Microsoft Entra Connect v3 : Sécurité et Architecture Hybride 2026

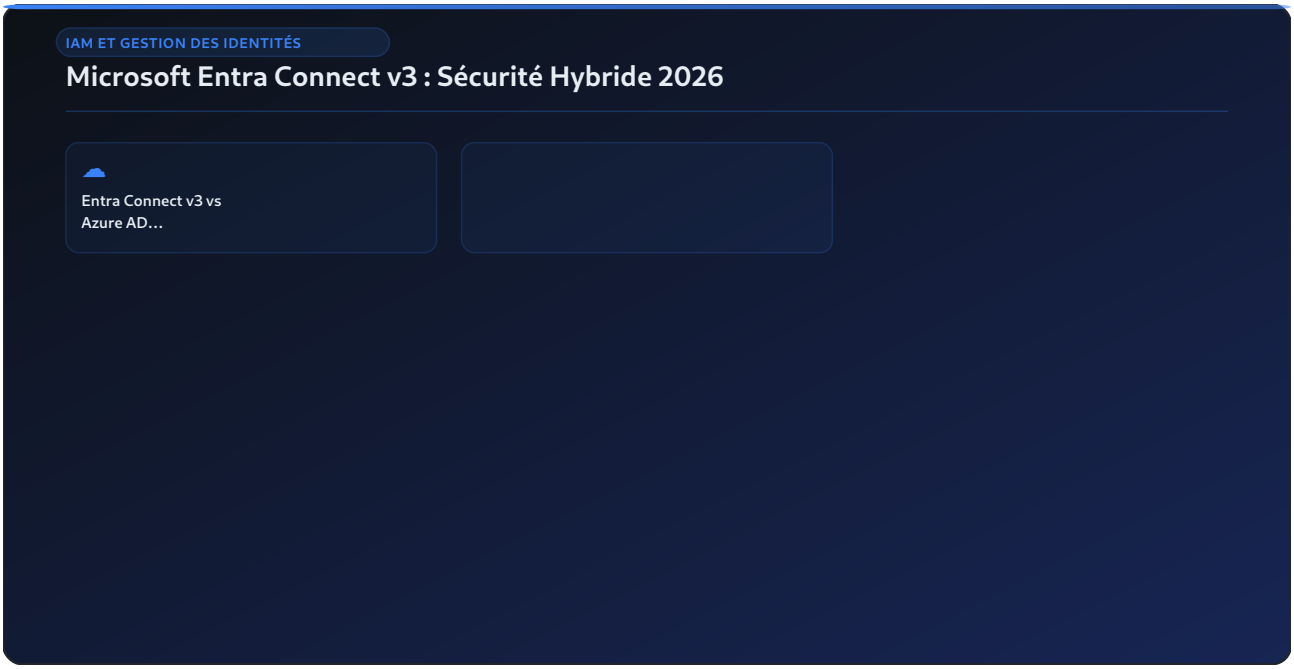
Sécurisez Microsoft Entra Connect v3 en environnement hybride AD/Entra ID : durcissement, PHS vs PTA, rotation AZUREADSSO, conformité NIS 2 pour RSSI.

📋 EN BREF

- Microsoft Entra Connect v3 remplace Azure AD Connect v2 (fin de support 2025) et s'impose comme le pivot de l'identité hybride AD/Entra ID pour les entreprises françaises.
- Le serveur Entra Connect est un actif Tier 0 : il doit être durci, isolé, et protégé comme un contrôleur de domaine.
- L'ANSSI recommande Password Hash Sync (PHS) plutôt que Pass-through Authentication (PTA) pour réduire la surface d'attaque réseau.
- Le compte AZUREADSSO (Seamless SSO) nécessite une rotation Kerberos mensuelle et une surveillance active des TGT émis.
- NIS 2 impose la traçabilité des authentifications hybrides : Entra Connect Health et Microsoft Sentinel sont les outils clés pour les RSSI en France.

Dans les entreprises françaises, la transition vers le cloud hybride Microsoft ne s'est pas faite en un jour : des milliers d'organisations de Paris à Lyon en passant par les ETI de toutes les régions maintiennent encore un Active Directory on-premises synchronisé avec Microsoft Entra ID (anciennement Azure Active Directory). Microsoft Entra Connect v3 est le composant central de cette architecture — et paradoxalement l'un des moins bien compris par les équipes sécurité. Pourtant, ce serveur de synchronisation dispose d'un niveau de privilèges équivalent à un contrôleur de domaine : il lit les hash de mots de passe NTLM, réécrit des attributs dans l'AD, et

peut initier des authentifications vers Entra ID. Pour les RSSI soumis à NIS 2, comprendre l'architecture, les modes d'authentification, et les techniques de durcissement d'Entra Connect v3 n'est pas une option — c'est une obligation réglementaire. Ce guide technique, orienté mise en œuvre, couvre la migration depuis Azure AD Connect v2, les bonnes pratiques de sécurisation du serveur, les recommandations ANSSI sur PHS versus PTA, et l'intégration avec les outils de détection modernes comme Microsoft Sentinel et Entra ID Protection pour les équipes sécurité françaises.



Microsoft a officiellement renommé Azure AD Connect en Microsoft Entra Connect lors du rebranding de sa suite d'identité en 2023. La version 3.x, disponible depuis fin 2024, apporte des changements fonctionnels et de support importants que les administrateurs français doivent maîtriser pour maintenir leur conformité.

Entra Connect v3 (2024-2025) : changements majeurs

La version 3 d'Entra Connect introduit plusieurs évolutions notables :

Portail d'administration unifié : la gestion migre progressivement vers le portail Entra ID (entra.microsoft.com), avec une vue consolidée synchronisation, santé et erreurs.

Support TLS 1.3 : les communications entre le serveur Entra Connect et les endpoints Microsoft utilisent désormais TLS 1.3 par défaut, abandonnant TLS 1.0 et 1.1.

Amélioration de la gestion des erreurs de synchronisation : le nouveau moteur de rapport d'erreurs distingue les erreurs transitoires des erreurs permanentes, réduisant le bruit opérationnel.

Support Windows Server 2025 : Entra Connect v3 est officiellement supporté sur Windows Server 2022 et 2025.

Synchronisation des groupes cloud-only vers l'AD : fonctionnalité Writeback v2 permettant de synchroniser les groupes Entra ID natifs vers l'Active Directory on-premises.

Fin de support Azure AD Connect v1 (2022) et v2 (2025)

Les dates de fin de support sont critiques pour la conformité NIS 2 :

Azure AD Connect v1.x : fin de support **août 2022**. Toute organisation utilisant encore cette version est en défaut de conformité et expose son infrastructure à des vulnérabilités non patchées.

Azure AD Connect v2.x : fin de support **31 décembre 2025**. La migration vers Entra Connect v3 doit être planifiée avant cette date.

Pour vérifier votre version actuelle depuis le serveur Entra Connect :

```
Get-ADSyncScheduler | Select-Object CurrentlyRunning, CustomizedSyncCycleInterval, NextSyncCycleP
(Get-Module ADSync).Version
```

Procédure de migration in-place vs fresh install

Migration in-place (recommandée pour la continuité) : télécharger l'installeur Entra Connect v3 depuis Microsoft, puis lancer l'installeur qui détecte l'installation existante et propose une mise à jour. Avant la migration, vérifiez les connecteurs existants :

```
Get-ADSyncGlobalSettings
Get-ADSyncConnector | Select-Object Name, Type, Enabled
```

Fresh install (recommandée pour changer de serveur ou passer à gMSA) : exporter la configuration depuis l'ancien serveur via `Get-ADSyncConfiguration`, déployer un nouveau serveur en mode Staging, valider les synchronisations, puis basculer.

Architecture Sécurisée Entra Connect

La sécurisation d'Entra Connect commence par la compréhension de ses comptes de service et de son modèle de filtrage. Chaque composant de l'architecture a des implications sécurité directes.

> ⚡ **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.

Compte de service AD DS Connector : permissions minimales requises

Le compte AD DS Connector est un compte Active Directory utilisé par Entra Connect pour lire (et parfois écrire) des objets dans l'AD. Par défaut, Microsoft recommande un compte avec les permissions suivantes :

Lecture de tous les objets et attributs de la forêt.

Réplication des changements de répertoire et **Réplication des changements de répertoire (tous)** — nécessaires uniquement pour Password Hash Sync.

Permissions d'écriture limitées aux attributs nécessaires (ex: `msDS-ExternalDirectoryObjectID`).

```
 $connectorAccount = "DOMAINE\svc-entrasync"
Get-ADUser $connectorAccount -Properties MemberOf | Select-Object MemberOf
(Get-ACL "AD:\DC=domaine,DC=fr").Access | Where-Object {$_.IdentityReference -like "*svc-entrasyn
```

Compte Azure AD Connector (Entra Connector) : rôle Hybrid Identity Administrator

Le compte Entra Connector est un compte cloud utilisé pour écrire dans Entra ID. Il doit avoir le rôle **Hybrid Identity Administrator** (anciennement Global Administrator dans les anciennes versions). Ce rôle donne accès à la gestion des paramètres de synchronisation, sans droits sur les applications ou la facturation.

```
 Connect-MgGraph -Scopes "Directory.Read.All"
Get-MgDirectoryRole | Where-Object {$_.DisplayName -eq "Hybrid Identity Administrator"} |
    ForEach-Object { Get-MgDirectoryRoleMember -DirectoryRoleId $_.Id }
```

Filtrage : OU-based, attribute-based, group-based

Le filtrage détermine quels objets AD sont synchronisés vers Entra ID. Trois méthodes existent :

Filtrage OU : le plus simple. Sélectionner uniquement les OUs contenant les utilisateurs et groupes à synchroniser. Exclure impérativement les OUs contenant les comptes Tier 0 (Domain Admins, etc.).

Filtrage par attribut : utiliser un attribut AD (ex: `cloudFiltered=TRUE`) pour marquer les objets à exclure. Plus granulaire mais nécessite une gestion d'attributs.

Filtrage par groupe : uniquement en phase pilote — limité à 50 000 objets, non recommandé en production.

Architecture haute disponibilité : Staging Mode

Le **Staging Mode** permet de déployer un second serveur Entra Connect qui importe et synchronise mais n'exporte pas vers Entra ID. En cas de panne du serveur principal, la bascule est quasi-immédiate.

```
Set-ADSyncScheduler -StagingModeEnabled $true
Get-ADSyncScheduler | Select-Object StagingModeEnabled
```

Durcissement du Serveur Entra Connect

Le serveur Entra Connect est un actif Tier 0 — il a les droits de lire les hash NTLM de tous les utilisateurs et peut écrire dans l'AD. Sa compromission équivaut à une compromission complète du domaine. Le durcissement n'est donc pas optionnel.

Serveur dédié Tier 0 (accès DC-level)

Dédier un serveur physique ou une VM isolée exclusivement à Entra Connect — aucun autre rôle.

Appliquer le modèle Tier 0 de Microsoft : seuls les comptes Tier 0 peuvent se connecter à ce serveur (GPO logon restrictions).

Activer le Credential Guard et le Protected Users Security Group pour les comptes administrateurs.

Restreindre les connexions RDP aux jump servers Tier 0 uniquement.

Désactiver l'accès Internet direct (proxy sortant)

Le serveur Entra Connect ne doit jamais avoir d'accès Internet direct. Configurez un proxy sortant filtrant pour les seules destinations Microsoft autorisées :

```
 netsh winhttp set proxy proxy-server="http://proxy.interne:8080" bypass-list="*.domaine.local"
Get-ADSyncGlobalSettings | Select-Object ConnectorHostName
```

Compte de service gMSA pour Entra Connect

Depuis Entra Connect 1.4.x, les comptes gMSA (Group Managed Service Accounts) sont supportés, éliminant la gestion manuelle des mots de passe de compte de service :

```
 New-ADServiceAccount -Name "svc-EntraConnect" -DNSHostName "entraconnect.domaine.fr" `
    -PrincipalsAllowedToRetrieveManagedPassword "SG-EntraConnect-Servers" `
    -ManagedPasswordIntervalInDays 30
Install-ADServiceAccount -Identity "svc-EntraConnect"
```

Script PowerShell : audit configuration Entra Connect

```
 function Invoke-EntraConnectAudit {
    Write-Host "=== AUDIT ENTRA CONNECT ===" -ForegroundColor Cyan
    $version = (Get-Module ADSync).Version
    Write-Host "[VERSION] ADSync: $version"
    $scheduler = Get-ADSyncScheduler
    Write-Host "[SCHEDULER] Suspended: $($scheduler.SchedulerSuspended), Staging: $($scheduler.St
    $connectors = Get-ADSyncConnector
    foreach ($conn in $connectors) {
        Write-Host "[CONNECTOR] $($conn.Name) - Type: $($conn.ConnectorTypeName)"
    }
    $customRules = Get-ADSyncRule | Where-Object {$_.IsStandardRule -eq $false}
    Write-Host "[CUSTOM RULES] $($customRules.Count) regles personnalisees"
    $errors = Get-ADSyncRunStepResult | Where-Object {$_.RunStepResultCode -ne "Success"} | Selec
    Write-Host "[ERRORS] $($errors.Count) erreurs recentes"
}
Invoke-EntraConnectAudit
```

Pass-through Authentication (PTA) vs Password Hash Sync (PHS) — Sécurité

Le choix entre PTA et PHS est l'une des décisions architecturales les plus importantes pour la sécurité de votre environnement hybride. Chaque méthode a des implications de sécurité distinctes que les RSSI français doivent peser dans le contexte NIS 2.

PTA : agents d'authentification, sécurité réseau, risque

Pass-through Authentication valide les mots de passe directement contre l'AD on-premises via des agents installés sur des serveurs membres du domaine. Implications de sécurité :

Agents exposés : 2 à 3 agents PTA minimum (haute disponibilité) maintiennent une connexion sortante persistante vers Entra ID. Ces agents deviennent des cibles privilégiées.

Disponibilité liée à l'AD : si l'AD on-premises est indisponible, les authentifications échouent — sauf si PHS est activé en fallback.

Surface d'attaque élargie : les serveurs hébergeant les agents PTA doivent être Tier 1 minimum, avec une surveillance renforcée.

Avantage de conformité sectorielle : les mots de passe ne quittent jamais l'AD, argument pertinent pour certaines réglementations sectorielles françaises (secteur bancaire, défense).

PHS : hash des hash NTLM dans Entra ID, implications de sécurité

Password Hash Sync envoie une version dérivée du hash NTLM (hash du hash MD4 avec salage et plusieurs itérations PBKDF2) vers Entra ID :

Ce qui est envoyé : pas le hash NTLM brut, mais `PBKDF2(MD4(password), salt, 1000 iterations)` — irréversible vers le mot de passe original.

Leaked credentials detection : Microsoft peut comparer ces hash dérivés avec des bases de credentials compromis, fonctionnalité disponible uniquement avec PHS.

Résilience : les authentifications fonctionnent même si l'AD on-premises est indisponible.

Entra ID Protection : toutes les fonctionnalités de risk-based policies sont disponibles avec PHS.

Seamless SSO : Kerberos delegation, compte AZUREADSSO

Seamless SSO crée un compte d'ordinateur `AZUREADSSO$` dans l'AD qui sert à émettre des tickets Kerberos pour les authentifications transparentes depuis des machines jointes au domaine :

```
Get-ADComputer AZUREADSSO -Properties * | Select-Object Name, PasswordLastSet, Enabled
Get-ADComputer AZUREADSSO -Properties ServicePrincipalNames | Select-Object -ExpandProperty Servi
```

Recommandations ANSSI : PHS préféré pour minimiser la surface d'attaque

L'ANSSI, dans ses guides sur l'identité hybride, recommande PHS comme méthode d'authentification principale pour les raisons suivantes :

Aucun agent réseau exposé en interne avec des connexions sortantes persistantes.

Résilience native en cas de panne AD on-premises.

Accès complet aux fonctionnalités d'Entra ID Protection (détection de fuite de credentials).

Surface d'attaque réduite sur le réseau interne, conforme au principe de défense en profondeur.

Entra Connect et la Détection des Comptes Compromis

Entra Connect joue un rôle central dans la capacité de détection des comptes compromis en environnement hybride. Comprendre ces mécanismes est essentiel pour les RSSI qui déploient des politiques d'accès conditionnel.

Identity Protection (Entra ID) : risque utilisateur, risk-based policies

Entra ID Protection analyse les signaux de connexion et attribue un score de risque aux utilisateurs et aux sessions :

User risk : probabilité que le compte soit compromis (basé sur des patterns d'activité anormaux, des IP malveillantes connues, des credentials leakés).

Sign-in risk : probabilité que la connexion spécifique soit illégitime (impossible travel, Tor exit node, etc.).

```
Connect-MgGraph -Scopes "IdentityRiskyUser.Read.All"
Get-MgRiskyUser -Filter "riskLevel eq 'high'" |
    Select-Object UserDisplayName, UserPrincipalName, RiskLevel, RiskState, RiskLastUpdatedDateTi
```

Leaked credentials detection via PHS

Avec PHS activé, Microsoft compare automatiquement les hash synchronisés avec des bases de données de credentials compromis collectées sur le darkweb. Lorsqu'une correspondance est trouvée :

Le risque utilisateur est automatiquement élevé à "High".

Les Conditional Access policies basées sur le risque peuvent forcer une réinitialisation de mot de passe ou bloquer l'accès.

L'alerte apparaît dans le portail Entra ID Protection et peut être transmise à Microsoft Sentinel.

Microsoft Sentinel integration : SigninLogs, AADNonInteractiveUserSignInLogs

```
// Détection de connexions hybrides anormales dans Sentinel
SigninLogs
| where TimeGenerated > ago(1d)
| where AuthenticationRequirement == "singleFactorAuthentication"
| where ClientAppUsed in ("Exchange ActiveSync", "IMAP4", "POP3", "SMTP")
| where ResultType == "0"
| summarize Count = count() by UserPrincipalName, ClientAppUsed, IPAddress
| where Count > 10
| order by Count desc
```

Compte AZUREADSSO : Sécurisation Critique

Le compte machine `AZUREADSSO$` est l'élément le plus critique de l'infrastructure Seamless SSO. Sa compromission permettrait à un attaquant de forger des tickets Kerberos valides pour n'importe quel utilisateur synchronisé — un risque majeur que les équipes sécurité françaises sous-estiment souvent.

Compte Kerberos AZUREADSSO : rotation du mot de passe (tous les 30 jours recommandé)

Contrairement aux comptes d'ordinateur AD standard dont le mot de passe tourne automatiquement tous les 30 jours, le compte AZUREADSSO$ ne se renouvelle pas automatiquement. Cette rotation doit être effectuée manuellement ou scriptée pour chaque forêt AD concernée.

`Update-AzureADSSOForest` : script de rotation planifiée

```
 $securePass = ConvertTo-SecureString $env:DOMAIN_ADMIN_PASS -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential ("DOMAINE\AdminTier0", $securePass)

Import-Module "C:\Program Files\Microsoft Azure Active Directory Connect\AzureADSSO.psd1"
New-AzureADSSOAuthenticationContext -AzureADCredentials $azureCreds
Update-AzureADSSOForest -OnPremCredentials $creds

Write-EventLog -LogName Application -Source "EntraSSO-Rotation" -EventId 9001 `
    -EntryType Information -Message "Rotation AZUREADSSO effectuee: $(Get-Date)"
```

Surveillance des TGT émis pour AZUREADSSO

```
Get-WinEvent -ComputerName "dc01.domaine.fr" -FilterHashtable @{
    LogName = "Security"
    Id = 4768
} | Where-Object {$_.Message -like "*AZUREADSSO*"} |
    Select-Object TimeCreated, Message |
    Format-Table -AutoSize
```

Entra Connect Health : Monitoring et Alertes

Entra Connect Health est le service de monitoring fourni par Microsoft pour surveiller la santé des composants d'identité hybride. Son déploiement est obligatoire pour toute organisation sérieuse sur la continuité d'activité.

Installation agent Health pour AD FS et AD DS

```
 # Sur chaque contrôleur de domaine à monitorer
$healthAgentPath = "C:\Temp\AdHealthAddsAgentSetup.exe"
Start-Process $healthAgentPath -ArgumentList "/quiet" -Wait
Register-AzureADConnectHealthADDSAgent -Credentials $azureCreds
```

Alertes : sync errors, latency, authentication failures

Le portail Entra Connect Health génère des alertes pour :

Erreurs de synchronisation : objets en quarantine, conflits d'attributs, violations de règles.

Latence de synchronisation : délai entre une modification AD et sa réplication dans Entra ID (SLA : 30 minutes maximum).

Echecs d'authentification : taux d'erreur sur les authentifications hybrides (pertinent pour AD FS).

Objets en quarantine : objets bloqués par Entra Connect suite à des erreurs d'attributs.

Dashboard Entra Portal

Accéder au monitoring depuis **entra.microsoft.com → Entra Connect → Connect Health**. Le dashboard affiche l'état des agents Health installés, les graphes de latence de synchronisation sur 7 et 30 jours, le tableau des 50 dernières erreurs de synchronisation avec détail de l'objet en erreur, et les alertes actives avec leur historique de résolution.

Sécurisation de la Synchronisation : Filtrage et Scoping

Le filtrage de synchronisation est un levier de sécurité souvent négligé. Un scope mal configuré expose Entra ID à des objets qui n'ont rien à y faire, élargissant inutilement la surface d'attaque cloud.

Exclure les comptes Tier 0 de la synchronisation

Les comptes Tier 0 (Domain Admins, Enterprise Admins, Schema Admins, comptes de service des DCs) ne doivent jamais être synchronisés vers Entra ID. Une compromission d'Entra ID pourrait sinon permettre un mouvement latéral vers l'AD on-premises via des scénarios d'écriture (password writeback, etc.).

```
 Set-ADUser "AdminTier0" -Replace @{cloudFiltered = "TRUE"}
# Via le Synchronization Rules Editor d'Entra Connect :
# Condition : memberOf = "CN=Tier-0-Admins,OU=Admin,DC=domaine,DC=fr"
# Action : cloudFiltered = TRUE
```

Attributs synchronisés : liste de contrôle

Auditez régulièrement les attributs synchronisés pour éviter l'exposition de données sensibles :

A surveiller : `telephoneNumber`, `mobile`, `streetAddress`, `employeeID` — peuvent exposer des données RH sensibles.

Ne jamais synchroniser : attributs contenant des données de santé, des secrets, ou des identifiants confidentiels.

Recommandé : documenter chaque attribut synchronisé avec sa justification métier dans votre PSSI.

```
$connector = Get-ADSyncConnector | Where-Object {$_.ConnectorTypeName -eq "Extensible2"}
$connector.ExportAttributeIncludeList | Sort-Object | Format-Table
```

Quarantine : comprendre les erreurs de sync

Les objets en quarantine sont des objets AD que Entra Connect ne peut pas synchroniser en raison d'erreurs d'attributs (doublons, caractères invalides, longueur dépassée). Les erreurs les plus fréquentes en environnement français :

`AttributeValueMustBeUnique` : ProxyAddresses ou UserPrincipalName en doublon entre deux objets.

`InvalidSoftMatch` : tentative de match sur un objet déjà lié à un autre compte Entra.

`LargeObject` : attribut dépassant la taille maximale (ex: photo de profil trop volumineuse).

Conformité NIS 2 : Identité Hybride comme Périmètre Critique

La directive NIS 2, transposée en droit français par la loi du 17 octobre 2024, impose des exigences de sécurité renforcées pour les entités essentielles et importantes. L'identité hybride AD/Entra est expressément concernée par plusieurs articles.

NIS 2 pour environnements hybrides AD/Entra

L'article 21 de NIS 2 impose notamment :

§2.b (gestion des incidents) : détecter et répondre aux incidents d'authentification hybride — Entra ID Protection et Sentinel remplissent ce rôle.

§2.e (continuité des activités) : l'architecture haute disponibilité Entra Connect (Staging Mode, failover) est requise pour les entités essentielles.

§2.i (authentification) : MFA obligatoire pour tous les accès administrateurs — s'applique aux comptes administrant Entra Connect lui-même.

Traçabilité des authentifications hybrides

Pour les audits NIS 2, conservez les logs suivants :

Logs Entra Connect : `%ProgramData%\AADConnect\` — rotation et archivage sur 12 mois minimum.

Logs Entra ID (SigninLogs, AuditLogs) : rétention native 30 jours à étendre via Log Analytics Workspace sur 12 mois.

Logs AD locaux (Event ID 4768, 4769, 4625) : archivage SIEM sur 12 mois.

Contexte entreprises françaises en cloud hybride

Selon les estimations Microsoft France, plus de 70% des entreprises françaises de plus de 500 salariés opèrent en mode hybride AD/Entra ID. Pour les RSSI de ces organisations, Entra Connect doit apparaître dans le registre des actifs critiques de niveau 1. Son serveur doit faire l'objet d'un test de pénétration annuel (Article 21§2.g NIS 2). La procédure de rotation du compte AZUREADSSO doit être documentée et testée, et les logs d'authentification hybride doivent être intégrés dans le plan de réponse aux incidents.

Pour approfondir la sécurisation de l'infrastructure d'authentification Windows, consultez nos guides sur les Authentication Silos Windows Server 2025 et Credential Guard Windows Server 2025. Pour l'administration sécurisée au quotidien, voir notre article sur JEA et JIT pour

l'administration sécurisée Microsoft. La surveillance des contrôleurs de domaine est couverte en détail dans notre guide sur les événements Windows à surveiller sur un contrôleur de domaine.

Questions fréquentes sur Entra Connect v3

Quelle est la différence entre Entra Connect v3 et Azure AD Connect v2 ?

Entra Connect v3 succède à Azure AD Connect v2 avec un support étendu jusqu'en 2027, une interface renommée, une meilleure intégration avec le portail Entra ID, et des améliorations sur la gestion des erreurs de synchronisation. Azure AD Connect v1 est hors support depuis 2022, v2 depuis fin 2025.

PHS ou PTA : que recommande l'ANSSI pour les entreprises françaises ?

L'ANSSI recommande Password Hash Synchronization (PHS) en priorité car il réduit la surface d'attaque : l'authentification s'effectue directement dans Entra ID sans agent local exposé. PTA nécessite des agents actifs sur le réseau interne, ce qui constitue un vecteur d'attaque supplémentaire.

Comment sécuriser le compte AZUREADSSO utilisé par Seamless SSO ?

Le compte AZUREADSSO doit avoir son mot de passe Kerberos rotaté tous les 30 jours via la cmdlet Update-AzureADSSOForest. Surveillez les TGT émis pour ce compte dans les logs d'audit Active Directory (Event ID 4768). Ce compte ne doit jamais être utilisé pour autre chose que le SSO hybride.

Faut-il exclure les comptes Tier 0 de la synchronisation Entra Connect ?

Oui, c'est une bonne pratique critique. Les comptes Admin de domaine, Enterprise Admin et autres comptes Tier 0 ne devraient pas être synchronisés vers Entra ID. En cas de compromission

Entra, cela empêche le mouvement latéral vers l'AD on-premises. Utilisez le filtrage par OU ou attribut pour les exclure.

Comment Entra Connect s'intègre-t-il avec Microsoft Sentinel ?

Entra Connect alimente Entra ID qui expose ses logs dans Microsoft Sentinel via le connecteur Azure Active Directory : tables SigninLogs, AADNonInteractiveUserSignInLogs, AuditLogs. Les erreurs de synchronisation apparaissent dans AADProvisioningLogs. Des règles analytiques Sentinel permettent de détecter les anomalies d'authentification hybride.

À RETENIR

Entra Connect v3 est un actif Tier 0 : traitez son serveur avec le même niveau de sécurité qu'un contrôleur de domaine, car il dispose d'un accès équivalent aux données d'identité de toute l'organisation.

Privilegiez Password Hash Sync (PHS) sur Pass-through Authentication (PTA) pour réduire la surface d'attaque réseau, tout en bénéficiant de la détection de credentials compromis d'Entra ID Protection.

Le compte AZUREADSSO$ nécessite une rotation manuelle mensuelle via Update-AzureADSSOForest — automatisez cette tâche avec Task Scheduler et auditez les Event ID 4768 sur vos DCs.

Excluez systématiquement les comptes Tier 0 (Domain Admins, Enterprise Admins) de la synchronisation vers Entra ID pour éviter les mouvements latéraux en cas de compromission cloud.

NIS 2 impose la traçabilité des authentifications hybrides sur 12 mois minimum : configurez un Log Analytics Workspace pour étendre la rétention des SigninLogs au-delà des 30 jours natifs d'Entra ID.

Sources

ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité