malgré la recommandation de Microsoft de migrer vers Entra ID (Azure AD), ADFS reste incontournable dans de nombreux contextes : environnements air-gapped, exigences de souveraineté des données, contraintes réglementaires imposant une authentification on-premise. Le durcissement d'ADFS sur Windows Server 2025 est donc un sujet d'actualité brûlant pour les RSSI parisiens et les équipes IAM des grandes

organisations françaises. Ce guide technique complet couvre l'architecture sécurisée d'ADFS, le durcissement TLS, la sécurisation des endpoints, la gestion du verrouillage extranet, le MFA, l'audit des claim rules, le monitoring via Event IDs et KQL Sentinel, ainsi que la conformité NIS 2 et DORA applicable aux opérateurs de services essentiels (OES) et entités financières françaises. Les équipes IAM trouveront ici un référentiel opérationnel complet aligné sur les standards 2026.



Une architecture ADFS sécurisée repose sur plusieurs composants distincts avec des rôles bien définis. La séparation entre les couches publique et privée est fondamentale pour limiter l'exposition.

ADFS Farm : SQL Server vs WID

La Farm ADFS peut utiliser deux types de base de données interne :

Critère	WID (Windows Internal Database)	SQL Server
Nœuds max	5 serveurs (1 primaire en écriture)	Illimité
Haute disponibilité	Limitée (basculement manuel)	Always On, clustering
Recommandé pour	Moins de 1000 utilisateurs fédérés	Production enterprise, OES
Backup	Via Export-AdfsDeploymentSQLScript	SQL Server backup standard
SAML artifact resolution	Non supporté	Supporté

Pour les OES et entités financières soumises à DORA, SQL Server avec Always On est **obligatoire** pour garantir le RTO/RPO exigé.

Web Application Proxy (WAP) en DMZ

Le WAP est le point d'entrée public d'ADFS. Il doit être placé en DMZ, séparé de la Farm ADFS interne par un pare-feu :

```
Internet
    |
[WAP 1]  [WAP 2]  (DMZ — Windows Server 2025)
    |
[Pare-feu interne — règles strictes]
    |
[ADFS Farm interne]  (réseau privé)
    |
[Domain Controllers AD]
```

Règles pare-feu strictes entre WAP et Farm ADFS :

HTTPS (TCP 443) : WAP → ADFS Farm uniquement

HTTP (TCP 80) : bloqué (jamais de trafic ADFS en clair)

RDP (TCP 3389) : WAP → Jump Server uniquement, pas directement depuis Internet

Certificats ADFS : SSL, Token Signing, Token Decryption

ADFS utilise trois types de certificats distincts :

SSL/TLS : Certificat public pour adfs.ayinedjimi.fr — ECDSA P-384 recommandé, durée 1 an

Token Signing : Signe les tokens SAML/JWT — auto-généré par ADFS, durée 1 an avec auto-renouvellement

Token Decryption : Déchiffre les tokens chiffrés par les Relying Parties — auto-géré par ADFS

```
# Vérifier les certificats ADFS
Get-AdfsCertificate | Select-Object CertificateType, Thumbprint,
    @{N="ExpiresOn";E={$_.Certificate.NotAfter}},
    @{N="DaysLeft";E={($_.Certificate.NotAfter - (Get-Date)).Days}} |
    Format-Table -AutoSize

# Alerter si expiration proche (moins de 30 jours)
Get-AdfsCertificate | Where-Object {
    ($_.Certificate.NotAfter - (Get-Date)).Days -lt 30
} | ForEach-Object {
    Write-Warning "ALERTE: Certificat ADFS $($_.CertificateType) expire dans $(($_.Certificate.No
}
```

Durcissement TLS/SSL d'ADFS

ADFS expose des services HTTPS critiques. La configuration TLS doit être durcie pour éliminer les protocoles obsolètes et les cipher suites faibles.

> ⚡ **Retour terrain**
>
> Dans les projets IAM, le cas le plus fréquent que je rencontre est celui des comptes de service sans propriétaire identifié — créés pour un projet terminé ou un prestataire parti, et jamais supprimés. Pour une banque régionale, l'inventaire a identifié 134 comptes de service sans propriétaire actif, dont 23 avaient des droits administrateurs locaux sur des

serveurs de production. La désactivation progressive de ces comptes sur 6 semaines n'a déclenché aucune anomalie applicative.

Script PowerShell : désactivation TLS 1.0/1.1 et SSL 3.0

```
# Durcissement TLS via registre Windows
# Désactiver SSL 3.0
$SSLPath = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0"
New-Item -Path "$SSLPath\Client" -Force | Out-Null
New-Item -Path "$SSLPath\Server" -Force | Out-Null
Set-ItemProperty -Path "$SSLPath\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$SSLPath\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path "$SSLPath\Server" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$SSLPath\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Write-Host "SSL 3.0 désactivé" -ForegroundColor Green

# Désactiver TLS 1.0
$TLS10Path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0
New-Item -Path "$TLS10Path\Client" -Force | Out-Null
New-Item -Path "$TLS10Path\Server" -Force | Out-Null
Set-ItemProperty -Path "$TLS10Path\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$TLS10Path\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path "$TLS10Path\Server" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$TLS10Path\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Write-Host "TLS 1.0 désactivé" -ForegroundColor Green

# Désactiver TLS 1.1
$TLS11Path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1
New-Item -Path "$TLS11Path\Client" -Force | Out-Null
New-Item -Path "$TLS11Path\Server" -Force | Out-Null
Set-ItemProperty -Path "$TLS11Path\Client" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$TLS11Path\Client" -Name "DisabledByDefault" -Value 1 -Type DWord
Set-ItemProperty -Path "$TLS11Path\Server" -Name "Enabled" -Value 0 -Type DWord
Set-ItemProperty -Path "$TLS11Path\Server" -Name "DisabledByDefault" -Value 1 -Type DWord
Write-Host "TLS 1.1 désactivé" -ForegroundColor Green

# Activer TLS 1.2 (déjà actif sur WS2025 mais expliciter)
$TLS12Path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2
New-Item -Path "$TLS12Path\Client" -Force | Out-Null
New-Item -Path "$TLS12Path\Server" -Force | Out-Null
Set-ItemProperty -Path "$TLS12Path\Client" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path "$TLS12Path\Client" -Name "DisabledByDefault" -Value 0 -Type DWord
Set-ItemProperty -Path "$TLS12Path\Server" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path "$TLS12Path\Server" -Name "DisabledByDefault" -Value 0 -Type DWord
Write-Host "TLS 1.2 activé" -ForegroundColor Green

# Activer TLS 1.3 (Windows Server 2025 le supporte nativement)
```

```
$TLS13Path = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.3
New-Item -Path "$TLS13Path\Client" -Force | Out-Null
New-Item -Path "$TLS13Path\Server" -Force | Out-Null
Set-ItemProperty -Path "$TLS13Path\Client" -Name "Enabled" -Value 1 -Type DWord
Set-ItemProperty -Path "$TLS13Path\Server" -Name "Enabled" -Value 1 -Type DWord
Write-Host "TLS 1.3 activé" -ForegroundColor Green

Write-Host "`nRedémarrage requis pour appliquer les changements TLS." -ForegroundColor Yellow
```

Configuration des Cipher Suites — Forward Secrecy obligatoire

```
# Configurer cipher suites avec Forward Secrecy uniquement
# Compatible ANSSI RGS et recommandations BSI/NCSC

$AcceptedCiphers = @(
    "TLS_AES_256_GCM_SHA384",                          # TLS 1.3
    "TLS_AES_128_GCM_SHA256",                          # TLS 1.3
    "TLS_CHACHA20_POLY1305_SHA256",                    # TLS 1.3
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",         # TLS 1.2 ECDSA
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",           # TLS 1.2 RSA
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",         # TLS 1.2 ECDSA
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",           # TLS 1.2 RSA
    "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",   # TLS 1.2 ECDSA
    "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"      # TLS 1.2 RSA
)

# Supprimer les ciphers non-FS (RSA key exchange sans ECDHE)
$CiphersToDisable = @(
    "TLS_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_3DES_EDE_CBC_SHA"
)

# Appliquer via Group Policy (ou directement via registre)
foreach ($cipher in $CiphersToDisable) {
    Disable-TlsCipherSuite -Name $cipher -ErrorAction SilentlyContinue
    Write-Host "Désactivé: $cipher" -ForegroundColor Yellow
}

# Vérifier la configuration finale
Get-TlsCipherSuite | Select-Object Name, Protocols | Format-Table
```

Sécurisation des Endpoints ADFS

ADFS expose de nombreux endpoints par défaut, dont certains sont inutiles et augmentent la surface d'attaque. Un inventaire et une désactivation sélective sont indispensables avant toute exposition sur le WAP.

Désactivation des endpoints dangereux

```
# Désactiver IdpInitiatedSignOn — endpoint permettant aux attaquants de tester des credentials
# et de déclencher des authentifications sans application cible
Set-AdfsEndpoint -TargetAddressPath "/adfs/ls/IdpInitiatedSignOn.aspx" -Proxy $false
Disable-AdfsEndpoint -TargetAddressPath "/adfs/ls/IdpInitiatedSignOn.aspx"
Write-Host "IdpInitiatedSignOn désactivé" -ForegroundColor Green

# Désactiver les endpoints de gestion web (accessibles uniquement depuis réseau interne)
$EndpointsToDisableOnProxy = @(
    "/adfs/portal/updatepassword/",
    "/adfs/services/trust/2005/windowstransport",
    "/adfs/services/trust/13/windowstransport",
    "/adfs/services/trust/2005/kerberosmixed",
    "/adfs/services/trust/13/kerberosmixed"
)

foreach ($endpoint in $EndpointsToDisableOnProxy) {
    try {
        Set-AdfsEndpoint -TargetAddressPath $endpoint -Proxy $false
        Write-Host "Endpoint désactivé sur proxy: $endpoint" -ForegroundColor Green
    } catch {
        Write-Host "Endpoint non trouvé: $endpoint" -ForegroundColor Yellow
    }
}

# Audit des endpoints actifs (à exporter et analyser)
Write-Host "`n=== ENDPOINTS ADFS ACTIFS ===" -ForegroundColor Cyan
Get-AdfsEndpoint | Where-Object {$_.Enabled -eq $true} |
    Select-Object AddressPath, Protocol, Proxy, Enabled |
    Sort-Object AddressPath |
    Format-Table -AutoSize
```

Script d'audit complet des endpoints ADFS

```
# Audit des endpoints ADFS — exporter en CSV pour revue
function Export-AdfsEndpointAudit {
    param([string]$OutputPath = "C:\Audit\ADFS-Endpoints-$(Get-Date -Format 'yyyyMMdd').csv")

    $AllEndpoints = Get-AdfsEndpoint | Select-Object `
        AddressPath,
        Protocol,
        SecurityMode,
        Proxy,
        Enabled,
        @{N="Risk";E={
            if ($_.AddressPath -like "*IdpInitiated*") { "HIGH - Désactiver" }
            elseif ($_.AddressPath -like "*windowstransport*") { "HIGH - Proxy=false" }
            elseif ($_.AddressPath -like "*kerberos*" -and $_.Proxy) { "MEDIUM - Vérifier" }
            else { "OK" }
        }}

    $AllEndpoints | Export-Csv -Path $OutputPath -NoTypeInformation -Encoding UTF8
    Write-Host "Audit exporté: $OutputPath" -ForegroundColor Green

    # Afficher les endpoints à risque
    $HighRisk = $AllEndpoints | Where-Object {$_.Risk -like "HIGH*"}
    if ($HighRisk) {
        Write-Warning "$($HighRisk.Count) endpoint(s) à risque détectés:"
        $HighRisk | Format-Table AddressPath, Proxy, Risk -AutoSize
    }
}

Export-AdfsEndpointAudit
```

Extranet Lockout et Smart Lockout ADFS

L'Extranet Lockout est la première ligne de défense contre les attaques par force brute sur les comptes exposés via ADFS. Son activation dès le déploiement est obligatoire pour tout environnement de production.

Extranet Soft Lockout vs Hard Lockout

Mode	Comportement	Avantage	Inconvénient
Soft Lockout	Bloque l'accès extranet mais permet l'accès interne	Continuité de service pour les utilisateurs légitimes en interne	N'empêche pas les tentatives (ralentit seulement)
Hard Lockout	Bloque tout accès (interne + extranet)	Arrêt complet des tentatives de bruteforce	Risque de DoS si threshold mal calibré
ESL (Enhanced Smart Lockout)	Verrouille par IP source (familière vs inconnue)	Ne bloque pas les IP connues (bureau domicile)	Requiert ADFS 2019+

Configuration de l'Extranet Lockout

```
# Configurer l'Extranet Smart Lockout (ESL) — recommandé pour ADFS 2019+/WS2025
Set-AdfsProperties `
    -EnableExtranetLockout $true `
    -ExtranetLockoutMode ADPasswordCounter `  # ESL: utilise les compteurs AD
    -ExtranetLockoutThreshold 10 `            # 10 tentatives échouées depuis IP inconnue
    -ExtranetObservationWindow (New-TimeSpan -Minutes 30) `  # Fenêtre de 30 minutes
    -ExtranetLockoutRequirePDC $false         # Ne pas bloquer si PDC indisponible

# Pour les IP connues (réseau bureau, VPN corporate) : seuil plus permissif
Set-AdfsProperties `
    -ExtranetLockoutThresholdFamiliarLocation 50  # 50 tentatives pour IP familières

# Vérifier la configuration
Get-AdfsProperties | Select-Object `
    EnableExtranetLockout,
    ExtranetLockoutMode,
    ExtranetLockoutThreshold,
    ExtranetLockoutThresholdFamiliarLocation,
    ExtranetObservationWindow

# Débloquer un compte verrouillé manuellement
Reset-AdfsAccountLockout -UserPrincipalName "utilisateur@ayinedjimi.fr"

# Vérifier le statut de verrouillage
Get-AdfsAccountActivity -UserPrincipalName "utilisateur@ayinedjimi.fr" |
    Select-Object BadPwdCountFamiliar, BadPwdCountUnknown, FamiliarIPs
```

Intégration avec Microsoft Entra ID Smart Lockout

Dans un scénario hybride (ADFS + Entra ID Connect), le Smart Lockout Entra ID complète l'Extranet Lockout ADFS pour les comptes synchronisés dans le cloud. Configurez des seuils cohérents entre les deux systèmes pour éviter les angles morts : un attaquant ciblant Entra ID directement peut contourner l'Extranet Lockout ADFS.

Authentification Multi-Facteurs (MFA) sur ADFS

Le MFA est obligatoire pour tout accès extranet ADFS dans les environnements soumis à NIS 2 et DORA. ADFS supporte plusieurs providers MFA natifs et tiers.

MFA obligatoire pour l'accès extranet

```
# Exiger le MFA pour tous les accès extranet
# Via Issuance Authorization Rules ou Additional Authentication Rules

# Méthode recommandée: Additional Authentication Rule globale
$MFARule = @"
c:[Type == "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork",
   Value == "false"]
=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod",
         Value = "http://schemas.microsoft.com/claims/multipleauthn");
"@

Set-AdfsAdditionalAuthenticationRule -AdditionalAuthenticationRules $MFARule
Write-Host "MFA extranet activé pour tous les utilisateurs" -ForegroundColor Green

# Vérifier la règle
Get-AdfsAdditionalAuthenticationRule
```

Providers MFA compatibles ADFS 2025

```
# Lister les providers MFA enregistrés
Get-AdfsAuthenticationProvider | Select-Object Name, Enabled, AdminName |
    Format-Table -AutoSize

# Activer un provider MFA spécifique (ex: Azure MFA NPS Extension)
Enable-AdfsAuthenticationProvider -Name "AzureMfaAuthentication"

# Configurer l'Azure MFA comme provider primaire pour l'extranet
Set-AdfsGlobalAuthenticationPolicy `
    -AdditionalAuthenticationProvider "AzureMfaAuthentication" `
    -Force
```

Claim Rules : Durcissement et Audit

Les claim rules ADFS définissent les attributs transmis aux Relying Parties (applications). Des claim rules mal configurées peuvent conduire à des élévations de privilèges invisibles — un utilisateur standard obtenant un claim indiquant qu'il est administrateur dans une application cible.

Script PowerShell d'export et analyse des claim rules

```
# Export complet des claim rules pour audit
function Export-AdfsClaimRulesAudit {
    param([string]$OutputPath = "C:\Audit\ADFS-ClaimRules-$(Get-Date -Format 'yyyyMMdd').txt")

    $Report = @()
    $Report += "=== AUDIT CLAIM RULES ADFS ==="
    $Report += "Date: $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss')"
    $Report += "Serveur: $env:COMPUTERNAME"
    $Report += ""

    # Claim rules des Relying Party Trusts
    $Report += "=== RELYING PARTY TRUSTS ==="
    foreach ($rp in Get-AdfsRelyingPartyTrust) {
        $Report += "`n[RP] $($rp.Name) ($($rp.Identifier -join ', '))"
        $Report += "IssuanceAuthorizationRules:"
        $Report += $rp.IssuanceAuthorizationRules
        $Report += "IssuanceTransformRules:"
        $Report += $rp.IssuanceTransformRules

        # Détecter les règles potentiellement dangereuses
        if ($rp.IssuanceTransformRules -match "role|admin|group|privilege") {
            Write-Warning "Règle suspecte dans: $($rp.Name) — contient references à roles/groupes
        }

        # Vérifier si Permit All (pas de règle d'autorisation)
        if ([string]::IsNullOrEmpty($rp.IssuanceAuthorizationRules)) {
            Write-Warning "[$($rp.Name)] Aucune IssuanceAuthorizationRule — TOUS les utilisateurs
        }
    }

    # Claim rules des Claims Provider Trusts
    $Report += "`n=== CLAIMS PROVIDER TRUSTS ==="
    foreach ($cp in Get-AdfsClaimsProviderTrust) {
        $Report += "`n[CP] $($cp.Name)"
        $Report += $cp.AcceptanceTransformRules
    }

    $Report | Set-Content -Path $OutputPath -Encoding UTF8
    Write-Host "Rapport exporté: $OutputPath" -ForegroundColor Green
}

Export-AdfsClaimRulesAudit
```

Exemple de claim rule dangereuse à détecter

```
# EXEMPLE DE RÈGLE DANGEREUSE (à ne PAS utiliser en production)
# Cette règle accorde le claim "admin" à TOUS les utilisateurs authentifiés
# => Élévation de privilèges si l'application utilise ce claim pour contrôler l'accès
$DangerousRule = @"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/authentication",
   Value == "true"]
=> issue(Type = "http://schemas.example.com/claims/role",
         Value = "admin");
"@

# RÈGLE CORRECTE: émettre le claim role uniquement pour les membres du groupe AD adéquat
$SecureRule = @"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
   Value == "S-1-5-21-XXXX-XXXX-XXXX-YYYY"]  # SID du groupe "ADFS-Admins-AppX"
=> issue(Type = "http://schemas.example.com/claims/role",
         Value = "admin");
"@
```

Logging et Monitoring ADFS

Le monitoring ADFS est souvent insuffisant dans les organisations — les logs existent mais ne sont pas corrélés dans le SIEM. Une configuration correcte des niveaux de logs et l'ingestion dans Sentinel ou Wazuh sont indispensables pour détecter les compromissions.

Configuration du niveau de logging ADFS

```
# Activer le logging verbose ADFS
Set-AdfsProperties -LogLevel @(
    "FailureAudits",
    "SuccessAudits",
    "Information",
    "Verbose",
    "Warnings",
    "Errors"
)

# Activer l'audit de sécurité Windows pour ADFS
auditpol /set /subcategory:"Application Generated" /success:enable /failure:enable

# Vérifier le niveau de log
Get-AdfsProperties | Select-Object -ExpandProperty LogLevel
```

Event IDs ADFS critiques

Event ID	Description	Canal	Priorité SIEM
342	Échec d'authentification (mauvais password)	AD FS/Admin	MEDIUM (corréler pour bruteforce)
411	Échec validation token (token altéré ou expiré)	AD FS/Admin	HIGH
1007	Token émis avec succès	AD FS/Admin	INFO (base de référence)
510	Extranet Lockout déclenché	AD FS/Admin	HIGH
516	Configuration ADFS modifiée	AD FS/Admin	HIGH — alerter immédiatement
403	Requête de token refusée (autorisation)	AD FS/Admin	MEDIUM

KQL Microsoft Sentinel pour ADFS

```
// Détection bruteforce ADFS extranet – pic d'échecs d'authentification
SecurityEvent
| where TimeGenerated > ago(1h)
| where EventID == 342 or EventID in (4625, 4771)
| where Computer has "adfs" or Computer has "wap"
| summarize FailureCount = count(), DistinctUsers = dcount(TargetUserName)
    by bin(TimeGenerated, 5m), IpAddress = tostring(EventData.IpAddress), Computer
| where FailureCount > 50
| extend Alert = strcat("Bruteforce suspect ADFS: ", FailureCount, " échecs en 5 min depuis ", Ip
| project TimeGenerated, Computer, IpAddress, FailureCount, DistinctUsers, Alert
| order by FailureCount desc

// Détection changement configuration ADFS (Event 516)
SecurityEvent
| where EventID == 516
| where TimeGenerated > ago(24h)
| extend
    Actor = tostring(EventData.Actor),
    Change = tostring(EventData.AuditDetail)
| project TimeGenerated, Computer, Actor, Change
| order by TimeGenerated desc

// Tokens émis hors heures ouvrables (comportement anormal)
SecurityEvent
| where EventID == 1007
| where TimeGenerated > ago(7d)
| extend Hour = hourofday(TimeGenerated)
| where Hour < 7 or Hour > 20
| summarize count() by bin(TimeGenerated, 1h), Computer
| where count_ > 100
| project TimeGenerated, Computer, TokenCount = count_
```

Migration ADFS vers Entra ID (Deprecation ADFS)

Microsoft a annoncé en 2023 sa recommandation de migrer les applications d'ADFS vers Entra ID (anciennement Azure AD). En 2026, cette migration est devenue stratégique pour réduire la dette technique et bénéficier des fonctionnalités Entra ID (Conditional Access, Identity Protection, SSPR).

Analyser les applications à migrer

```
# Inventaire des Relying Party Trusts pour prioriser la migration
function Get-AdfsAppMigrationPriority {
    $RPs = Get-AdfsRelyingPartyTrust | Select-Object `
        Name,
        Identifier,
        Enabled,
        LastUpdateTime,
        @{N="Protocol";E={
            if ($_.WSFedEndpoint) { "WS-Fed" }
            elseif ($_.SamlEndpoints) { "SAML" }
            else { "OpenID/OAuth" }
        }},
        @{N="ClaimsCount";E={@($_.IssuanceTransformRules -split "=>").Count - 1}},
        @{N="MigrationComplexity";E={
            # Complexité basée sur le nombre de claim rules et le protocol
            $score = (@($_.IssuanceTransformRules -split "=>").Count - 1) * 2
            if ($_.ClaimsProviderName -eq "Active Directory") { $score += 0 }
            else { $score += 5 }  # Fédération tierce = plus complexe
            if ($score -le 4) { "SIMPLE - Migrer en priorité" }
            elseif ($score -le 8) { "MOYENNE - Migrer phase 2" }
            else { "COMPLEXE - Étude approfondie requise" }
        }}

    return $RPs | Sort-Object MigrationComplexity
}

Get-AdfsAppMigrationPriority | Format-Table -AutoSize

# Exporter vers CSV
Get-AdfsAppMigrationPriority |
    Export-Csv "C:\Audit\ADFS-Migration-Plan-$(Get-Date -Format 'yyyyMMdd').csv" `
    -NoTypeInformation -Encoding UTF8
```

Stratégie de migration par phases

La migration d'ADFS vers Entra ID ne doit pas être précipitée. Une approche en trois phases est recommandée pour les organisations françaises :

Phase 1 — Applications simples (3-6 mois) : Applications SaaS modernes supportant SAML 2.0 ou OpenID Connect nativement (Salesforce, ServiceNow, Office 365 si ce n'est pas déjà fait). Risque de régression minimal.

Phase 2 — Applications d'entreprise (6-12 mois) : Applications internes utilisant WS-Federation ou SAML avec peu de claim rules personnalisées. Nécessite des tests approfondis.

Phase 3 — Applications legacy complexes (12-24 mois) : Applications avec des claim rules complexes, dépendances NTLM, authentification par certificat client. Peut nécessiter une réécriture partielle.

Conformité NIS 2 et DORA : ADFS comme Infrastructure Critique

Pour les organisations françaises soumises à NIS 2 (OES, OIV) et DORA (entités financières), ADFS est une infrastructure critique dont la compromission peut entraîner des obligations de notification réglementaire.

ADFS dans le périmètre NIS 2

Disponibilité : ADFS est dans le périmètre des actifs essentiels — toute indisponibilité prolongée doit être documentée et peut déclencher une notification ANSSI si elle résulte d'un incident de sécurité

Mesures techniques NIS 2 Art. 21 : Authentification multifacteur, chiffrement des données, gestion des accès — toutes applicables à ADFS

Gestion des vulnérabilités : Les patches ADFS (via Windows Update) doivent être appliqués dans les délais définis par la politique de gestion des vulnérabilités (généralement 30 jours pour les critiques)

Tests de pénétration : ADFS doit être inclus dans le périmètre des tests de pénétration annuels exigés par NIS 2

DORA Article 12 — Journalisation et monitoring ADFS

DORA (règlement UE 2022/2554, applicable depuis janvier 2025) impose aux entités financières françaises :

Journalisation complète : Tous les événements d'authentification ADFS doivent être journalisés et conservés minimum 5 ans pour les logs de sécurité (DORA art. 12)

Monitoring en temps réel : Alertes automatiques sur les anomalies d'authentification ADFS (bruteforce, tokens suspects, changements de configuration)

Tests de résilience ICT : ADFS inclus dans les TLPT (Threat-Led Penetration Testing) imposés aux établissements financiers d'importance systémique

Notification d'incident : Compromission ADFS = incident ICT majeur à notifier à l'ACPR et l'AMF dans les 24h

Pour compléter votre architecture IAM sécurisée, consultez nos guides sur JEA et JIT pour l'administration sécurisée Microsoft, les silos d'authentification Windows Server 2025, et Credential Guard. La combinaison ADFS durci + Credential Guard + Authentication Silos forme une architecture de défense en profondeur cohérente pour les organisations les plus exposées.

Questions fréquentes sur le durcissement ADFS

Faut-il encore investir dans le durcissement ADFS ou migrer directement vers Entra ID ?

Les deux approches ne s'excluent pas. Si votre organisation a des applications sur ADFS qui ne peuvent pas migrer rapidement (contraintes réglementaires, applications legacy, exigences de souveraineté des données), le durcissement ADFS est obligatoire dès aujourd'hui. La migration vers Entra ID doit être planifiée sur 12 à 24 mois selon la complexité du parc applicatif, mais

entre-temps un ADFS non durci représente une surface d'attaque critique. Commencez par le durcissement TLS, la désactivation des endpoints inutiles et l'activation de l'Extranet Lockout — ces mesures prennent moins de 4 heures et réduisent considérablement le risque.

Quels sont les Event IDs ADFS les plus importants à surveiller dans un SIEM ?

Les Event IDs ADFS prioritaires pour la détection SIEM sont : 342 (échec d'authentification — à corréler pour détecter les bruteforces), 411 (échec de validation de token — peut indiquer une tentative de replay d'un token modifié), 510 (Extranet Lockout déclenché — alerte immédiate requise), et 516 (modification de configuration ADFS — changement non planifié = compromission potentielle). Ces événements se trouvent dans le canal AD FS/Admin du journal Windows Events. Dans Microsoft Sentinel, utilisez la table SecurityEvent avec filtrage sur Computer contenant "ADFS" ou "WAP". Assurez-vous que les serveurs ADFS et WAP sont bien couverts par votre agent Log Analytics.

L'Extranet Lockout ADFS peut-il créer un déni de service pour les utilisateurs légitimes ?

Oui, un Extranet Hard Lockout mal calibré peut verrouiller des comptes légitimes si le threshold est trop bas (moins de 5 tentatives). Deux précautions essentielles : premièrement, commencez par le mode Soft Lockout (ExtranetLockoutMode AdPasswordCounter) qui bloque uniquement l'accès extranet tout en permettant l'accès interne, ce qui évite le blocage total. Deuxièmement, calibrez le threshold selon le comportement normal de vos utilisateurs (10 à 20 tentatives pour les IP inconnues, 50 pour les IP familières) et testez avec un compte de test avant déploiement en production. L'Extranet Smart Lockout (ESL), disponible depuis ADFS 2019, distingue les IP familières des IP inconnues et est bien plus efficace que l'Extranet Lockout classique.

Comment auditer les claim rules ADFS pour détecter des risques d'élévation de privilèges ?

L'audit des claim rules ADFS nécessite d'examiner deux aspects : les Issuance Transform Rules (ce qui est émis dans le token) et les Issuance Authorization Rules (qui peut obtenir un token).

Cherchez les règles qui émettent des claims de rôle/groupe sans vérification de groupe AD réel — une règle du type "si l'utilisateur est authentifié, lui donner le claim admin" est une élévation de privilèges directe. Exportez toutes les règles avec Get-AdfsRelyingPartyTrust et analysez celles contenant "role", "admin", "group", "privilege". Vérifiez également qu'aucun Relying Party Trust n'a de règle d'autorisation vide (Permit All) pour des applications sensibles.

Quelles sont les obligations DORA spécifiques concernant la journalisation ADFS pour les entités financières françaises ?

Le règlement DORA (UE 2022/2554, applicable depuis janvier 2025) impose aux entités financières françaises supervisées par l'ACPR une conservation des journaux ICT de 5 ans minimum pour les événements de sécurité. Pour ADFS, cela implique : archivage de tous les Event IDs d'authentification (succès et échecs), des modifications de configuration, des tokens émis avec leur timestamp et l'identifiant de la Relying Party. La solution recommandée est l'ingestion des logs ADFS dans un SIEM centralisé (Sentinel, Splunk, QRadar) avec politique de rétention configurée à 5 ans. Les tests de résilience DORA imposent également d'inclure ADFS dans les exercices de reprise d'activité et les TLPT annuels.

À RETENIR

Points clés à retenir

Désactivez IdpInitiatedSignOn.aspx et tous les endpoints ADFS non nécessaires sur le WAP — chaque endpoint exposé est une surface d'attaque potentielle accessible depuis Internet.

Activez l'Extranet Smart Lockout (ESL) en mode Soft avant de passer en Hard Lockout, et calibrez les thresholds selon le comportement réel de vos utilisateurs pour éviter tout déni de service.

Auditez trimestriellement les claim rules ADFS — une règle mal configurée peut accorder des privilèges d'administrateur à tous les utilisateurs authentifiés sans aucune alerte visible.

> Ingérez les Event IDs ADFS (342, 411, 510, 516, 1007) dans votre SIEM et configurez des alertes sur les anomalies — sans monitoring, une compromission ADFS peut rester invisible pendant des semaines.
>
> Planifiez la migration vers Entra ID par phases, en commençant par les applications simples — mais durcissez ADFS dès maintenant car la migration prendra 12 à 24 mois dans la plupart des organisations.

Pour une architecture IAM complète et sécurisée, combinez ce guide avec nos ressources sur la surveillance des événements Windows sur contrôleur de domaine et sur Credential Guard Windows Server 2025. Votre équipe sécurité bénéficiera d'une vision cohérente de l'ensemble de l'infrastructure d'identité Microsoft.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité