IDENTITY DAYS

20 octobre 2026
PARIS

PIÈCE N°01

Comment tuer Active Directory ?

Une élimination propre, méthodique, documentée.

Jean-Sébastien Duchêne
Directeur technique – Magellan

MVP Microsoft Most Valuable Professional Security

microsofttouch
linkedin.com/in/jeansebastienduchene

CONFIDENTIEL

IDENTITY DAYS

20 octobre 2026 – PARIS

COLD OPEN — ÉPISODE 0

Le Passager Noir

« Tout le monde a une part sombre.
La mienne veut éteindre des contrôleurs de domaine. »

○ PIÈCE N°02

DC éteint

Passager Noir

Méthode

AVANT DE COMMENCER

Avertissement

Lisez ceci avant de franchir le ruban.

RIME SCENE – DO NOT CROSS – CRIME SCENE – DO NOT CROSS – CRIME SCENE – DO NOT CROSS – CRIME SCENE – DO NOT CROS

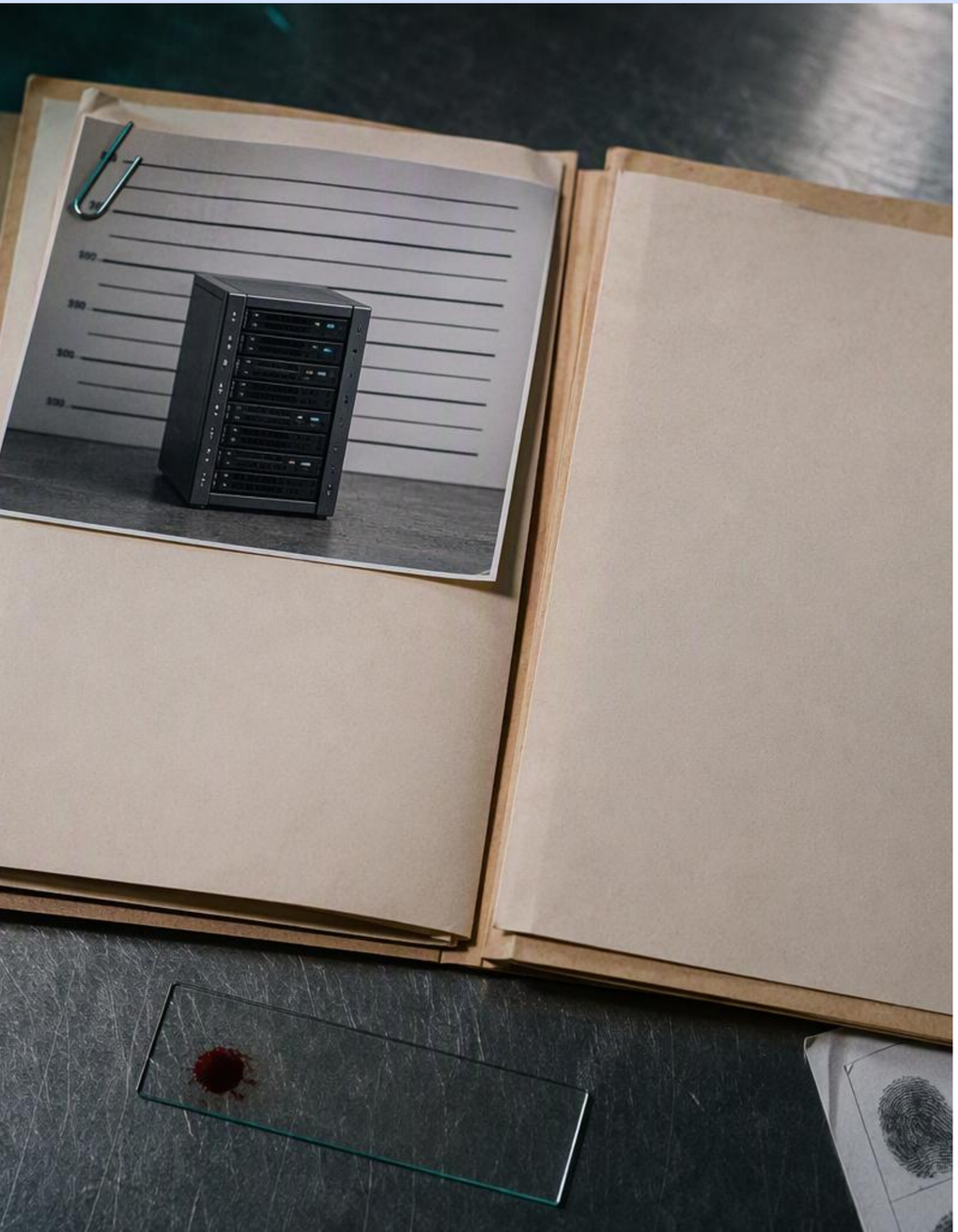
Aucun contrôleur de domaine n'a été maltraité pendant la préparation de cette session.

Toute ressemblance avec votre système d'information serait purement… documentée.

Les protocoles cités sont majeurs et consentants. Sauf NTLM.

DO NOT CROSS – CRIME SCENE – DO NOT CROSS – CRIME SCENE – DO NOT CROSS – CRIME SCENE – DO NOT CROSS – CRIME

AVERTISSEMENT



ÉPISODE 1 — LA VICTIME

PIÈCE N°04

La victime

Fiche d'identité — dossier d'autopsie n°04.

NOM	Active Directory Domain Services
NAISSANCE	17 février 2000 — Windows 2000 Server
ÂGE	26 ans, dont 15 en sursis
DOMICILE	Tier 0, salle serveur, fond du couloir
SIGNES PARTICULIERS	Kerberos, NTLM, LDAP, GPO, DNS
ENTOURAGE	Plus de 25 ans de dépendances qui refusent de partir

DOSSIER OUVERT

ÉPISODE 1 — LA VICTIME

PIÈCE N°05

Pourquoi elle est increvable

Six raisons de survivre à tous les projets de migration.

Ancienneté

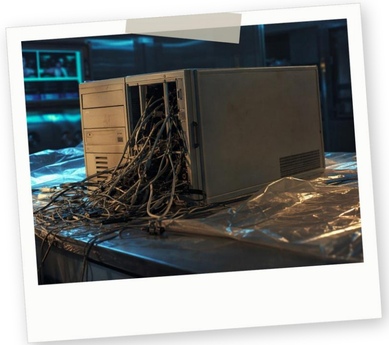
Plus de 25 ans de réflexes et de scripts oubliés

Centralité

Tout s'authentifie contre elle

Confort des GPO

3 000 paramètres, zéro documentation



Applications legacy

LDAP gravé dans le code depuis 2009

Peur du métier

« Si ça casse la paie, on fait quoi ? »

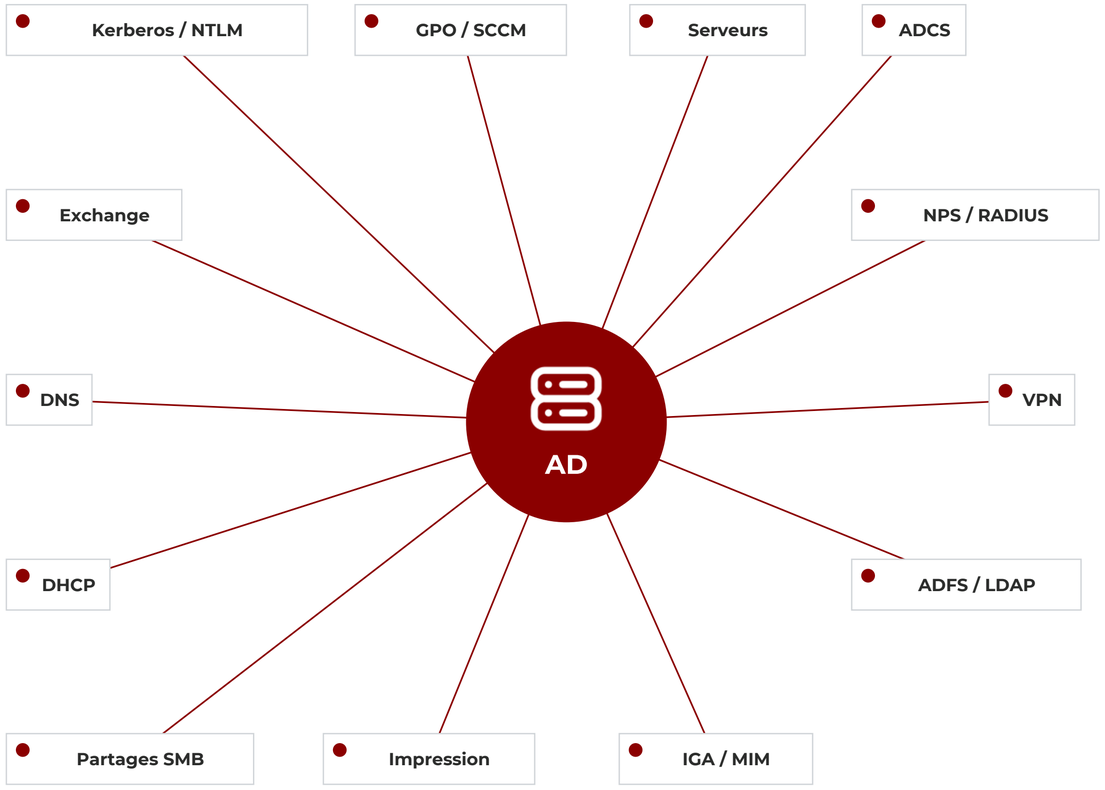
Absence de propriétaire

Tout le monde s'en sert.
Personne n'en répond.

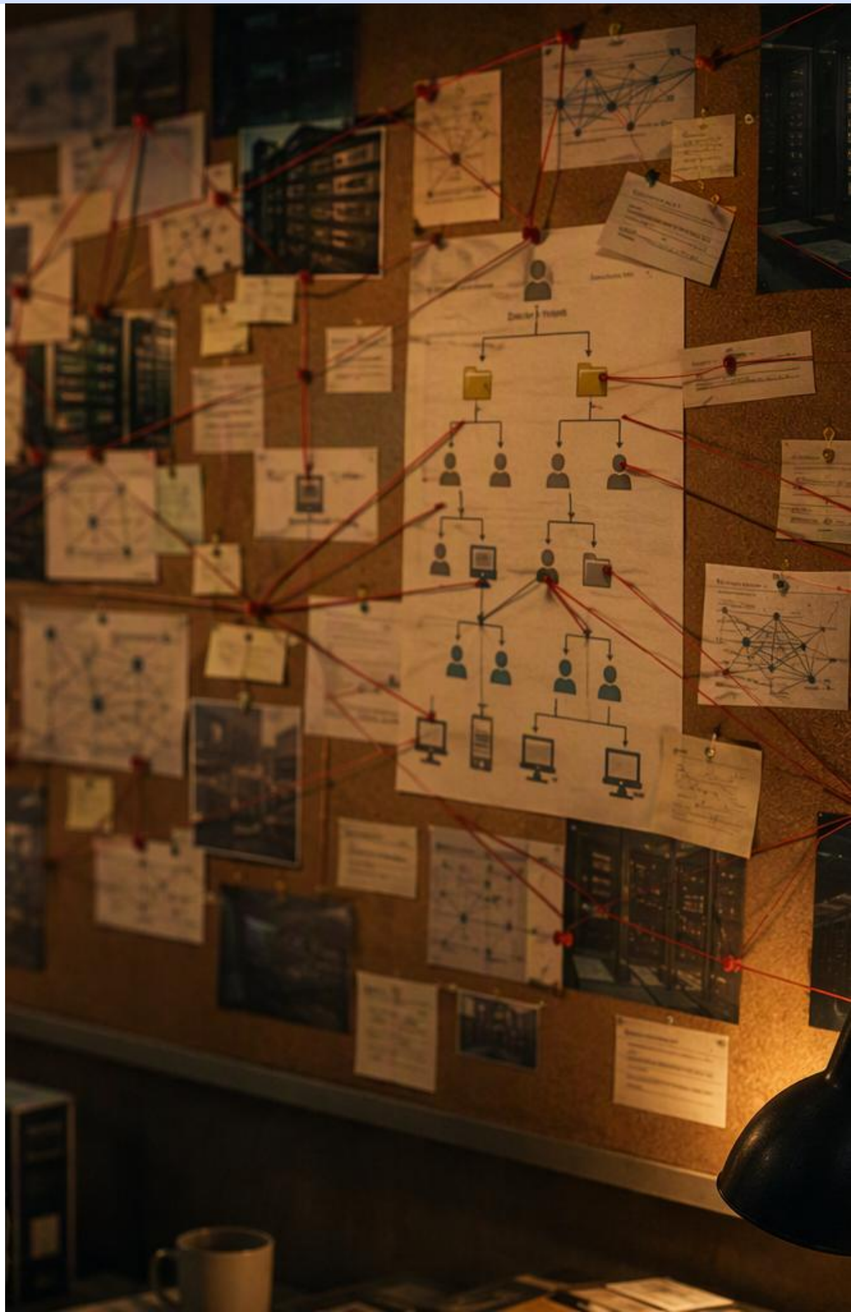
ÉPISODE 1 — LA VICTIME

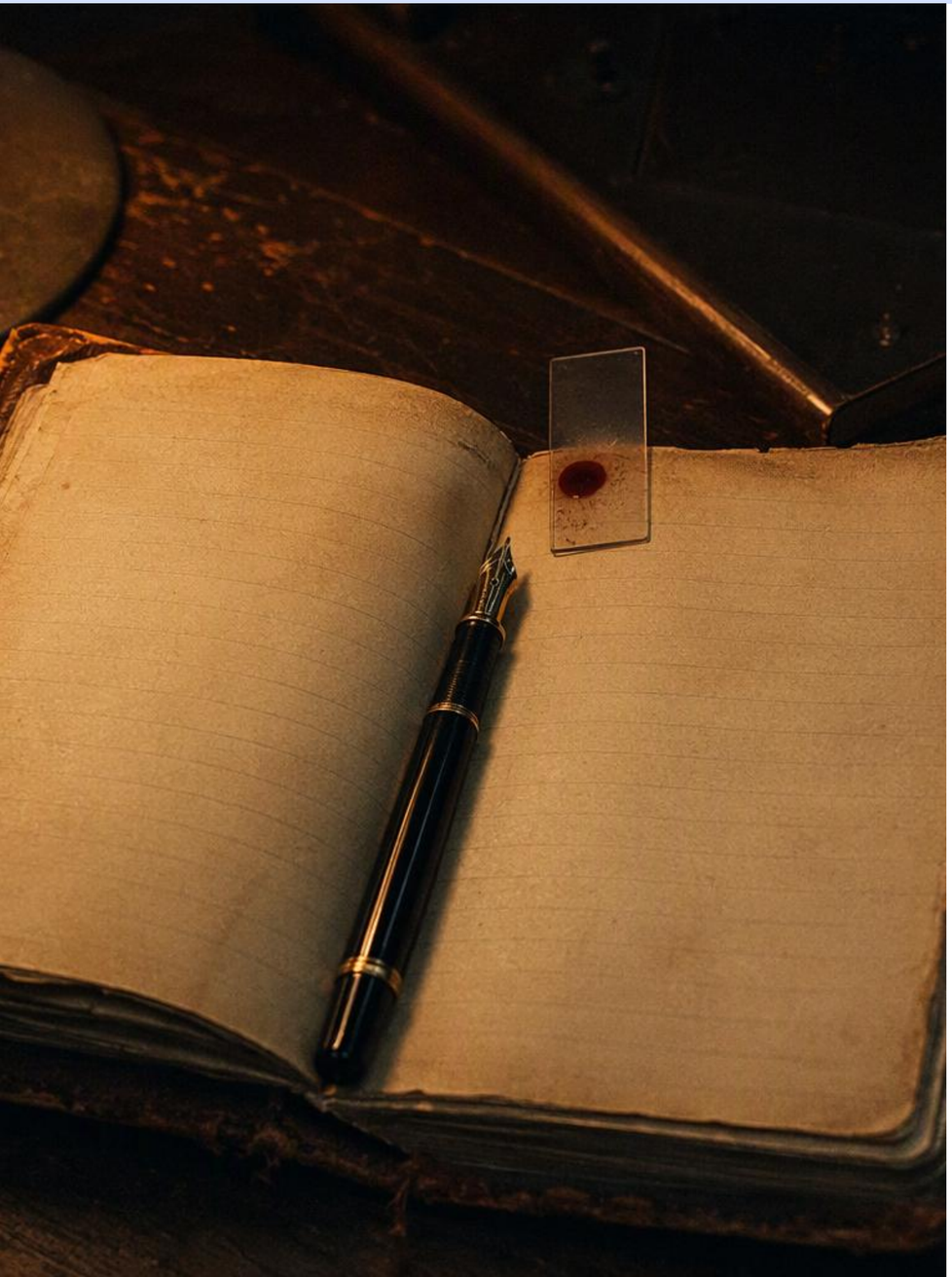
Le mur des indices

Treize fils rouges. Treize organes à retirer.



○ PIÈCE N°06





ÉPISODE 2 — LE CODE DE HARRY

PIÈCE N°07

Le Code de Harry

Six règles. Pas une de moins.

01 **Cartographier**

Chaque dépendance, chaque flux, chaque compte.

02 **Ne jamais tuer sans preuve**

Journaux, audits, inventaires : la preuve avant l'acte.

03 **Préparer la kill room**

Un environnement isolé, propre, réversible.

04 **Remplacer chaque organe avant de le retirer**

L'équivalent cloud tourne avant qu'AD ne s'arrête.

05 **Ne laisser aucune trace**

Pas de bind LDAP orphelin, pas de SRV fantôme.

06 **Garder un plan de repli**

Sauvegarde de forêt testée, retour arrière par objet.

ÉPISODE 2 — LE CODE DE HARRY

PIÈCE N°08

L'enquête médico-légale

Révéler ce qui touche encore AD avant de couper.

Outil ITDR / Defender for Identity

Qui parle à quel DC, avec quel protocole

Journaux LDAP — Event 2889

Les binds simples et non signés

Audit NTLM

Event 4624 / 8004 : qui utilise encore NTLM

Inventaire ADFS

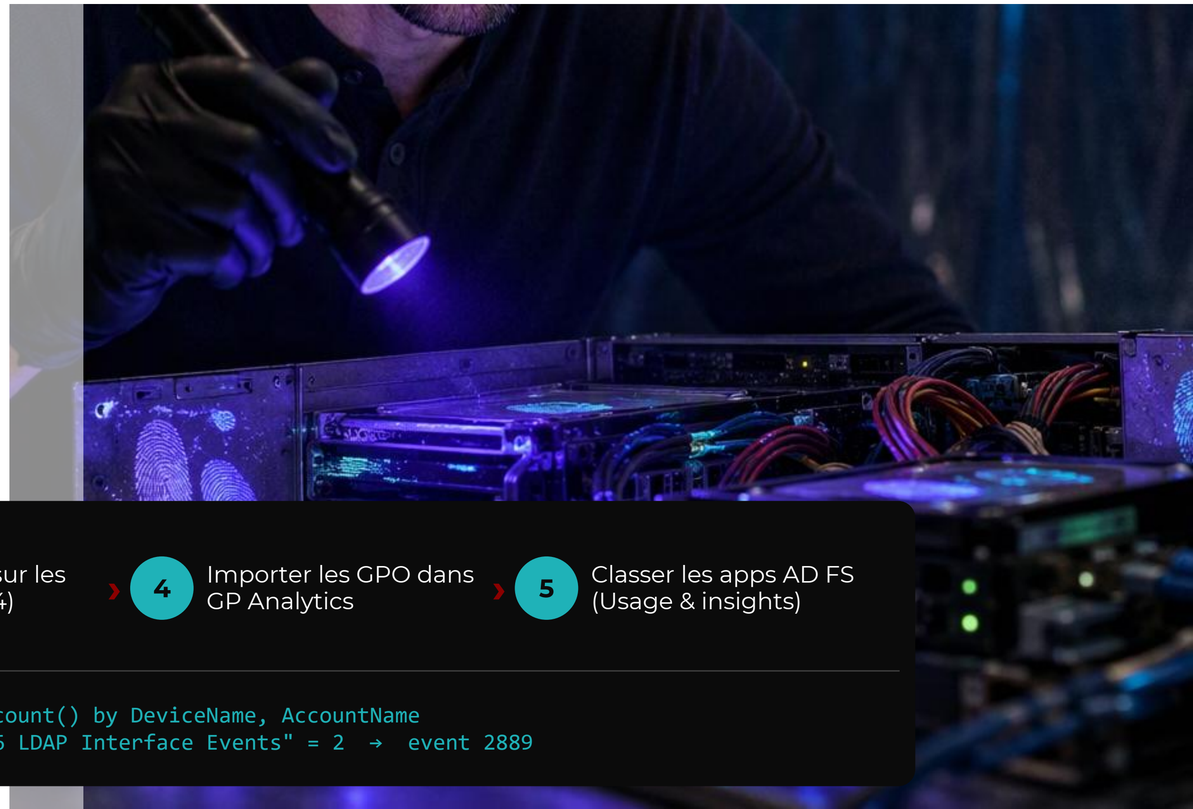
Relying parties, certificats, claims

Group Policy Analytics

Ce qui est migrable vers Intune

Inventaire des certificats

Modèles ADCS, usages, échéances



LABO

procédure

1. Passer « 16 LDAP Interface Events » à 2
2. Collecter les events 2887 / 2889
3. Auditer NTLM sur les DC (event 8004)
4. Importer les GPO dans GP Analytics
5. Classer les apps AD FS (Usage & insights)

REQUÊTE

```
IdentityLogonEvents | where Protocol =~ "ntlm" | summarize count() by DeviceName, AccountName
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics  "16 LDAP Interface Events" = 2  →  event 2889
```

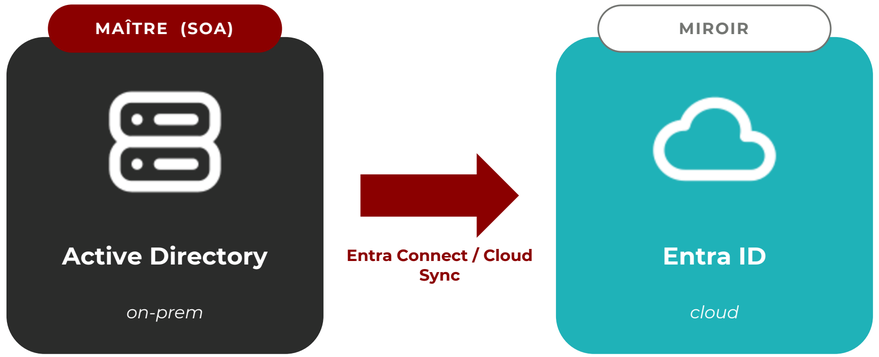
ÉPISODE 3 — ENTRA ID FIRST

○ PIÈCE N°09

Inverser le sang

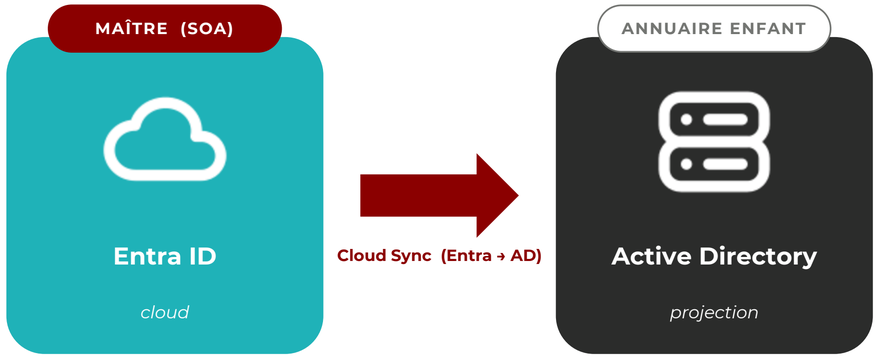
Le maître devient la projection. La projection devient le maître.

AUJOURD'HUI



Identités créées et gérées on-prem ; Entra reçoit une copie.

DEMAIN



Identités nées dans Entra ; AD ne reçoit que ce dont il a besoin.

ÉPISODE 3 — ENTRA ID FIRST

Road to the Cloud : les cinq états

Où en êtes-vous ?

PIÈCE N°10

VOUS ÊTES PROBABLEMENT ICI

1

Cloud attached

AD maître,
sync vers Entra

2

Hybride

Postes hybrides,
appli SaaS dans Entra

3

Cloud first

Tout nouveau
naît dans Entra

4

AD minimisé

Annuaire technique
confiné

CIBLE RÉALISTE

5

100 % cloud

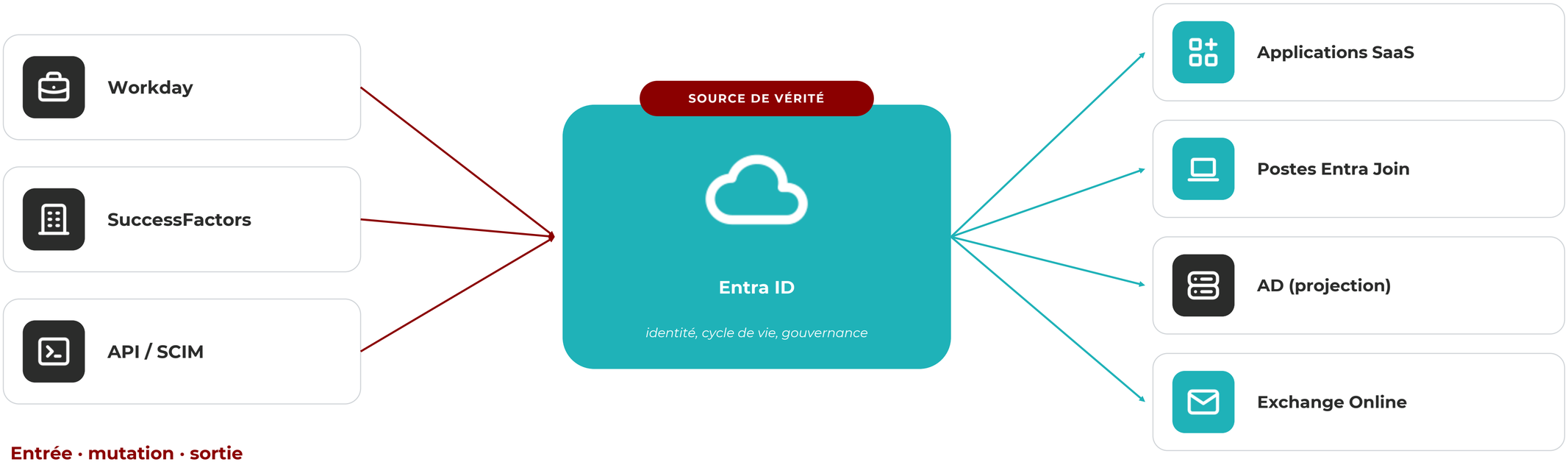
Plus de DC.
Affaire classée.

ÉPISODE 3 — ENTRA ID FIRST

La source RH

« Harry avait raison : la vérité vient de la source. » Préparée avant, activée au cutover.

○ PIÈCE N°11



Entrée · mutation · sortie

Par cohorte : stop RH → AD, transfert du SOA, puis start RH → Entra.

LABO

procédure

1. Brancher Workday, SuccessFactors ou l'API
2. Mapper employeeHireDate / LeaveDateTime
3. Pousser des lots SCIM (50 opérations)
4. Créer les workflows Joiner / Leaver
5. Déclencher à J-x de l'arrivée / du départ

API

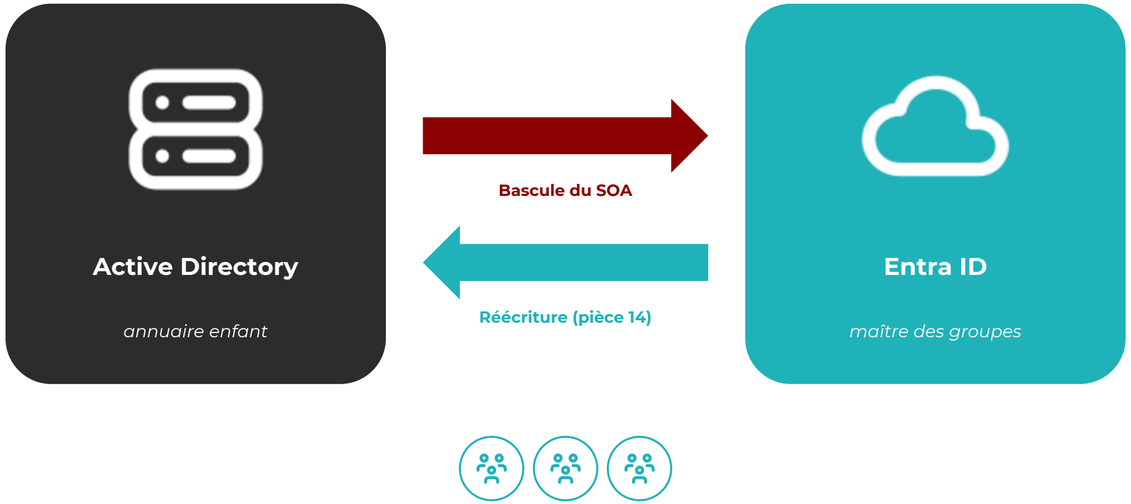
```
POST /servicePrincipals/{id}/synchronization/jobs/{jobId}/bulkUpload    (application/scim+json)
# permission SynchronizationData-User.Upload  ·  déclencheurs LCW : employeeHireDate, employeeLeaveDateTime
```

ÉPISODE 3 — ENTRA ID FIRST

Transférer le SOA des groupes

Le premier organe qu'on greffe dans le cloud.

○ PIÈCE N°12



- **Gestion dans le cloud** : création, membres, propriétaires
- **Réécriture vers AD** : sécurité universels, SID conservé
- **Entra ID Governance** : access packages, revues, expiration
- **Groupe par groupe** : basculer, tester, verrouiller

Jamais d'écriture dans les deux sens sur le même objet.

Groupes · SID conservé · Governance · Verrouillé

LABO *procédure*

1. Connect Sync ou Cloud Sync : dernière version
2. Passer les groupes AD en Universel
3. Basculer isCloudManaged via Graph
4. Cloud Sync : réécrire vers AD, même OU
5. Event 6956, puis gérer dans Entra

API GRAPH

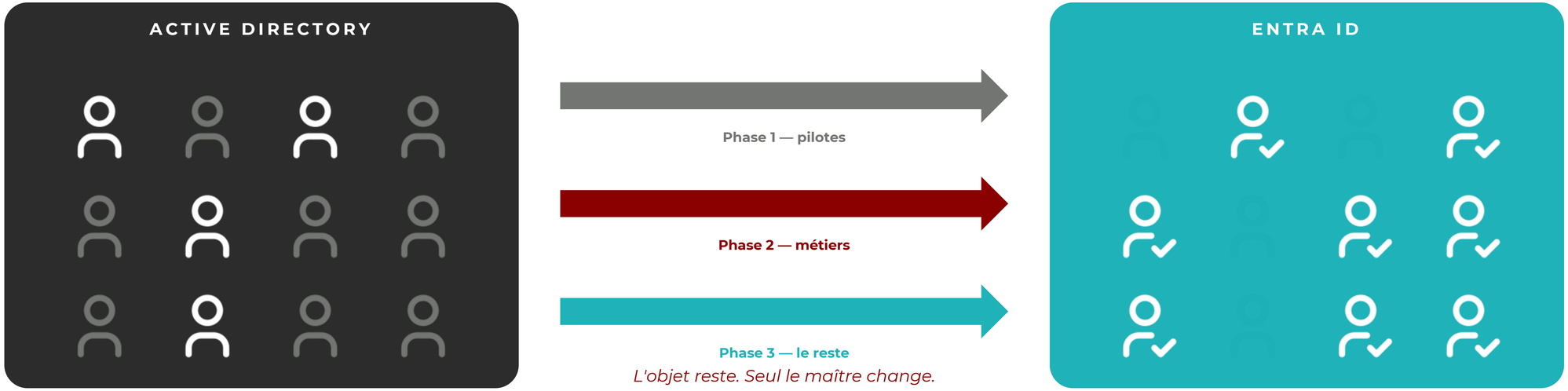
```
PATCH /v1.0/groups/{id}/onPremisesSyncBehavior    {"isCloudManaged": true}
# retour arrière : {"isCloudManaged": false}  ·  imbrication : convertir du bas vers le haut
```

ÉPISODE 3 — ENTRA ID FIRST

Transférer le SOA des utilisateurs

Objet par objet. Par phases. Sans que la victime ne s'en aperçoive.

PIÈCE N°13



Utilisateurs | Contacts | Retour arrière par objet | Transfert SOA : GA

LABO

procédure

1. RH préparée ; flux RH → AD arrêté (cohorte)
2. Postes prêts : WHfB cloud Kerberos trust (16-17)
3. Dernière synchro OK, puis isCloudManaged
4. Vérifier l'event 6956 (sync bloquée)
5. Activer RH → Entra pour la cohorte

API GRAPH

```
PATCH /v1.0/users/{id}/onPremisesSyncBehavior    {"isCloudManaged": true}
# contacts : /v1.0/contacts/{id}/onPremisesSyncBehavior  ·  pas de writeback mot de passe, pas d'AD FS
```

ÉPISODE 3 — ENTRA ID FIRST

Entra Cloud Sync : le chemin retour

Entra écrit, AD recopie. AD n'est plus qu'une projection.

○ PIÈCE N°14

Entra ID

source de vérité

provisioning

Cloud Sync

agent léger, sans SQL

création / mise à jour

LECTURE SEULE POUR L'HUMAIN

Active Directory

projection

STATUT DU RETOUR ENTRA → AD · le transfert du SOA (pièces 12-13), lui, est GA

Groupes — GA

Appartenances — GA

SID — GA

Utilisateurs — PRÉVERSION

Pas de retour vers AD pour ce qu'AD n'a pas besoin de connaître : on projette le minimum.

LABO

procédure

1. Agent de provisioning : dernière version
2. Créer « Microsoft Entra ID to AD sync »
3. Choisir le périmètre et l'OU cible
4. Tester à la demande, puis activer
5. Lire les journaux de provisioning

ANCRE

```
msDS-ExternalDirectoryObjectId  <->  onPremisesSecurityIdentifier · onPremisesSamAccountName
# SOA converti : même objet AD, même SID  ·  utilisateur cloud natif : nouveau SID écrit en retour
```

ÉPISODE 4 — LA DISSECTION

Treize organes. Treize lames.

Un trophée par fonction remplacée. Une boîte qui se remplit.

+ 3 pièces complémentaires : 20 · 23 bis · 29

Authentification

Premier organe à remplacer : celui qui fait battre le cœur.

MIGRABLE

PIÈCE N°16

AVANT — Active Directory

- **Kerberos & NTLM** : le mot de passe voyage jusqu'au DC
- **Cartes à puce ADCS** : une PKI interne à nourrir
- **Contrôleur de domaine** : point unique de confiance

Mot de passe · Smart card · DC on-prem

APRÈS

- **Windows Hello for Business** – cloud Kerberos trust
- **FIDO2 / passkeys** + authentification par certificat
- **Fin de NTLM** : audit, blocage, silence.

Kerberos cloud · Passkeys · Certificat · NTLM off

LABO

procédure

1. Installer le module Hybrid Authentication
2. Créer l'objet Kerberos Entra par domaine
3. Intune : Use Cloud Trust For On Prem Auth
4. Déployer passkeys (FIDO2) et CBA
5. Auditer NTLM, puis le restreindre

COMMANDE

```
Set-AzureADKerberosServer -Domain $domain -UserPrincipalName $upn    # crée krbtgt_AzureAD (RODC)
# NTLMv1 retiré de Windows 11 24H2 et Server 2025  ·  NTLMv2 déprécié, toujours actif
```

Poste de travail

Le poste ne demande plus la permission au domaine.

MIGRABLE

PIÈCE N°17

AVANT — Active Directory

- **Jonction au domaine** + 3 000 paramètres de GPO
- **SCCM** : déploiement, inventaire, patchs
- **Scripts d'ouverture de session** et lecteurs mappés

Domain join · GPO · SCCM

APRÈS — sans AD

- **Entra Join + Intune** : Autopilot, zéro image
- **Settings Catalog** : les GPO utiles, sans le reste
- **LAPS cloud** + co-management transitoire

Entra Join · Autopilot · Settings Catalog · LAPS

LABO

procédure

1. Importer les hash matériels Autopilot
2. Joindre les postes à Entra + Intune
3. Recréer les GPO utiles (Settings Catalog)
4. LAPS : sauvegarder dans Entra ID
5. Basculer les 7 workloads ConfigMgr

PARAMÈTRE

```
./Device/Vendor/MSFT/LAPS/Policies/BackupDirectory = 1      # 1 = Entra ID · 2 = AD
Get-WindowsAutopilotInfo -Online      # import du hash matériel
```

Serveurs

Les serveurs restent. Leur laisse change de main.

CONTOURNABLE

PIÈCE N°18

AVANT — Active Directory

- **Membres du domaine** : GPO, comptes de service
- **gMSA** et mots de passe partagés
- **Administration RDP** avec comptes AD privilégiés

Domaine · gMSA · RDP

APRÈS — sans AD

- **Azure Arc** : SSH Entra pour Linux
- **PIM** : rôles VM Login just-in-time
- **Identité managée Arc** : accès aux ressources Azure

Azure Arc · Linux · PIM · Identité managée

LABO

procédure

1. Connecter le serveur à Azure Arc
2. Déployer AADSSHLoginForLinux
3. Rôle VM Admin / User Login via PIM
4. Se connecter : az ssh arc
5. Identité Arc pour Azure ; gMSA pour AD

COMMANDE

```
az ssh arc --resource-group <RG> --name <serveur>      # rôle Virtual Machine Administrator Login
# Windows : la connexion RDP Entra est documentée pour les VM Azure, pas pour les serveurs Arc
```

PKI

Sans certificat, rien ne s'authentifie. Sans ADCS, tout continue.

MIGRABLE

PIÈCE N°19

AVANT — Active Directory

- **ADCS** : autorité racine sur un DC de 2012
- **Autoenrollment GPO** : magie noire
- **CRL / OCSP** internes, jamais surveillés

ADCS · Autoenroll · CRL

APRÈS — sans AD

- **Microsoft Cloud PKI** : autorité gérée
- **SCEP via Intune** : appareils inscrits uniquement
- **Certificats Wi-Fi, VPN, connexion** sans serveur

Cloud PKI · SCEP / PKCS · Auth. certificat

« Les certificats sont les empreintes digitales du SI. »

LABO

procédure

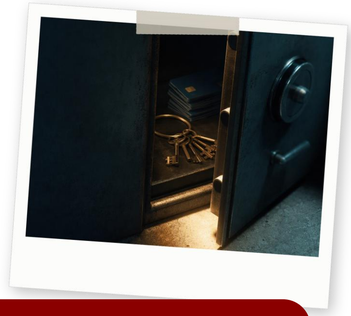
1. Créer l'AC racine Cloud PKI (ou BYOCA)
2. Créer l'AC émettrice, copier l'URI SCEP
3. Déployer les certificats racine approuvés
4. Déployer le profil SCEP Intune
5. Ajouter le SID en SAN URI si AD consomme

PARAMÈTRE

```
SAN URI = {{OnPremisesSecurityIdentifier}}   →   tag:microsoft.com,2022-09-14:sid:<SID>
# 3 AC max par tenant  ·  appareils inscrits dans Intune uniquement  ·  licence Cloud PKI (Intune Suite ou add-on)
```

PKI : les serveurs

Cloud PKI ne signe que pour Intune. Les serveurs restent dans l'ombre.



CONTOURNABLE

PIÈCE N°20

COMPLÉMENT DE LA PIÈCE 19

HORS DE PORTÉE

Windows Server
pas d'inscription Intune

Linux & appliances
hors MDM

Contrôleurs de domaine
LDAPS, Kerberos

Sites web internes
TLS serveur

Key Vault + Azure Arc

Certificats émis dans Key Vault, déployés et renouvelés par l'extension Arc.

Windows · Linux

OPTION 1

ACME / PKI SaaS

Solution tierce, renouvellement automatique : prête pour 200 puis 47 jours.

Web · appliances

OPTION 2

ADCS résiduel confiné

Racine hors ligne, Tier 0, serveurs uniquement.

DC · LDAPS · RDP

OPTION 3

« Peu importe qui signe. Ce qui tue, c'est le renouvellement manuel. »

LABO

procédure

1. Créer le certificat dans Key Vault
2. Émettre : AC intégrée ou CSR + merge
3. Activer l'identité managée Arc
4. Lui donner « Key Vault Secrets User »
5. Déployer KeyVaultForWindows / Linux

COMMANDE

```
az connectedmachine extension create --publisher Microsoft.Azure.KeyVault --type KeyVaultForWindows …
# renouvellement auto : DigiCert, GlobalSign  ·  AC privée : CSR + merge  ·  ACME : solution tierce
```

Réseau 802.1X

Le RADIUS demande toujours à AD. Jusqu'à ce qu'il ne demande plus.

CONTOURNABLE

PIÈCE N°21

AVANT — Active Directory

- **NPS / RADIUS** hébergé… sur un DC
- **Certificats ADCS** pour EAP-TLS
- **Groupe AD = VLAN** : l'annuaire pilote le réseau

NPS · ADCS · VLAN

APRÈS — sans AD

- **EAP-TLS** avec Cloud PKI
- **RADIUS cloud partenaire** (hors Microsoft)
- **Conformité Intune** comme critère d'accès

EAP-TLS · RADIUS cloud · Conformité

LABO

procédure

1. Inventorier SSID et ports EAP-TLS NPS
2. Constat : poste Entra = aucun objet AD
3. Hybride : certificat utilisateur + SID
4. Cible : RADIUS cloud partenaire
5. Surveiller les events KDC 39 / 40 / 41

STATUT

```
KB5014754 : Full Enforcement depuis 2025  ·  mappage faible rejeté par défaut
# NPS mappe le certificat à un compte AD : un poste Entra Join n'a pas de compte ordinateur
```

VPN

On ne rentre plus dans le réseau. On rentre dans l'application.

MIGRABLE

PIÈCE N°22

AVANT — Active Directory

- **VPN + NPS** : authentification AD
- **Accès réseau plat** : tout ou rien
- **Split tunnel** bricolé, jamais maintenu

VPN · Réseau plat · Tout ou rien

APRÈS — sans AD

- **ZTNA** – Global Secure Access Private Access
- **Conditional Access** par application
- **Zero Trust** : identité, poste, contexte

Private Access · Conditional Access · Poste conforme

LABO

procédure

1. Installer le connecteur réseau privé
2. Activer le profil Private Access
3. Quick Access : plages IP et FQDN
4. Déployer le client GSA via Intune
5. Segmenter par app + accès conditionnel

PIÈGE

```
SSO Kerberos via Private Access  =  publier aussi les contrôleurs de domaine (Kerberos 88 …)
# connecteur : Windows Server 2016+, sortant 443, jonction au domaine non requise
```

Applications héritées

L'organe qui refuse la greffe.

RÉSIDUEL | **PIÈCE N°23**

AVANT — Active Directory

- **ADFS** : fédération à maintenir
- **Kerberos / IWA** : SSO intranet
- **LDAP bind** codé en dur dans l'application

ADFS | IWA | LDAP bind

APRÈS — sans AD

- **Entra SAML / OIDC** : ADFS décommissionné
- **App Proxy / Private Access** + délégation Kerberos
- **LDAP** : réécrire, Entra DS… ou résiduel

SAML / OIDC | App Proxy | Entra DS | Résiduel

LABO

procédure

1. Inventorier : AD FS app migration
2. Migrer les apps « Ready to migrate »
3. IWA : App Proxy + KCD, connecteur joint
4. LDAP / NTLM : réécrire ou Entra DS
5. Le reste : DC résiduel confiné

COMMANDE

```
Set-ADComputer <serveurWeb> -PrincipalsAllowedToDelegateToAccount <connecteur>     # KCD (RBCD)
# Entra DS : option de transition pour les apps hébergées dans Azure  →  voir pièce 23-bis
```

Entra Domain Services

Le domaine sous scellés : on ne l'administre plus. Il existe toujours.

CONTOURNABLE

PIÈCE N°23 BIS

COMPLÉMENT DE LA PIÈCE 23

CE QU'IL APPORTE

Zéro DC à gérer
patchs, sauvegardes : côté Microsoft

LDAP · LDAPS · Kerberos · NTLM
les protocoles legacy, intacts

GPO & jonction au domaine
pour les VM de l'application

Délégation Kerberos contrainte
basée sur la ressource (RBCD)

SES LIMITES

Sync à sens unique
Entra → DS : objets en lecture

Pas de Domain Admin
ni extension de schéma

1 domaine par tenant
dans un VNet Azure

Hash de mot de passe requis
à rebours du passwordless

VERDICT DU LABO

OUI POUR

› App LDAP / Kerberos réhébergée dans Azure
› Sas de transition, le temps de réécrire

NON POUR

› OT, industriel, applis restées on-prem
› Progiciel qui étend le schéma

TRANSITION

« Un domaine qu'on n'administre plus reste un domaine. »

LABO

procédure

1. Créer le domaine managé (VNet dédié)
2. DNS du VNet → IP du domaine managé
3. Comptes cloud : nouveau mot de passe
4. Joindre les VM de l'application
5. LDAPS : certificat + NSG restrictif

PIÈGE

```
Admins = groupe « AAD DC Administrators »  ·  ni Domain Admin, ni Enterprise Admin
# 1 domaine managé / tenant · sync Entra → DS à sens unique · trust de forêt : statut à vérifier
```

Fichiers

Le partage réseau, c'est le cadavre dans le placard.

MIGRABLE

PIÈCE N°24

AVANT — Active Directory

- **Partages SMB** + ACL NTFS par groupe AD
- **DFS** et espaces de noms
- **Lecteurs mappés** par GPO

SMB · DFS · Lecteurs GPO

APRÈS — sans AD

- **SharePoint / OneDrive** : Known Folder Move
- **Azure Files** + Entra Kerberos, même cloud-only
- **Accès par identité**, plus par lettre de lecteur

OneDrive · Azure Files · Entra Kerberos

LABO

procédure

1. Activer Entra Kerberos sur le stockage
2. Donner le consentement administrateur
3. Exclure l'app stockage de la MFA (AC)
4. Intune : activer le ticket Kerberos cloud
5. OneDrive : KFMSilentOptIn = Tenant ID

PARAMÈTRE

```
Kerberos/CloudKerberosTicketRetrievalEnabled = 1     ·     OneDrive KFMSilentOptIn = <TenantID>
Set-AzStorageAccount … -EnableAzureActiveDirectoryKerberosForFile $true
```

Impression

Le plus petit organe. Le plus bruyant.

MIGRABLE

PIÈCE N°25

AVANT — Active Directory

- **Serveur d'impression** membre du domaine
- **Pilotes déployés** par GPO
- **Files partagées** et permissions AD

Serveur · Pilotes GPO · Permissions AD

APRÈS — sans AD

- **Universal Print** : plus de serveur
- **Imprimante native** ou connecteur
- **Déploiement Intune** par groupe Entra

Universal Print · Native · Intune

LABO

procédure

1. Installer le connecteur Universal Print
2. Enregistrer les imprimantes héritées
3. Partager, donner l'accès aux groupes
4. Intune : catalogue › Printer Provisioning
5. Couper l'option « hybrid AD » du connecteur

PARAMÈTRE

```
Printer Provisioning : Action = Install · Cloud Device ID · Printer Shared ID · Shared Name
# connecteur : Windows 11 / Server 2022-2025  ·  PrintProvisioning et printers.csv : dépréciés
```

Exchange Hybrid

On l'a gardé au congélateur. On peut enfin l'enterrer.

MIGRABLE

PIÈCE N°26

AVANT — Active Directory

- **Dernier serveur Exchange** : patché, exposé
- **Attributs mail** modifiables on-prem seulement
- **Relais SMTP** des imprimantes et applis

Exchange · Congelé · Relais SMTP

APRÈS — sans AD

- **Attributs Exchange** gérés dans Exchange Online
- **SOA groupes & contacts** transféré au cloud
- **Relais migré**, puis désinstallation

Exchange Online · SOA cloud · Désinstallé

LABO

procédure

1. Passer les boîtes en gestion cloud
2. SOA groupes et contacts vers le cloud
3. Migrer le relais SMTP, couper le CMT
4. MX / Autodiscover vers EXO, vider le SCP
5. Retirer l'hybride, puis désinstaller

COMMANDE

```
Set-Mailbox -Identity <alias> -IsExchangeCloudManaged $true
Set-OrganizationConfig -ExchangeAttributesCloudManagedByDefault $true    # après la dernière boîte
```

DHCP

Il distribue les adresses. Avec la bénédiction d'AD.

MIGRABLE

PIÈCE N°27

AVANT — Active Directory

- **Autorisation dans AD** : sinon, aucun bail
- **Souvent hébergé sur un DC**, par habitude
- **PXE SCCM** : IP helper ou options 66/67

Hébergé sur DC · Autorisation AD · PXE

APRÈS — sans AD

- **Serveur membre** : hors DC, enregistrement DNS
- **Ou DDI** : DHCP, DNS et IPAM unifiés
- **Équipement réseau** : si le DNS est ailleurs

Serveur membre · DDI / IPAM · Équipement réseau

« Une adresse IP ne devrait pas dépendre d'un contrôleur de domaine. »

LABO

procédure

1. Lister les DHCP autorisés dans AD
2. Sortir le DHCP des DC (membre ou DDI)
3. Provisionner avec Autopilot, pas PXE
4. Désautoriser dans AD si DHCP non Windows

COMMANDE

```
Get-DhcpServerInDC    ·    Remove-DhcpServerInDC -DnsName "dhcp01.contoso.com"
# DHCP Windows hors domaine : pas d'autorisation, mais il s'arrête s'il voit un DHCP de domaine
```

DNS

L'annuaire téléphonique de la victime. Plein de faux numéros.

CONTOURNABLE

PIÈCE N°28

AVANT — Active Directory

- **Zones intégrées AD** répliquées par les DC
- **Enregistrements SRV** _ldap, _kerberos, _gc
- **Les DC sont les résolveurs** de tout le monde

Zones AD | SRV | DC résolveur

APRÈS — sans AD

- **Azure DNS / Private Resolver**
- **Nettoyage des SRV** orphelins
- **Redirection conditionnelle** vers la zone résiduelle

Azure DNS | SRV nettoyés | Redirection

LABO

procédure

1. Inventorier les DC et les SRV (nltest)
2. Créer le Private Resolver (2 subnets /28)
3. Règle : zone AD → DC résiduels
4. Lier le ruleset aux VNet
5. Nettoyer métadonnées et SRV des DC retirés

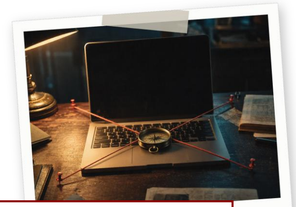
COMMANDE

```
New-AzDnsForwardingRulesetForwardingRule … -DomainName "corp.contoso.com." -TargetDnsServer $dc
nltest /dsgetdc:corp.contoso.com /force   ·   Get-DnsServerResourceRecord -ZoneName <zone> -RRType Srv
```

ÉPISODE 4 — LA DISSECTION · COMPLÉMENT DE LA PIÈCE 28

DNS : qui guide les postes ?

Le DC ne résout plus. Chaque poste doit pourtant trouver son chemin.



PIÈCE N°29

Au bureau : DHCP

Options 6 et 15/119 : résolveurs et suffixes

En mobilité : Private DNS

Global Secure Access : une règle de résolution par suffixe interne

PRÉVERSION

Politique : Intune

CSP ADMX_DnsClient : liste de suffixes

Enregistrement : DHCP / DDI

DHCP Windows ou DDI : il inscrit les postes Entra Join

POSTE ENTRA JOIN

Poste → **Résolveur réseau / Private Resolver** → redirection → **Zone AD résiduelle**

LABO

procédure

1. DHCP : options 6, 15 et 119
2. GSA : activer Private DNS + suffixes
3. Contrôler la NRPT sur le poste
4. Intune : ADMX_DnsClient (suffixes)
5. DHCP : enregistrer A / PTR à leur place

COMMANDE

```
Set-DhcpServerv4DnsSetting -DynamicUpdates Always -DeleteDnsRROnLeaseExpiry $true
Get-DnsClientNrptPolicy      # une entrée par suffixe GSA  ·  Kerberos : toujours en FQDN
```

Gouvernance & cycle de vie

La partie que personne ne voit. Celle qui compte.

MIGRABLE

PIÈCE N°30

AVANT — Active Directory

- **MIM 2016** : support étendu jusqu'en janvier 2029
- **Scripts de provisioning** maison
- **Revues manuelles** dans un tableur

MIM · Scripts · Tableur

APRÈS — sans AD

- **Lifecycle Workflows** : entrée, mutation, sortie
- **Access packages** : demande, approbation, expiration
- **Access reviews** : recertifier, puis éteindre MIM

Lifecycle · Access packages · Reviews

« La boucle ouverte avec la source RH (pièce 11) se referme ici. »

LABO

procédure

1. Entrée / mutation / sortie : Lifecycle Workflows
2. Étendre via Logic Apps (Consumption)
3. Distribuer les accès par packages
4. Recertifier par revues d'accès
5. Planifier la sortie de MIM avant 2029

STATUT

```
MIM 2016 SP2 : fin du support étendu le 9 janvier 2029
# Lifecycle Workflows : 14 modèles intégrés  ·  licence Entra ID Governance ou Entra Suite
```

ÉPISODE 5 — LA SURVEILLANCE

Le sergent vous observe.

Un AD à moitié migré est une cible idéale.

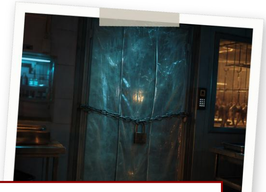
- Deux mondes, deux surfaces d'attaque
- Des comptes de synchronisation surpuissants
- Une vigilance qui baisse avec la migration
- L'attaquant, lui, ne migre pas

PIÈCE N°31

ÉPISODE 5 — LA SURVEILLANCE

Durcir la kill room

Pendant la migration, la victime doit être mieux protégée qu'avant.



PIÈCE N°32

Tiering

Tier 0 isolé, admin dédiée

PIM

Privilèges juste-à-temps

LAPS

Plus de mot de passe local partagé

Comptes dormants

Désactiver, puis supprimer

Kerberos durci

AES only, pas de délégation libre

ITDR / SIEM
MDI + Sentinel

Détection, corrélation, réponse

Comptes de sync

Traités comme du Tier 0

Restauration de forêt

Testée. Vraiment testée.

KILL ROOM – ACCÈS RESTREINT – TIER 0 – KILL ROOM – ACCÈS RESTREINT – TIER 0

LABO

procédure

1. Reset krbtgt 2×, 10 h d'écart
2. Admins dans Protected Users
3. Imposer AES, en finir avec RC4
4. Serveurs Entra Connect = Tier 0
5. LAPS DSRM, MDI, reprise de forêt testée

ATTRIBUT

```
msDS-SupportedEncryptionTypes = 0x18      # AES128 + AES256 uniquement
# audit RC4 : events 4768 / 4769  ·  Protected Users : jamais de comptes de service
```

ÉPISODE 5 — LA SURVEILLANCE

La trinité des protocoles

Trois suspects. Trois dossiers. Un seul verdict.

○ PIÈCE N°33

NTLM

CHEF D'ACCUSATION

Relais, pass-the-hash, mots de passe faibles.

Né en 1993. Toujours en liberté.

À NEUTRALISER

LDAP simple bind

CHEF D'ACCUSATION

Mot de passe en clair sur le réseau.

Event 2889 : ses aveux.

À NEUTRALISER

Délégation Kerberos non contrainte

CHEF D'ACCUSATION

Un serveur qui peut être n'importe qui.

Complice de tous les mouvements latéraux.

À NEUTRALISER

LABO

procédure

1. Auditer NTLM, puis Restrict NTLM
2. Exiger la signature LDAP sur les DC
3. Channel binding : When supported → Always
4. Traquer la délégation non contrainte
5. Vérifier que NTLMv1 a disparu

GPO

```
DC : LDAP server signing requirements = Require  ·  LDAP channel binding token = Always
Get-ADComputer -Filter {TrustedForDelegation -eq $true}      # en excluant les DC
```

○ PIÈCE N°34

FINALE — AD MINIMIZATION

On ne le tue pas toujours.

Certaines victimes méritent l'exil, pas l'exécution.

- **Industrie & OT** : SCADA, automates, contrôle-commande
- **Progiciels propriétaires** : LDAP gravé dans le code
- **Sites isolés** : réseaux fermés, zéro cloud
- **→ L'exil dans la forêt** : confiné, minimal, surveillé.

OT / industriel

Progiciel legacy

AD confiné

FINALE — AD MINIMIZATION

L'annuaire technique industriel

Un AD enfant, alimenté par Entra, enfermé dans sa cage.

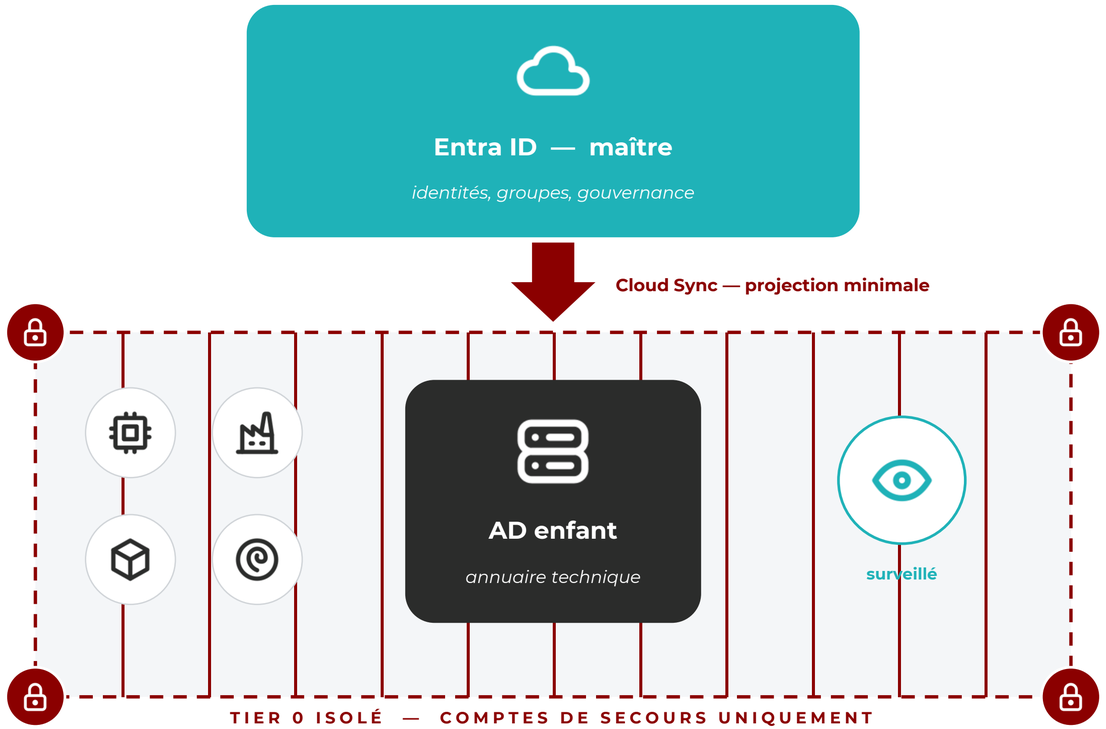
PIÈCE N°35

Alimenté par Entra

Cloud Sync filtré · utilisateurs : préversion

Administration minimale

Comptes de secours, pas de console



Pas de poste utilisateur

Aucune session interactive

Minimum d'objets

Comptes de service, machines, groupes

LABO

procédure

1. Réduire la synchro aux OU utiles
2. Cloud Sync : filtre par OU ou groupe
3. GPO : refuser l'ouverture locale
4. GPO : refuser l'ouverture RDP
5. Cibler les utilisateurs standard

DROITS

```
SeDenyInteractiveLogonRight + SeDenyRemoteInteractiveLogonRight  →  groupe des utilisateurs standard
# un refus l'emporte toujours : jamais les comptes d'administration ni de service
```

FINALE — AD MINIMIZATION

La feuille de route

Sept étapes. Le sang pâlit à chaque lame rangée.

PIÈCE N°36

1 — Cadrage

inventaire, preuves, kill room

2 — Entra ID First

source RH, SOA des groupes

3 — Postes & identités

Entra Join, Windows Hello, puis SOA utilisateurs

4 — PKI · Réseau · VPN

Cloud PKI, 802.1X, Global Secure Access

5 — Applications

ADFS → Entra, App Proxy

6 — Minimisation

AD technique confiné

7 — Décommission ou confinement

affaire classée

Chaque étape a sa preuve, son plan de repli et sa lame dans la boîte.

FINALE — AD MINIMIZATION

Affaire classée

Les quatre preuves qu'il ne reste plus rien à tuer.

PIÈCE N°37

RAPPORT DE CLÔTURE — DOSSIER ACTIVE DIRECTORY

- **Plus de NTLM**
  Audit vide 90 jours (périmètre éliminé)
- **Plus de bind LDAP non identifié**
  Event 2889 : silence (hors AD confiné)
- **Plus d'ADFS**
  Domaines Managed + 0 connexion AD FS
- **Plus de poste joint au domaine**
  100 % Entra Join + Intune

CASE CLOSED

Le corps peut être enlevé.

LABO

procédure

1. NTLM : 0 event 8004 / 90 j (périmètre)
2. LDAP : 0 event 2889 (niveau 2)
3. AD FS : domaines Managed + 0 connexion
4. Postes : 0 PC actif joint à AD
5. Exchange désinstallé, SCP nettoyé

PREUVE

```
Get-ADComputer -Filter 'OperatingSystem -notlike "*Server*"' -Properties LastLogonDate
# GET /v1.0/domains → authenticationType = "Managed"  ·  LastLogonDate : précision ≈ 14 jours
```

IDENTITY DAYS

20 octobre 2026 – PARIS

« On ne tue pas Active Directory par vengeance.
On le tue par évolution. »

CASE CLOSED

○ PIÈCE N°38

Questions ?

Jean-Sébastien Duchêne
Directeur technique — Magellan

LinkedIn · Jean-Sébastien Duchêne

Identity Days 2026 · Paris