

GUIDE DE RÉFÉRENCE · SÉCURITÉ & FORENSIQUE

Les logs Microsoft

Active Directory · Entra ID · Microsoft 365

Quel log pour quoi — sources, champs, rétention, KQL, playbooks d'investigation et architecture de collecte.



Frédéric PEREZ

Architecte IAM & Expert Sécurité — Entra ID / M365

Les logs Microsoft — AD, Entra ID & Microsoft 365

Ce guide vise un objectif : faire de vous une référence sur les journaux Microsoft. Il couvre les trois plans — **Active Directory on-prem, Microsoft Entra ID et Microsoft 365 / Purview** — jusqu'au niveau des Event IDs, codes d'échec, champs, types d'enregistrement et tables de chasse. Chaque section répond à trois questions : quel journal, quelle information exacte, comment y accéder et combien de temps il reste disponible.

À jour (2026) — faits volatils vérifiés sur Microsoft Learn : rétentions Entra 7/30 j et Purview 180 j / 1 an / 10 ans, Graph activity logs, dépréciation de Get-MessageTrace (→ Get-MessageTraceV2, sept. 2025), et bascule de la recherche d'audit vers l'API Graph AuditLogQuery. Recoupez avant tout audit formel.

Sommaire

1. L'écosystème de journalisation
2. Fondamentaux transverses
3. Active Directory (on-premises)
4. Microsoft Entra ID
5. Microsoft 365 & Purview
6. Architecture de collecte & rétention
7. Cartographie MITRE ATT&CK → source de log
8. Playbooks d'investigation
9. Boîte à outils KQL & PowerShell
10. Pièges & bonnes pratiques
- A. Annexe — Champs pivots par journal
- B. Annexe — Glossaire & sources

1. L'écosystème de journalisation

La règle d'or : les trois plans sont des silos distincts. Chacun a ses propres journaux, sa propre rétention et ses propres outils d'accès. Un même incident laisse des traces dans plusieurs silos — la maîtrise consiste à savoir lequel interroger, dans quel ordre, et à recoller les événements par leurs identifiants de corrélation.

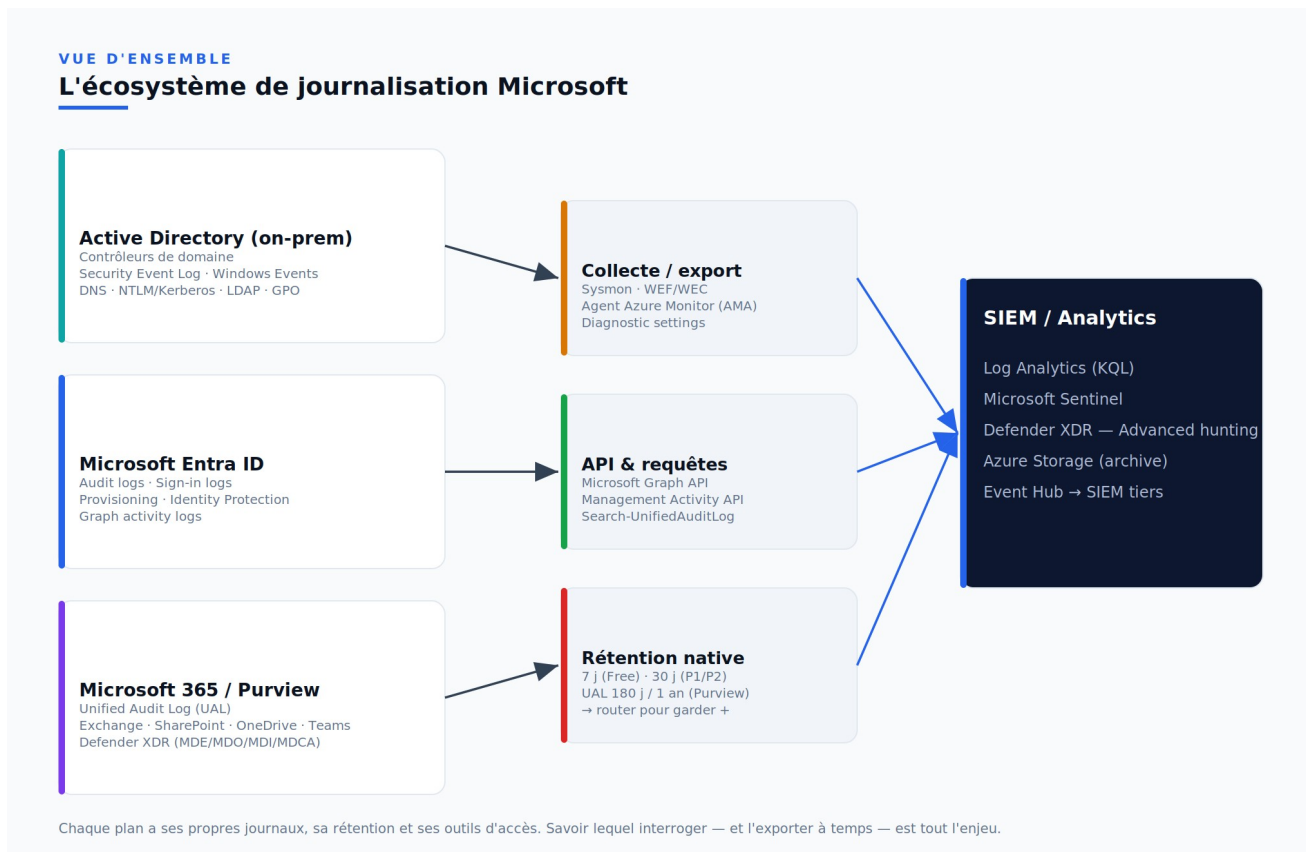


Figure 1 — Les trois plans de journalisation et leurs chemins de collecte vers un SIEM.

1.1 Trois plans, trois logiques

- **Active Directory (on-prem)** : journalisation Windows (Event Log) sur les contrôleurs de domaine. Riche mais bruyante, locale à chaque DC, à centraliser soi-même.
- **Microsoft Entra ID** : journaux cloud structurés (audit, connexions, provisioning, risque), exposés via le portail et Microsoft Graph. Rétention courte par défaut.
- **Microsoft 365 / Purview** : le Unified Audit Log agrège l'activité applicative (Exchange, SharePoint, Teams...) plus les événements Entra ID. Rétention gérée par Purview, indépendante d'Entra.

Piège fondateur — la rétention du Unified Audit Log (Purview) et celle des logs Entra ID sont sur deux horloges différentes. Une licence qui prolonge l'une n'a aucun effet sur l'autre. La piste identité — souvent le point de départ d'une intrusion — est fréquemment la plus courte du tenant.

2. Fondamentaux transverses

2.1 Le réflexe « quel log pour quoi »

Avant d'ouvrir un journal, formulez la question. La figure fait correspondre les questions d'investigation les plus fréquentes à la source qui y répond le plus directement.

Quel log pour quelle question ?

Qui s'est connecté, d'où, avec quel résultat ?	→ Entra Sign-in logs (+ Conditional Access)
Qui a modifié un rôle, une app, une policy ?	→ Entra Audit logs (directoryAudits)
Compte compromis : risque & détections ?	→ Identity Protection (riskDetections)
Règle de transfert, accès boîte mail ?	→ UAL / Exchange (New-InboxRule, MailItemsAccessed)
Partage externe, téléchargement massif ?	→ UAL / SharePoint-OneDrive (AnonymousLink, FileDownloaded)
Appli malveillante : consentement OAuth ?	→ Entra Audit + UAL (Consent to application)
Auth on-prem : Kerberos/NTLM, spray, DA ?	→ Windows Security 4768/4769/4776/4624/4672 · MDI
Reconnaissance AD (énumération) ?	→ Defender for Identity — IdentityQueryEvents
Appels d'API applicatifs anormaux ?	→ Microsoft Graph activity logs

Figure 2 — Aide-mémoire : à chaque question son journal de référence.

2.2 Horodatage, corrélation, identités

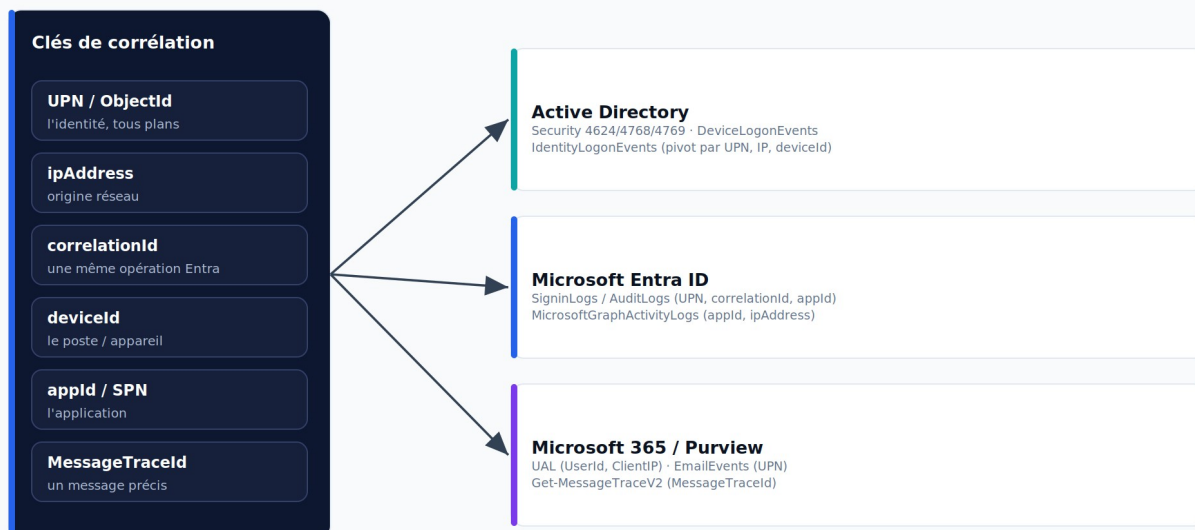
- **UTC partout.** Les journaux cloud sont en UTC. Convertissez au fuseau local seulement pour la lecture, jamais pour la corrélation.
- **correlationId.** Fil conducteur d'Entra ID : une même opération (connexion + Conditional Access + audit) partage souvent un correlationId. La clé pour recoller une « histoire ».
- **Identités multiples.** UPN, ObjectId (GUID), SID on-prem, ImmutableId. Un même utilisateur apparaît sous des identifiants différents selon le plan — gardez une table de correspondance.
- **Acteur vs cible.** Distinguez qui agit (initiatedBy / SubjectUserName) de sur quoi (targetResources / ObjectId).

2.3 Pivoter entre les plans

Une intrusion moderne traverse les silos. La méthode consiste à isoler une clé de corrélation, puis à la retrouver dans chaque plan pour reconstituer la chronologie complète.

MÉTHODE

Pivoter entre les plans avec les clés de corrélation



Une intrusion traverse les plans : partez d'une clé (un UPN, une IP), retrouvez-la dans chaque journal, recollez la chronologie en UTC.

Figure 3 — Les clés de corrélation et les journaux qu'elles déverrouillent dans chaque plan.

Clé	Portée et usage
UPN / Objectid	L'identité sur tous les plans. Objectid (GUID) est stable, l'UPN peut changer.
ipAddress / ClientIP	Origine réseau ; recouper avec l'ASN et la géolocalisation Entra.
correlationId	Relie les événements d'une même opération Entra (sign-in ↔ audit ↔ CA).
deviceId	Le poste/appareil ; joint SignInLogs, DeviceLogonEvents, IntuneDevices.
appId / SPN	L'application ; pivot vers ServicePrincipalSignInLogs et Graph activity.
MessageTraceId / NetworkMessageId	Un message précis (Get-MessageTraceV2, EmailEvents).

2.4 Licences & prérequis (ce qui débloque quoi)

Capacité	Prérequis	Note
Audit & Sign-in logs 30 j	Entra ID P1/P2	7 j en Free
Identity Protection (riskyUsers, détections détaillées)	Entra ID P2	P1 = signaux limités
Graph activity logs	P1/P2 + diagnostic setting	0 j sans export
MailItemsAccessed, Send, SearchQueryInitiated	Purview Audit (Premium) / E5	Crucial en BEC
UAL 1 an (→ 10 ans)	Purview Audit Premium / add-on	Standard = 180 j
Détections identité on-prem (4662→DCSync...)	Defender for Identity (MDI)	Capteur sur les DC
Corrélation multi-source, UEBA, rétention longue	Microsoft Sentinel	Log Analytics + connecteurs

3. Active Directory (on-premises)

Sur AD, tout se joue dans le journal de sécurité Windows des contrôleurs de domaine. La donnée est là, mais brute, volumineuse et dispersée : la valeur vient de la politique d'audit activée et de la centralisation.

3.1 Où vivent les journaux

Journal / canal	Contenu	Emplacement
Security	Authentifications, gestion comptes/groupes, accès objets (SACL)	Event Viewer · DC & hôtes
Directory Service	Réplication, LDAP, modifications d'annuaire (5136-5141)	Event Viewer · DC
DNS Server	Requêtes et modifications de zones	DC DNS / canal Analytic
NTLM/Operational	Authentifications NTLM entrantes/sortantes (8001-8004)	Microsoft-Windows-NTLM
PowerShell/Operational	Script blocks (4104), modules (4103)	Microsoft-Windows-PowerShell
System	Services, tâches planifiées, Netlogon (5827/5828)	Event Viewer · tout hôte

3.2 Activer le bon audit (Advanced Audit Policy)

Par défaut, l'audit AD est partiel. Activez l'Advanced Audit Policy via GPO sur les catégories qui comptent :

- **Account Logon** — validation Kerberos/NTLM sur les DC (4768, 4769, 4771, 4776).
- **Logon/Logoff** — ouvertures de session (4624/4625), privilèges (4672).
- **Account / Group Management** — création/modification de comptes et groupes (47xx).
- **DS Access** — accès aux objets d'annuaire via SACL (4662) : indispensable pour DCSync et la reconnaissance.
- **Detailed Tracking** — création de processus (4688) avec ligne de commande (à activer séparément).

Sans SACL, pas de 4662. L'audit DS Access ne produit d'événements que si une SACL est posée sur les objets à surveiller. Pour détecter un DCSync, auditez le droit de réplication (DS-Replication-Get-Changes-All, GUID 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2) sur l'objet domaine.

3.3 Flux d'authentification et Event IDs

ACTIVE DIRECTORY

Flux d'authentification et Event IDs clés

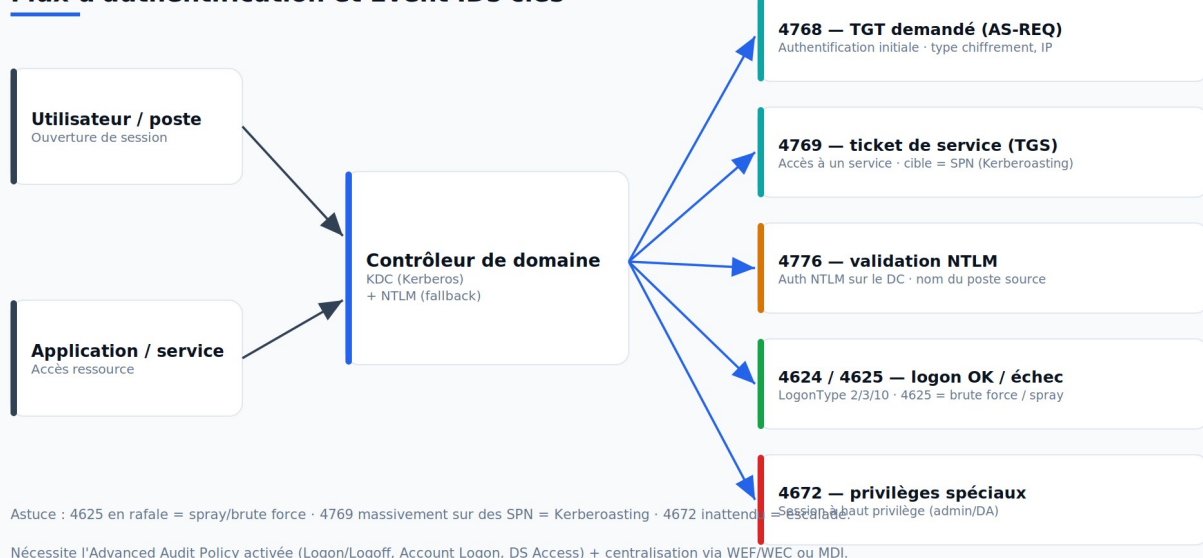


Figure 4 — Du poste au contrôleur de domaine : les Event IDs à connaître.

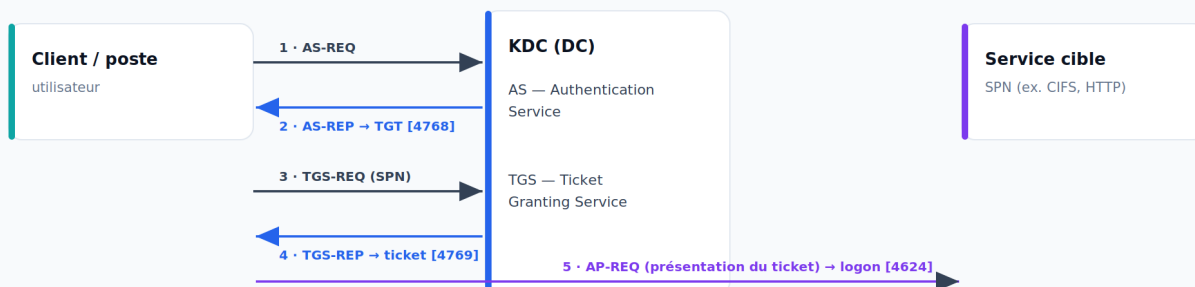
Aide-mémoire Event IDs

ID	Signification	Usage en investigation
4624	Ouverture de session réussie	LogonType (voir 3.4) ; TargetUserName, IpAddress
4625	Échec d'ouverture de session	En rafale = brute force / password spray ; Sub-Status
4634 / 4647	Fermeture de session	Durée de session, corrélation avec 4624
4672	Privilèges spéciaux assignés	Session à haut privilège (admin, Domain Admin)
4768	TGT Kerberos demandé (AS-REQ)	Type de chiffrement, IP source, code de résultat
4769	Ticket de service (TGS)	Cible = SPN ; volume/RC4 anormal = Kerberoasting
4771	Échec de pré-auth Kerberos	Codes 0x18 (mdp), 0x12 (compte KO)
4776	Validation NTLM (DC)	Codes 0xC000006A, 0xC0000234... ; poste source
4740	Compte verrouillé	Corréler avec 4625/4771 pour la source
4720 / 4722 / 4726	Compte créé / activé / supprimé	Cycle de vie des comptes
4728 / 4732 / 4756	Ajout à groupe (global/local/universel)	Escalade via groupe privilégié
4738	Compte modifié	Changement UAC, mot de passe, attributs
4662	Opération sur objet AD (SACL)	Réplication (DCSync), reconnaissance
5136 / 5141	Objet d'annuaire modifié / supprimé	Modif d'attribut (scriptPath, msDS-*)
4688	Création de processus	Ligne de commande ; exécution suspecte
1102	Journal de sécurité effacé	Anti-forensique — alerte forte
4104 / 4103	PowerShell Script Block / Module	Contenu et pipeline des scripts

3.4 Kerberos en détail

ACTIVE DIRECTORY — KERBEROS

Échanges de tickets, Event IDs et codes d'échec



Types de chiffrement (ticket)

0x12 · AES256 — sain
0x11 · AES128 — sain
0x17 · RC4-HMAC — legacy / Kerberoasting
0x03 · DES — obsolète

Codes d'échec 4768 / 4769 / 4771

0x6 · utilisateur inconnu
0x12 · compte désactivé / verrouillé / expiré
0x18 · mauvais mot de passe (pré-auth)
0x25 · dérive d'horloge (clock skew)

NTLM (fallback) : événement 4776 sur le DC — codes 0xC000006A (mauvais mdp), 0xC0000064 (utilisateur inconnu), 0xC0000234 (verrouillé).

Astuce : pic de 4769 en RC4 (0x17) sur des SPN = Kerberoasting · rafale de 4771/4776 multi-comptes = password spray.

Figure 5 — Échanges de tickets Kerberos, Event IDs et codes d'échec associés.

LogonType (champ de 4624/4625)

Type	Sens	Signal
2	Interactif (console)	Ouverture locale au clavier
3	Réseau	Accès à un partage/service ; NTLM/Kerberos
4	Batch	Tâche planifiée
5	Service	Démarrage d'un service (compte de service)
7	Unlock	Déverrouillage de session
8	NetworkCleartext	Identifiants en clair (IIS basic, legacy)
9	NewCredentials	RunAs /netonly (souvent pass-the-hash)
10	RemoteInteractive	RDP / Terminal Services
11	CachedInteractive	Identifiants mis en cache (hors ligne)

Signaux à haute valeur — LogonType 9 (NewCredentials) inattendu = potentiel pass-the-hash · LogonType 10 depuis une IP inhabituelle = RDP suspect · 4769 en RC4 (0x17) sur des SPN = Kerberoasting · 4662 avec droit de réplication depuis un hôte non-DC = DCSync.

3.5 Sources complémentaires souvent oubliées

Source	Ce qu'elle apporte
AD CS (Certificate Services)	4886/4887 (demande/émission de certificat), 4898 (modèle) — abus ESC1-8, persistance par certificat.
LDAP signing / channel binding	2887/2889 (liaisons non signées), 3039-3041 — durcissement LDAP, détection d'outils d'énumération.
Requêtes LDAP (1644)	Requêtes coûteuses/inefficaces — traque de reconnaissance (BloodHound).
Netlogon (5827/5828)	Connexions sécurisées refusées/autorisées — Zerologon, comptes machine vulnérables.

Source	Ce qu'elle apporte
NTLM/Operational (8001-8004)	Auth NTLM entrantes/sortantes — legacy à éliminer, relais NTLM.
AMSI / Defender (1116/1117)	Détections de scripts malveillants en mémoire.

Sysmon — Event IDs de référence

ID	Événement	Usage
1	Création de processus	Hash, ligne de commande, parent
3	Connexion réseau	IP/port source et destination
7	Chargement d'image (DLL)	DLL non signées, injection
8	CreateRemoteThread	Injection de code inter-processus
10	ProcessAccess	Accès à LSASS (vol d'identifiants)
11	Création de fichier	Dépôt de payload, persistance
12/13/14	Registre	Persistance (Run keys, services)
22	Requête DNS	C2, exfiltration DNS
23 / 25	Suppression de fichier / altération de process	Anti-forensique, tampering

3.6 Centraliser et détecter

- **WEF/WEC** — Windows Event Forwarding sans agent : abonnements source-initiated (le plus scalable) ou collector-initiated ; les événements arrivent dans le canal ForwardedEvents, filtrés en XPath.
- **Sysmon** — télémétrie enrichie pilotée par une configuration (ex. base SwiftOnSecurity/Olaf) ; incontournable en threat hunting.
- **Defender for Identity (MDI)** — capteur sur les DC/AD CS qui transforme ces événements bruts en détections (reconnaissance, mouvement latéral, DCSync, Golden Ticket) et alimente l'Advanced Hunting.

Scénarios AD emblématiques

- **Password spray** : multiples 4625/4771 sur de nombreux comptes depuis une même IP ; pics de 4740.
- **Kerberoasting** : pic de 4769 sur des SPN en chiffrement RC4 (0x17).
- **DCSync** : 4662 avec DS-Replication-Get-Changes-All depuis un hôte non-DC (détecté nativement par MDI).
- **Pass-the-hash / lateral** : 4624 LogonType 9, 4776 NTLM en chaîne entre postes.
- **Escalade** : 4728/4732 ajoutant un compte à Domain Admins, souvent précédé d'un 4672.

4. Microsoft Entra ID

Entra ID expose des journaux cloud structurés, accessibles via le portail (Monitoring & health) et Microsoft Graph. Quatre familles à connaître : Audit, Sign-ins, Provisioning et Identity Protection — plus les Graph activity logs.

4.1 Audit logs (directoryAudits)

Le « quoi » : toute modification de l'annuaire et opération administrative — attribution de rôle, création d'app, ajout de secret, modification de policy, consentement. Champs clés : `activityDisplayName`, `category`, `initiatedBy`, `targetResources`, `result`, `correlationId`.

Catégories utiles : `UserManagement`, `GroupManagement`, `ApplicationManagement`, `RoleManagement`, `Policy`, `Device`, `DirectoryManagement`, `AuthorizationPolicy`.

4.2 Sign-in logs — 4 types à ne pas confondre

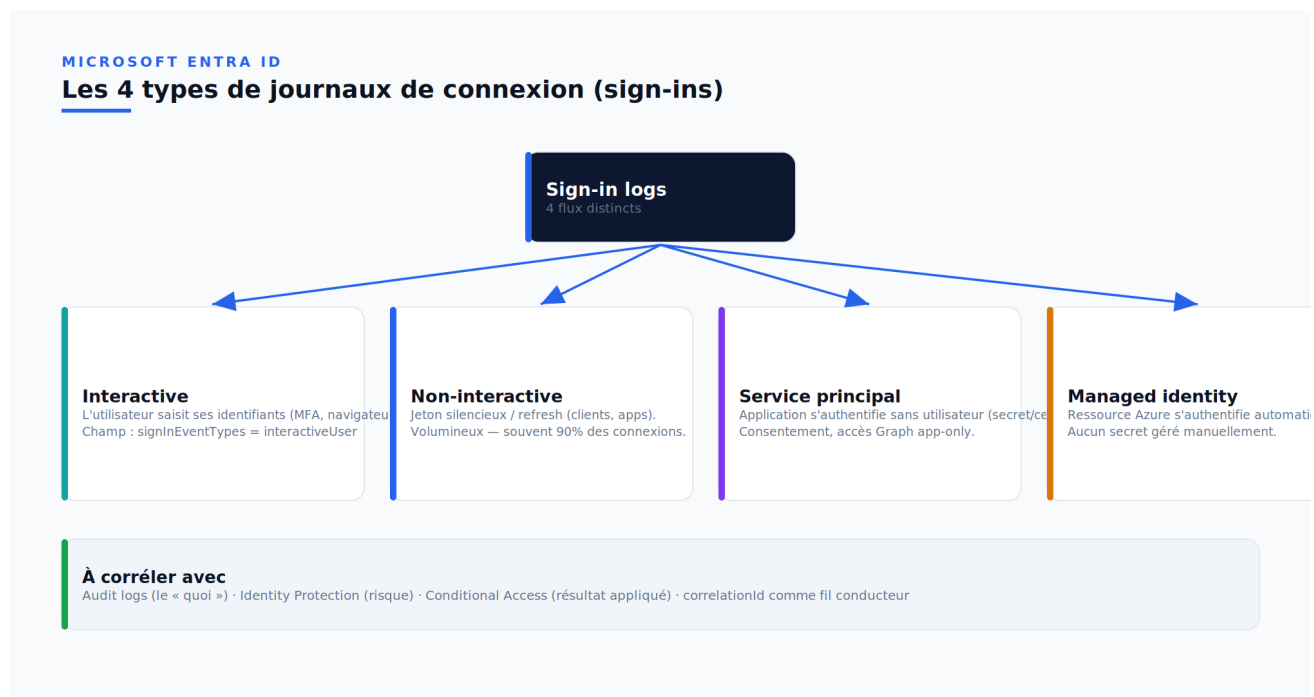


Figure 6 — Les quatre flux de connexion Entra ID.

Type	Ce qu'il capture	Signal
Interactive	Utilisateur saisit ses identifiants (MFA, navigateur)	Point de départ d'une compromission
Non-interactive	Jetons silencieux / refresh (clients, apps)	Très volumineux (souvent >80 %)
Service principal	Application s'authentifie sans utilisateur	Accès app-only, secrets/certs
Managed identity	Ressource Azure s'authentifie seule	Aucun secret manuel

Champs à exploiter : `userPrincipalName`, `appDisplayName`, `ipAddress`, `location`, `status.errorCode`, `conditionalAccessStatus`, `authenticationRequirement`, `authenticationDetails`, `riskLevelAggregated`, `resourceDisplayName`.

Codes d'erreur de connexion fréquents (status.errorCode)

Code	Signification
0	Connexion réussie
50126	Identifiant invalide (mauvais mot de passe) — brique du password spray
50053	Compte verrouillé (Smart Lockout) ou spray détecté

Code	Signification
50055 / 50057	Mot de passe expiré / compte désactivé
50074 / 50076	MFA requise / MFA nécessaire depuis un nouvel emplacement
53003	Bloqué par une stratégie d'accès conditionnel
50158	Échec d'exigence externe (challenge de sécurité)
65001 / 90095	Consentement requis / consentement admin requis (apps OAuth)
700016	Application introuvable dans le tenant
50097 / 530032	Device authentication requise / bloqué par restriction de sécurité

Accès conditionnel dans le log

Chaque connexion porte `conditionalAccessStatus` (success / failure / notApplied) et le détail `appliedConditionalAccessPolicies` (politiques évaluées, `grantControls` appliqués). C'est là qu'on voit si le MFA a réellement été exigé — et contourné.

4.3 Provisioning & Identity Protection

- **Provisioning logs** — synchronisation d'identités vers/depuis des apps SaaS (SCIM) et provisioning on-prem. Trace un compte créé automatiquement.
- **Identity Protection** — `riskDetections` et `riskyUsers` (P2). Le « pourquoi c'est risqué ».

Types de détection de risque (`riskEventType`)

<code>riskEventType</code>	Sens
<code>leakedCredentials</code>	Identifiants trouvés dans une fuite publique
<code>unfamiliarFeatures</code>	Connexion aux caractéristiques inhabituelles pour l'utilisateur
<code>unlikelyTravel</code>	Voyage impossible entre deux connexions
<code>anonymizedIPAddress</code>	IP anonyme (Tor, VPN d'anonymisation)
<code>maliciousIPAddress</code>	IP connue pour activité malveillante
<code>passwordSpray</code>	Schéma de password spray détecté
<code>newCountry / suspiciousBrowser</code>	Nouveau pays / navigateur suspect
<code>tokenIssuerAnomaly</code>	Anomalie d'émetteur de jeton (fédération falsifiée)
<code>mcasSuspiciousInboxManipulation</code>	Règles de boîte suspectes (via Defender for Cloud Apps)
<code>adminConfirmedUserCompromised</code>	Compromission confirmée par un administrateur

4.4 Microsoft Graph activity logs

Généralement disponibles depuis avril 2024, ils enregistrent chaque requête HTTP adressée à Microsoft Graph. Champs : `requestUri`, `requestMethod`, `responseStatusCode`, `appId`, `ipAddress`, `userAgent`, `roles/scopes`. Complémentaires du UAL (qui journalise des actions, pas des appels d'API). Précieux pour repérer un usage anormal d'une application ou l'exfiltration via Graph.

Attention rétention — les Graph activity logs exigent une licence P1/P2 et ne sont PAS conservés par défaut : sans diagnostic setting vers Log Analytics/Storage/Event Hub, aucune donnée n'est gardée.

4.5 Rétention Entra ID par licence

Journal	Free	Entra ID P1 / P2
Audit logs	7 jours	30 jours
Sign-in logs	7 jours	30 jours
Graph activity logs	Non disponible	0 j — export requis dès le 1er jour
Risky users / risk detections	—	Jusqu'à remédiation (P2)

4.6 Exporter : diagnostic settings & tables Log Analytics

Le diagnostic setting (rôle Security Administrator) sélectionne des catégories et une destination. Correspondance catégorie → table KQL :

Catégorie de diagnostic	Table Log Analytics
AuditLogs	AuditLogs
SignInLogs	SignInLogs
NonInteractiveUserSignInLogs	AADNonInteractiveUserSignInLogs
ServicePrincipalSignInLogs	AADServicePrincipalSignInLogs
ManagedIdentitySignInLogs	AADManagedIdentitySignInLogs
ProvisioningLogs	AADProvisioningLogs
RiskyUsers / UserRiskEvents	AADRiskyUsers / AADUserRiskEvents
MicrosoftGraphActivityLogs	MicrosoftGraphActivityLogs

Accéder aux journaux Entra — exemples

```
# PowerShell (Microsoft Graph)
Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq 'Add member to role'" -Top 50
Get-MgAuditLogSignIn -Filter "userPrincipalName eq 'user@contoso.com'" -Top 50

# Graph REST – connexions non-interactives
GET /auditLogs/signIns?$filter=signInEventTypes/any(t:t eq 'nonInteractiveUser')
```

5. Microsoft 365 & Purview

5.1 Unified Audit Log (UAL)

Le journal d'audit unifié agrège l'activité de plus de 1 600 types d'actions à travers les charges de travail M365, y compris Entra ID. C'est le point d'entrée unique pour l'activité applicative.

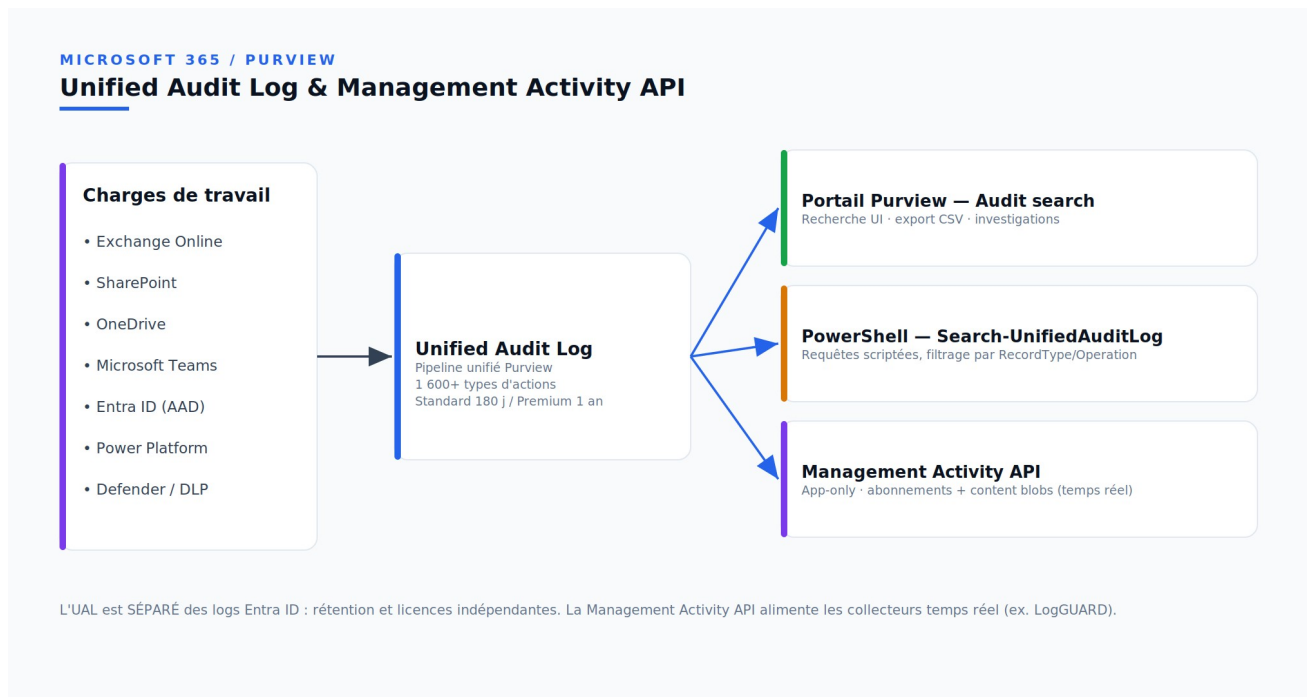


Figure 7 — Du UAL aux trois modes d'accès : portail, PowerShell, Management/AuditLogQuery API.

Champs pivots : CreationTime, Operation, RecordType, Workload, UserId, ClientIP, ObjectId, ResultStatus — plus un bloc AuditData JSON riche, propre à chaque workload.

RecordType — repères

RecordType	Contenu
AzureActiveDirectory (8/15)	Événements identité (connexions, consentements) dans le UAL
ExchangeAdmin (1)	Cmdlets d'administration Exchange
ExchangeItem (2)	Actions sur éléments de boîte (accès, envoi, suppression)
SharePointFileOperation (6)	Accès, téléchargement, modification de fichiers
SharePointSharingOperation (14)	Partages, liens anonymes, invitations
OneDrive (4)	Opérations OneDrive
MicrosoftTeams (25/28)	Messages, réunions, appartenances
SecurityComplianceCenter / ThreatIntelligence	DLP, alertes, détections Defender

5.2 Exchange Online — trois journaux et les opérations clés

- **Mailbox audit** — accès et actions dans les boîtes (activé par défaut ; alimente le UAL). Attention à AuditBypassEnabled qui masque un compte.
- **Admin audit** — cmdlets exécutées par les administrateurs (via Search-UnifiedAuditLog ; Search-AdminAuditLog retiré en 2024).
- **Message trace** — trajet des messages via Get-MessageTraceV2 (Get-MessageTrace déprécié depuis le 1er sept. 2025) ; 90 jours d'historique.

Opération	Signification / risque
MailItemsAccessed	Accès au contenu d'une boîte — pièce maîtresse en BEC (Premium/E5)
New-InboxRule / Set-InboxRule / UpdateInboxRules	Règle de boîte — transfert/masquage (exfiltration, réponse à phishing)
Set-Mailbox (ForwardingSmtpAddress)	Transfert externe silencieux
Add-MailboxPermission (FullAccess)	Accès délégué à une boîte tierce
Send / SendAs / SendOnBehalf	Envoi usurpé au nom d'un tiers
New-TransportRule	Règle de flux au niveau organisation

5.3 SharePoint / OneDrive / Teams — opérations à surveiller

Opération	Signal
FileDownloaded / FileSyncDownloadedFull	Téléchargement en masse — exfiltration
AnonymousLinkCreated / AnonymousLinkUsed	Partage public — fuite de données
SharingInvitationCreated / CompanyLinkCreated	Partage externe / à l'échelle de l'org
SearchQueryPerformed	Reconnaissance de contenu sensible
MemberAdded (Teams) / BotAddedToTeam	Ajout non autorisé, bot malveillant

5.4 Defender XDR — catalogue d'Advanced Hunting

Les produits Defender écrivent dans un schéma KQL unifié interrogeable dans le portail Defender. Principales familles de tables :

Famille	Tables (KQL)
Endpoint	DeviceLogonEvents, DeviceProcessEvents, DeviceNetworkEvents, DeviceFileEvents, DeviceRegistryEvents, DeviceImageLoadEvents, DeviceEvents
Email (MDO)	EmailEvents, EmailAttachmentInfo, EmailUrlInfo, EmailPostDeliveryEvents, UrlClickEvents
Identity (MDI)	IdentityLogonEvents, IdentityQueryEvents, IdentityDirectoryEvents, IdentityInfo
Cloud Apps (MDCA)	CloudAppEvents
Alertes / comportements	AlertInfo, AlertEvidence, BehaviorInfo, BehaviorEntities
Entra (via connecteur)	AADSignInEventsBeta, AADSpnSignInEventsBeta

Prérequis — une table ne renvoie des résultats que si son service est déployé :
 IdentityDirectoryEvents/QueryEvents dépendent de Defender for Identity sur vos DC ; les tables Device* de l'onboarding Defender for Endpoint.

5.5 Rétention Purview (Standard vs Premium)

	Audit (Standard)	Audit (Premium)
Rétention défaut	180 jours	1 an (Entra, Exchange, OneDrive, SharePoint) · 180 j sinon
Rétention max	180 jours	10 ans (add-on dédié requis)
Licence	M365 / O365 (défaut)	E5 / E5 Compliance / add-on
Politiques personnalisées	Non	Oui (service / activité / utilisateur)

Historique : le défaut Standard est passé de 90 à **180 jours** pour les enregistrements générés depuis le 17 octobre 2023.

5.6 Accéder au UAL — méthodes et limites

Méthode	Limites	Usage
Portail Purview — Audit search	Asynchrone, UI	Investigations ponctuelles, export CSV
Search-UnifiedAuditLog	Synchrone, 50 000 max (5 000/page)	Scripts, filtrage RecordType/Operation
AuditLogQuery (Graph API)	Async, 10 jobs, résultats 30 j	Gros volumes (>50 000), automatisation
Management Activity API	App-only, abonnements + blobs	Collecte temps réel (SIEM, LogGUARD)

6. Architecture de collecte & rétention

Les fenêtres natives sont courtes. Pour investiguer un incident découvert plusieurs jours après coup, il faut exporter les journaux avant qu'ils n'expirent. La collecte se pilote par diagnostic settings vers trois destinations.



Figure 8 — Router les journaux vers Log Analytics, Storage ou Event Hub.

- **Log Analytics** — requêtes KQL, alertes, workbooks, base de Microsoft Sentinel. Le choix par défaut pour la détection.
- **Azure Storage** — archive longue durée à faible coût (conformité, immuabilité).
- **Event Hub** — streaming vers un SIEM tiers (Splunk, QRadar...).

6.1 Matrice de rétention consolidée

Source	Défaut	Pour aller plus loin
AD Security (on-prem)	Taille du journal	WEF/WEC → SIEM ; MDI
Entra Audit / Sign-ins	7 j (Free) · 30 j (P1/P2)	Diagnostic settings → LA/Storage
Graph activity logs	0 j (export requis)	Diagnostic settings (P1/P2)
UAL (Purview Standard)	180 jours	Purview Premium (1 an)
UAL (Purview Premium)	1 an	Add-on 10 ans + politique custom

7. Cartographie MITRE ATT&CK → source de log

Pour chaque tactique adverse, la (ou les) source(s) où trouver la trace. C'est la grille de lecture qui transforme une alerte en investigation dirigée.

Tactique	Technique (exemple)	Source de log
Reconnaissance	Énumération AD (BloodHound)	IdentityQueryEvents · LDAP 1644 · 4662
Initial Access	Phishing, valid accounts	Entra Sign-ins · EmailEvents · UrlClickEvents
Credential Access	Password spray, Kerberoasting	4625/4771 · 4769 (RC4) · riskDetections (passwordSpray)
Persistence	Règle de transfert, app OAuth, certificat	New-InboxRule · Audit (Consent) · AD CS 4887
Privilege Escalation	Ajout à un rôle/groupe admin	4728/4732 · AuditLogs (Add member to role)
Defense Evasion	Effacement de journaux, AuditBypass	1102 · Set-Mailbox (AuditBypassEnabled)
Lateral Movement	Pass-the-hash, RDP, DCSync	4624 (type 9/10) · 4662 (réplication) · DeviceLogonEvents
Collection / Exfiltration	Accès boîte, download massif	MailItemsAccessed · FileDownloaded · Graph activity
Command & Control	Beaconing, DNS tunneling	DeviceNetworkEvents · Sysmon 3/22

8. Playbooks d'investigation

8.1 Compte compromis

- Sign-ins Entra : localisation/IP inhabituelle, MFA contourné (conditionalAccessStatus), connexions non-interactives anormales.
- Identity Protection : détections (unlikelyTravel, anonymizedIPAddress, leakedCredentials).
- Audit Entra : ajout de méthode MFA, création de secret d'app, consentement.
- UAL / Exchange : New-InboxRule (transfert), MailItemsAccessed (contenu consulté).

8.2 Consentement d'application illicite (OAuth)

- Audit Entra : « Consent to application » / « Add delegated permission grant » ; portées demandées.
- Sign-ins service principal + Graph activity : première activité de l'app, volume d'appels.
- UAL : accès aux données consécutifs via l'app (mail, fichiers).

8.3 Password spray

- Entra : rafales d'errorCode 50126/50053, nombreux UPN, même IP/ASN ; riskDetection passwordSpray.
- AD : 4625/4771 multi-comptes depuis une IP ; 4740 (verrouillages).

8.4 Exfiltration de données

- SharePoint/OneDrive : FileDownloaded en masse, AnonymousLinkCreated, partage externe.
- Exchange : règles de transfert, Get-MessageTraceV2 vers domaines externes, MailItemsAccessed.
- Graph activity logs : volume anormal de lectures via une application.

8.5 Escalade & mouvement latéral

- AD : 4728/4732/4756 (groupe privilégié), 4672, 4624 LogonType 9/10, 4662 (DCSync).
- Entra : « Add member to role » (rôles admin), activation PIM inattendue.

9. Boîte à outils KQL & PowerShell

9.1 KQL (Log Analytics / Sentinel / Defender)

```
// Password spray : échecs groupés par IP
SigninLogs
| where TimeGenerated > ago(24h) and ResultType != 0
| summarize tentatives=count(), comptes=dcount(UserPrincipalName) by IPAddress
| where comptes > 10 | order by tentatives desc

// Attributions de rôles privilégiés
AuditLogs
| where OperationName == "Add member to role"
| project TimeGenerated, InitiatedBy, TargetResources, Result

// Accès au contenu des boîtes (BEC) – nécessite Audit Premium
OfficeActivity
| where Operation == "MailItemsAccessed" and ClientIPAddress != ""
| summarize count() by UserId, ClientIPAddress

// Reconnaissance AD (Defender for Identity)
IdentityQueryEvents
| where Timestamp > ago(7d) and QueryType == "EnumerateUsers"
| summarize count() by AccountUpn, DeviceName
```

9.2 PowerShell (Exchange / Purview)

```
# Recherche synchrone dans le UAL (<= 50 000 enregistrements)
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) `
  -Operations New-InboxRule,Set-Mailbox -ResultSize 5000 -SessionCommand ReturnLargeSet

# Gros volumes : API Graph AuditLogQuery (asynchrone)
New-MgBetaSecurityAuditLogQuery -DisplayName "IR-consent" `
  -FilterStartDateTime (Get-Date).AddDays(-30) -FilterEndDateTime (Get-Date)
Get-MgBetaSecurityAuditLogQueryRecord -AuditLogQueryId $id

# Trajet des messages (Get-MessageTrace deprecie -> V2)
Get-MessageTraceV2 -StartDate (Get-Date).AddDays(-2) -EndDate (Get-Date) |
  Where-Object { $_.RecipientAddress -notlike "*@contoso.com" }
```

10. Pièges & bonnes pratiques

- **Deux horloges.** Rétention Entra ≠ rétention UAL. Vérifiez les deux, séparément.
- **Exporter tôt.** Un incident découvert à J+9 a déjà perdu les premiers jours en P1/P2 sans export.
- **Graph activity logs = 0 par défaut.** Configurez le diagnostic setting avant d'en avoir besoin.
- **SACL obligatoires.** Pas d'audit DS Access (4662) sans SAcl posées.
- **MailItemsAccessed = Premium.** Sans Audit Premium/E5, l'accès au contenu des boîtes n'est pas journalisé.
- **Migrer les scripts.** Get-MessageTrace → Get-MessageTraceV2 ; gros exports → AuditLogQuery.
- **Ne pas jeter le non-interactif.** C'est souvent là que se cache le rejeu de jeton.
- **1102 = alerte rouge.** Effacement du journal de sécurité : anti-forensique.
- **Corréler par correlationId.** Recollez connexion, Conditional Access et audit d'une même opération.

Annexe A — Champs pivots par journal

Journal	Champs à extraire en priorité
Windows Security (4624/4625)	TargetUserName, LogonType, IpAddress, WorkstationName, LogonProcessName
Kerberos (4768/4769)	TicketEncryptionType, ServiceName (SPN), Status, ClientAddress
Entra Sign-in	userPrincipalName, appDisplayName, ipAddress, status.errorCode, conditionalAccessStatus, correlationId
Entra Audit	activityDisplayName, initiatedBy, targetResources, result, correlationId
UAL (Office)	CreationTime, Operation, RecordType, UserId, ClientIP, ObjectId
Graph activity	requestUri, requestMethod, responseStatusCode, appId, ipAddress
EmailEvents (MDO)	SenderFromAddress, RecipientEmailAddress, NetworkMessageId, ThreatTypes

Annexe B — Glossaire & sources

Terme	Définition
UAL	Unified Audit Log — journal d'audit unifié Microsoft 365 (Purview).
MDI / MDCA	Defender for Identity (DC on-prem) / Defender for Cloud Apps.
SACL	System Access Control List — déclenche l'audit d'accès aux objets AD.
SPN	Service Principal Name — cible d'un ticket Kerberos (4769).
correlationId	Identifiant reliant les événements d'une même opération Entra.
AuditLogQuery	API Graph asynchrone de recherche d'audit (remplace à terme Search-UnifiedAuditLog pour les gros volumes).
KQL	Kusto Query Language — langage de requête Azure Monitor / Defender.

Sources (Microsoft Learn)

- Microsoft Entra data retention — [reference-reports-data-retention](#).
- Manage audit log retention policies / Auditing solutions — [purview/audit-*](#).
- Microsoft Graph activity logs overview — [graph/microsoft-graph-activity-logs-overview](#).
- Advanced hunting schema (Identity/Device/Email tables) — [defender-xdr/advanced-hunting-*](#).
- Get-MessageTraceV2 & AuditLogQuery API — [powershell/module/exchange](#) ; [graph/api/security-auditlogquery](#).

© Frédéric PEREZ — Guide de référence « Les logs Microsoft ». Faits volatils vérifiés en 2026 ; recouper avant tout audit formel.