RECEVOIR VOTRE PISTE D'AUDIT DANS

Amazon S3

Recevez la piste d'audit REVIEWIT sous forme d'objets dans un bucket Amazon S3 — ou dans un stockage objet compatible S3 de votre réseau (StorageGRID, MinIO…) : lots et manifestes adjacents, signés dans les métadonnées d'objet, vérifiables au repos.

VERSION
1.0 · Octobre 2026

DURÉE
Vingt minutes, en trois étapes

DIFFUSION
Confidentiel · Clients REVIEWIT

CE QU'IL VOUS FAUT

01 **Un administrateur AWS** capable de créer un bucket et un utilisateur IAM à une seule permission — ou, pour un stockage compatible S3, l'exploitant de ce stockage, capable de créer un bucket et une clé d'accès limitée à l'écriture dedans.

02 **Un administrateur de la souscription** REVIEWIT. Créer, activer et remplacer un identifiant exigent une authentification forte de moins de dix minutes : la console vous envoie chez votre fournisseur d'identité et vous ramène.

03 **L'ordre de ce guide** : d'abord la cible chez vous, puis la destination dans REVIEWIT, puis le test. Rien n'est livré avant qu'une écriture réelle sous vos identifiants ait réussi.

LE PARCOURS, EN TROIS ÉTAPES

ÉTAPE 1

Préparer la cible

Créer le point de réception et l'identifiant que REVIEWIT utilisera — droits minimaux, rien de plus.

ÉTAPE 2

Déclarer la destination

Quatre écrans dans le Subscription Manager : cible, résidence, contenu, récapitulatif.

ÉTAPE 3

Tester, puis activer

Une écriture de sonde sous vos identifiants ; un refus dit pourquoi. La livraison commence dans la minute.

DANS CE GUIDE

1 Comment BEACON livre votre piste d'audit

2 Ce que vous recevez

3 Préparer la cible chez Amazon S3

4 Déclarer la destination dans REVIEWIT

5 Tester et activer

6 Vérifier hors ligne avec beacon-verify

7 Exploiter

8 Dépannage et liste de contrôle

01 Comment BEACON livre votre piste d'audit

BEACON est le canal de diffusion de la piste d'audit REVIEWIT. Il ne produit pas la preuve et ne possède pas les événements : **la piste d'audit prouve, REVIEWIT SEAL scelle, BEACON livre.** Chaque événement d'audit devient un maillon — un rang strictement croissant, le SHA-256 de l'enregistrement, l'empreinte du maillon précédent et l'enregistrement original verbatim — et la tête de chaque chaîne est signée par l'autorité de scellement. Ce qui arrive chez vous est une chaîne que vous recalculez et un sceau que vous contrôlez, sans jamais rappeler REVIEWIT.

VOTRE RÉGION

Piste d'audit

Événements chaînés par domaine et classe de rétention, scellés toutes les heures par REVIEWIT SEAL.

→

VOTRE RÉGION

BEACON

Une passe par minute : des lots de 500 événements ou 5 Mo au plus, un manifeste par lot, un battement toutes les 15 minutes.

→

CHEZ VOUS

Amazon S3

Votre bucket : deux objets par lot (données, puis manifeste), un objet de battement, un objet de sonde — sous des clés d'accès qui ne savent qu'écrire.

PRINCIPE DIRECTEUR

Rien n'est perdu et rien n'est prétendu. La livraison avance chaîne par chaîne, sur un acquittement strict seulement ; un échec reprend exactement où il s'est arrêté ; après douze tentatives, la destination est mise en pause et une alerte est levée. Une purge de rétention est livrée comme une coupe signée, un filtre laisse des jalons qui gardent la chaîne vérifiable, et le silence est couvert par le battement : jamais de trou non signé.

PRIS EN CHARGE PAR

La carte **Amazon S3** de l'assistant de destination (profil stockage objet). Deux formes de cible : la forme virtual-host régionale d'AWS, `https://{bucket}.s3.{région}.amazonaws.com`, où REVIEWIT **observe** la région et attend le compte propriétaire ; et, depuis octobre 2026, un **stockage compatible S3 de votre réseau**, `https://{hôte}[:8088]/{bucket}` (adressage par chemin), où la résidence est **déclarée**. Les clés d'accès sont confiées une fois et scellées sous garde REVIEWIT SEAL. C'est le seul transport où la signature HMAC de transport reste vérifiable au repos.

02 Ce que vous recevez

Trois sortes d'enregistrements voyagent vers votre cible, toutes en JSON UTF-8 dont l'ordre des propriétés est le contrat. Un **maillon** est un événement d'audit : `metadata.uid` (l'identifiant stable de l'événement), `reviewit.chain` (clé, genèse), `reviewit.integrity` (`sequence`, `previous_hash`, `hash`, `raw_data`). Un **manifeste** clôt chaque lot : chaîne, plage, empreintes d'entrée et de sortie, décomptes, `batch_id`, et la référence du dernier sceau de la chaîne. Un **battement** porte, toutes les 15 minutes, la tête et la position acquittée de chaque chaîne.

ENREGISTREMENT	OÙ IL ARRIVE	À QUOI IL SERT
`{from}-{to}-{batch_id}.ndjson.gz`	`beacon/{souscription}/{destination}/{classe}/g{génération}/{chaîne}/` — `from` et `to` sur 20 chiffres	Les maillons, NDJSON gzippé, le manifeste en dernière ligne
`….manifest.json`	La même clé, suffixée ; écrit **après** l'objet de données	La ligne `{"reviewit_manifest/v1":{…}}` — un lot n'est livré que lorsque cet objet existe
`heartbeat.json`	`beacon/{souscription}/{destination}/`, réécrit toutes les 15 minutes	L'état de chaque chaîne — alertez sur son absence
`probe.json`	Même préfixe ; à la création, à chaque test et à l'activation	L'écriture de sonde qui prouve le bucket, les clés et le propriétaire

INGÉREZ SUR LE MANIFESTE, JAMAIS SUR L'OBJET DE DONNÉES SEUL

Un objet de données sans manifeste adjacent est un lot en cours ou échoué : ne l'ingérez jamais. Un lot réessayé est réécrit à l'identique sous la même clé ; un lot replanifié sur une plage plus large laisse l'objet de données précédent orphelin — une règle de cycle de vie peut purger les objets `.ndjson.gz` sans manifeste après quelques jours. Les clés ne portent pas de date : elles sont ordonnées par chaîne et par rang. REVIEWIT ne supprime jamais rien : les objets sont à vous, votre politique de cycle de vie s'applique.

AU MOINS UNE FOIS, DÉDOUBLONNÉ PAR VOUS

Après un doute réseau, le même lot peut être présenté de nouveau, avec le même `batch_id` et les mêmes identifiants d'événements. Dédoublonnez sur `metadata.uid`, et ordonnez entre chaînes par l'heure de l'occurrence. Un enregistrement qui n'arrive jamais est un trou que votre SIEM peut voir : chaque maillon est numéroté, et le battement dit où se tient la tête.

LE PULL, MÊME CONTRAT

Votre SIEM peut aussi lire la piste lui-même par l'API publique REVIEWIT, sous la portée `audit.read` : `GET /api/v1/audit/chains` liste les chaînes de votre souscription avec leur curseur de départ, `GET /api/v1/audit/stream?cursor=…&limit=500&manifest=true` rend les mêmes maillons et les mêmes manifestes que le push. Push et pull se vérifient avec le même outil.

03 Préparer la cible chez Amazon S3

Un administrateur prépare le bucket et un identifiant qui ne sait **qu'écrire sous le préfixe** `beacon/`. Rien d'autre : REVIEWIT ne lit rien, ne liste rien, ne supprime rien ; sur AWS la région s'observe sans clé.

01 Amazon S3 : le bucket

Un nom **sans point** (la forme virtual-host est la seule admise sur AWS, et un point casse la validation TLS que REVIEWIT ne désactive jamais), dans la région voulue. Chiffrement par défaut activé (SSE-S3 ou SSE-KMS) : REVIEWIT n'envoie aucun en-tête de chiffrement, la politique du bucket s'applique. Écrasement autorisé : une re-livraison réécrit la même clé — une politique qui impose des écritures conditionnelles ferait échouer les re-livraisons ; le versioning est compatible.

02 Amazon S3 : l'utilisateur IAM et sa politique

Un utilisateur IAM dédié avec la seule déclaration ci-dessous — `s3:PutObject` sur `arn:aws:s3:::<bucket>/beacon/*`. Créez-lui une paire de clés d'accès ; notez l'**identifiant de compte à 12 chiffres** propriétaire du bucket : chaque écriture porte `x-amz-expected-bucket-owner`, pour qu'un nom de bucket repris un jour par un autre compte refuse l'écriture au lieu d'y recevoir votre piste.

03 Stockage compatible S3 de votre réseau

StorageGRID, MinIO, Ceph RGW ou tout stockage exposant l'API S3 en HTTPS sur **443 ou 8088**, adressé **par chemin** : `https://<hôte>[:8088]/<bucket>`. Le certificat est celui de l'hôte, le nom du bucket peut donc porter des points. Créez le bucket et une clé d'accès limitée à l'écriture dedans ; la signature se fait sous la région conventionnelle `us-east-1`. Aucun compte propriétaire n'est attendu ; la résidence est celle que vous déclarez. Un hôte AWS ne s'écrit jamais sous cette forme.

04 Gardez les clés pour l'assistant seul

L'identifiant de clé d'accès et le secret se saisissent une fois dans REVIEWIT (section 4). REVIEWIT écrit `probe.json` sous ces clés avant de les confier : si l'écriture échoue — clé sans droit, mauvais compte propriétaire — rien n'est créé ni confié.

POLITIQUE IAM DE L'UTILISATEUR DÉDIÉ (AMAZON S3)

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::<bucket>/beacon/*"
  }]
}
```

CE QUE VOUS SAISIREZ DANS L'ASSISTANT

CHAMP DE L'ASSISTANT	VALEUR
Transport	**Amazon S3** (stockage objet)
Nom	Comment la destination se lira dans votre liste — « Archive S3 — conformité ».
URL de la cible	AWS : `https://<bucket>.s3.<région>.amazonaws.com` (pas de point dans le nom, la région est observée). Compatible S3 : `https://<hôte>[:8088]/<bucket>` (vous déclarez alors la géographie).
Compte propriétaire du bucket	AWS seulement : l'identifiant de compte à 12 chiffres propriétaire du bucket.
Identifiant de la clé d'accès · Clé d'accès secrète	La paire de clés dédiée. Testée par une écriture de sonde avant d'être retenue.
Géographie de la cible	AWS : observée depuis la région réelle du bucket, affichée « Bucket observé en … — géographies : … ». Compatible S3 : déclarée.

04 Déclarer la destination dans REVIEWIT

Subscription Manager › **Paramètres** › **Intégrations & IA** › **BEACON** › **Nouvelle destination**. L'assistant a quatre écrans ; rien n'est créé avant le dernier, et la cible est contrôlée par la garde d'egress avant que la destination existe.

01 Cible

Nommez la destination, choisissez la carte **Amazon S3**, saisissez l'URL de la cible et l'identifiant de la section 3. L'identifiant est ouvert en mémoire pour ce seul geste, puis scellé sous garde REVIEWIT SEAL : l'écran ne le montre plus jamais.

02 Résidence

Sur AWS la région est **observée** : un bucket à Paris est en France et en Europe, et l'écran dit si elle est dans la géographie de votre souscription. Hors de celle-ci, une reconnaissance avec justification écrite est exigée et consignée dans la piste d'audit. Sur un stockage compatible S3 rien ne s'observe : vous **déclarez** où il se trouve, et la même règle s'applique.

03 Contenu

Départ : depuis le début de chaque chaîne (historique complet) ou depuis l'activation (seulement ce qui suit). **Événements envoyés en clair** : laissez vide pour le flux complet. Un filtre remplace chaque événement écarté par un jalon — rang et empreintes, aucune donnée métier — et la preuve scellée s'arrête au premier jalon ; l'écran le dit avant que vous confirmiez.

04 Récapitulatif

Relisez, puis cliquez **Créer**. La garde d'egress juge d'abord la cible : HTTPS seulement, aucun identifiant dans l'URL, port 443 ou 8088, un hôte routable publiquement. Une cible refusée nomme le contrôle fautif ; rien n'est créé.

LA GARDE D'EGRESS, AVANT CHAQUE ENVOI

Chaque cible passe les mêmes sept contrôles à la création, à chaque test et avant chaque livraison : URL valide · HTTPS · aucun identifiant dans l'URL · port 443 ou 8088 · aucune zone interne REVIEWIT · l'hôte se résout · l'hôte n'est pas une adresse privée ou réservée. Les redirections ne sont jamais suivies, et la vérification TLS n'est jamais désactivée.

05 Tester et activer

Une destination n'est activée qu'après une écriture réelle sous vos identifiants. Ouvrez le panneau de la destination et cliquez **Tester la cible** : REVIEWIT écrit un enregistrement de sonde (`probe.json` sous vos clés). « La cible passe la garde d'egress » signifie que l'hôte, l'identifiant et ses droits sont prouvés. Un refus dit sa cause — jamais le secret.

01 Tester la cible

REVIEWIT écrit `probe.json` sous les clés d'accès, avec le compte propriétaire attendu sur AWS. « La cible passe la garde d'egress » signifie que le bucket, les clés et le propriétaire sont prouvés. Un refus nomme sa cause : « le bucket refuse cette destination » — clé sans `s3:PutObject` sur le préfixe `beacon/`, mauvais compte propriétaire, nom de bucket avec un point, ou URL par chemin sur un hôte AWS.

02 Activer

Depuis le panneau, **Activer** (ou cochez « Activer dès la création » dans l'assistant). La livraison commence à la passe suivante, dans la minute ; le premier battement suit.

03 Lire le panneau

Par chaîne : le point de reprise acquitté, l'âge du plus ancien événement non livré, la marge avant la prochaine coupe de rétention, le dernier sceau et ce qui est au-delà. L'historique des lots liste chaque manifeste ; le journal du canal liste chaque geste d'administration avec son code d'audit.

06 Vérifier hors ligne avec beacon-verify

`beacon-verify` est un outil en ligne de commande, distribué avec sa spécification publique. Il lit ce que votre cible a reçu et le trousseau que REVIEWIT publie à `/.well-known/seal-keyring.json`, ancré sur l'empreinte de la clé racine imprimée dans l'annexe sécurité de votre contrat, et rend un verdict par chaîne et par plage — sans réseau et sans appel à REVIEWIT.

THE COMMAND

```
beacon-verify <export> --keys seal-keyring.json --root <empreinte racine> --namespace <v
otre espace de scellement>
```

Votre **espace de scellement** est affiché dans le panneau de la destination (`t-` suivi de 26 caractères). Passez-le avec `--namespace` : un sceau d'un autre espace est, pour vous, une rupture. Sans `--root` ni `--namespace`, les plages sont rendues scellées *sous réserve*.

01 Rassembler les objets d'une chaîne

Téléchargez, depuis le préfixe de la chaîne, les objets de données `.ndjson.gz` dont le `.manifest.json` existe, plus les manifestes. Un dossier est lu en entier : `beacon-verify <dossier>`. Ne décompressez ni ne resérialisez jamais : le vérificateur lit aussi bien le gzip (1F 8B) que le NDJSON en clair.

02 Lancer le vérificateur

`beacon-verify ./export-beacon --keys seal-keyring.json --root <racine> --namespace <t-…>`. Code 0 quand tout ce qui précède le dernier sceau est scellé ; 3 quand une chaîne n'a pas encore de sceau sous votre espace.

03 Vérifier une signature de transport au repos

S3 est le seul transport qui garde les octets signés. Chaque objet porte `x-amz-meta-beacon-batch-id`, `-sequence-range`, `-timestamp` et `-signature` (`v1=base64(HMAC-SHA256(secret, "{timestamp}.{batch_id|heartbeat}.{sha256 hex minuscule de l'objet}"))`). `beacon-verify hmac <objet> --timestamp <secondes> --subject <batch_id|heartbeat> --signature <v1=…>`, avec le secret dans la variable d'environnement `BEACON_HMAC_SECRET`, jamais en argument. Pendant une rotation ouverte, la métadonnée porte deux signatures, `v1=neuve,v1=ancienne` : acceptez l'objet si l'une des deux se vérifie.

VERDICT	SIGNIFICATION
`SCELLÉ`	Chaîné jusqu'à une tête dont la signature est valide, trousseau ancré, espace épinglé.
`SCELLÉ SOUS RÉSERVE`	Idem, mais la racine ou l'espace n'ont pas été épinglés sur la ligne de commande.
`CHAÎNAGE SEUL`	Intact, au-delà du dernier sceau ou derrière un jalon — le prochain sceau le couvrira.
`NON VÉRIFIABLE`	Un sceau sans espace, un algorithme inconnu ou une clé absente du trousseau — jamais dit faux.
`ROMPU`	Une empreinte fausse, un trou, un doublon divergent, une signature invalide ou un espace étranger — avec la cause et le rang.

Codes de sortie : **0** rien de rompu et tout ce qui précède le dernier sceau est scellé · **1** une rupture ou un espace étranger · **2** entrée inexploitable (une propriété JSON en double, une valeur à la fois brute et enveloppée, un enregistrement tronqué à l'indexation) · **3** rien de rompu, preuve incomplète.

07 Exploiter

Chaque geste sur une destination est posé par un administrateur de la souscription, tracé dans la piste d'audit sous son nom, et les gestes sensibles exigent une authentification forte de moins de dix minutes. Le canal qui exporte la piste est lui-même sous la piste.

Faire tourner les clés d'accès	Créez la nouvelle paire de clés, puis panneau › **Remplacer les clés d'accès** : les clés neuves doivent réussir une écriture de sonde avant d'être retenues. Désactivez ensuite l'ancienne paire de votre côté. Le secret HMAC tourne à part — **Faire tourner le secret** montre la nouvelle valeur une fois, les deux signent jusqu'à **Clôturer la rotation**.
Pause pour échecs	Un refus persistant — identifiant révoqué, droit retiré, cible disparue — met la destination en pause après douze tentatives et lève une alerte dans le Centre d'alertes. Rien n'est perdu : la reprise repart du point de reprise acquitté de chaque chaîne, automatiquement quand la sonde horaire revoit la cible, ou par **Reprendre**.
Changer de cible	**Modifier** › nouvelle URL, même forme. Un bucket ne se change pas en place : créez une nouvelle destination pour un nouveau bucket, désactivez l'ancienne.
Retirer	**Désactiver**, puis supprimer ou archiver. Une destination qui a livré est archivée, jamais supprimée : ses manifestes sont des preuves de livraison. Révoquez ensuite l'identifiant de votre côté : il ne sert plus à rien.

08 Dépannage

CE QUE VOUS VOYEZ	CAUSE	CE QU'IL FAUT FAIRE
« Le bucket refuse cette destination » à la création	Pas de `s3:PutObject` sur `beacon/*`, mauvais compte propriétaire, ou un nom de bucket avec un point	Corrigez la politique ou l'identifiant de compte ; renommez le bucket sans point ; réessayez — rien n'a été créé.
URL de la cible refusée sur un stockage compatible S3	Un port autre que 443 ou 8088, plus d'un segment de chemin, ou un hôte AWS écrit par chemin	Utilisez `https://<hôte>[:8088]/<bucket>` ; les buckets AWS utilisent la forme virtual-host.
La garde d'egress refuse : « L'hôte se résout en adresse privée ou réservée »	Le stockage n'est joignable que sur votre réseau privé	Dans l'offre cloud, exposez-le sur une adresse publique ; sur une installation REVIEWIT sur site, déclarez le réseau privé à la garde d'egress de l'installation.
Des objets de données sans manifeste s'accumulent	Lots replanifiés sur une plage plus large entre deux tentatives	Normal ; ingérez sur le manifeste seulement ; une règle de cycle de vie peut purger les orphelins après quelques jours.
Géographie affichée hors de celle de la souscription	La région réelle du bucket est ailleurs	Reconnaissez avec une justification (tracée), ou créez le bucket dans la bonne région.
Destination en pause, « après échecs »	Clés désactivées, politique changée, politique de bucket imposant des écritures conditionnelles	Corrigez côté stockage, **Tester la cible**, puis **Reprendre**. Rien n'a été perdu.

Liste de contrôle avant de commencer

7 POINTS

- [ ] AWS : un bucket sans point, chiffrement activé, écrasement autorisé ; ou un stockage compatible S3 en 443 ou 8088
- [ ] Un utilisateur ou une clé dédiés, limités à l'écriture sous `beacon/`
- [ ] AWS : l'identifiant de compte propriétaire à 12 chiffres
- [ ] L'identifiant de clé d'accès et le secret, utilisés seulement dans l'assistant
- [ ] La géographie du bucket et sa justification si elle diffère de celle de votre souscription
- [ ] Un administrateur de la souscription avec son second facteur prêt
- [ ] L'empreinte racine de l'annexe de votre contrat, pour beacon-verify

Ce guide est fourni aux clients REVIEWIT qui raccordent leur SIEM ou leur stockage à BEACON. Les chemins de menus sont ceux des consoles des éditeurs à la date de publication ; ils peuvent évoluer. En cas d'écart, le support REVIEWIT vous accompagne.