AYI NEDJIMI Consultants

Cloud Forensics : Guide Investigation Incident Cloud 2026

Catégorie : Cloud Security Lecture : 9 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Méthodologie investigation forensique cloud : préservation preuves, collecte CloudTrail Activity Log, analyse timeline et reconstruction chaîne.

L'investigation forensique dans les environnements cloud représente un défi méthodologique considérable pour les équipes de réponse aux incidents. Les principes fondamentaux de la forensique numérique, la préservation de l'intégrité des preuves, la documentation de la chaîne de custody et l'analyse systématique des artefacts, restent applicables mais les techniques d'implémentation diffèrent radicalement de la forensique traditionnelle sur serveurs physiques. L'absence d'accès physique aux supports de stockage, l'éphéméralité des instances cloud, la distribution géographique des données et la dépendance aux logs fournis par le provider créent un paradigme d'investigation entièrement nouveau. En 2026, la fréquence des incidents de sécurité cloud impose aux équipes DFIR de maîtriser les spécificités forensiques de chaque cloud provider. Ce guide présente une méthodologie structurée d'investigation forensique cloud, couvrant la préparation, la préservation, la collecte, l'analyse et le reporting, avec des procédures détaillées pour AWS et Azure et des références pour GCP.

Résumé exécutif

Méthodologie d'investigation forensique cloud : préservation des preuves, collecte via APIs, analyse des timelines CloudTrail et Activity Log, investigation d'incidents spécifiques et rapport forensique adapté au cloud.

Retour d'expérience : lors de la réponse à un incident de compromission d'un environnement AWS hébergeant une application critique, nous avons identifié que l'attaquant avait utilisé des credentials STS temporaires obtenus via une instance EC2 compromise pour créer une Lambda de persistance et exfiltrer des données S3 pendant 18 jours. La reconstruction complète de la timeline a nécessité la corrélation de CloudTrail, VPC Flow Logs, Lambda Execution Logs et S3 Access Logs sur une période de 30 jours, mobilisant deux analystes pendant cinq jours. La préservation proactive des logs avait été configurée en amont, ce qui a rendu l'investigation possible dans des délais acceptables. Face à la complexité croissante des environnements cloud hybrides et multi-cloud, les organisations doivent adopter des stratégies de sécurité adaptées aux spécificités de chaque fournisseur tout en maintenant une cohérence globale. Les équipes sécurité sont confrontées à des défis inédits : surfaces d'attaque dynamiques, configurations éphémères, gestion des identités à grande échelle et conformité réglementaire multi-juridictionnelle. Ce guide technique présente les approches éprouvées en environnement de production, les erreurs fréquentes à éviter et les stratégies de durcissement prioritaires. Chaque recommandation est issue de retours d'expérience concrets en entreprise et a été validée sur des architectures cloud de production à grande échelle.

Préparation forensique cloud : le fondement de l'investigation

La capacité d'investigation forensique se prépare **avant** l'incident. La configuration proactive du logging est la première priorité. Sur AWS, **CloudTrail** doit être activé en mode multi-région avec logging des événements de données pour S3 et Lambda, validation de l'intégrité des fichiers et envoi vers un bucket S3 dans un compte de sécurité séparé avec chiffrement KMS et politique de rétention de minimum 365 jours. Les **VPC Flow Logs** doivent être activés pour tous les VPC avec un format enrichi incluant les ports source et destination. *Amazon GuardDuty* fournit des findings de détection qui constituent souvent le point de départ de l'investigation.

Sur Azure, l'**Activity Log** doit être configuré avec une rétention étendue via l'envoi vers un workspace Log Analytics dédié à la sécurité. Les **Sign-in Logs** et **Audit Logs** d'Entra ID sont essentiels pour les investigations impliquant des compromissions d'identité. Les **NSG Flow Logs** avec Traffic Analytics fournissent la visibilité réseau. La configuration d'un *compte forensique* dédié avec des rôles d'accès pré-approuvés permet une réponse rapide sans retard lié aux processus d'habilitation. Consultez CIS Benchmarks pour les recommandations AWS sur la préparation forensique. Notre article sur Cloud Encryption Chiffrement Donnees Cles détaille les aspects complémentaires de la sécurité et du monitoring AWS.

Préservation et collecte des preuves cloud

La **préservation des preuves** dans le cloud doit être immédiate car les ressources cloud sont éphémères et peuvent être détruites par l'attaquant ou par des processus automatisés. Les **snapshots** des volumes EBS (AWS) ou des disques managés (Azure) capturent l'état du système de fichiers à un instant précis. Les **images mémoire** sont plus difficiles à obtenir dans le cloud, mais des outils comme *LiME* peuvent capturer la mémoire volatile des instances EC2 si un accès SSH ou SSM est disponible. Les **métadonnées d'instance** (tags, security groups, rôle IAM, adresse IP, date de création) doivent être documentées avant toute modification ou terminaison.

La collecte des logs via les **APIs cloud** est la méthode principale d'acquisition de preuves. Les outils `aws cli`, `az cli` et `gcloud` permettent l'extraction structurée des logs avec des filtres temporels et contextuels. Les *outils spécialisés* comme **CloudTrail Lake** (AWS), **Log Analytics KQL** (Azure) et **Invictus IR** facilitent les requêtes forensiques complexes. La **chaîne de custody** doit documenter chaque opération de collecte : qui a collecté quoi, quand, comment, et avec quelle intégrité vérifiable (hashes des fichiers collectés). Le stockage des preuves dans un bucket/container dédié avec chiffrement, versioning et politique d'immuabilité garantit leur intégrité pour une éventuelle utilisation judiciaire. Notre guide sur Kubernetes Offensif Rbac apporte des perspectives complémentaires sur la réponse aux incidents cloud. Consultez Google Cloud Security pour les fonctionnalités d'investigation d'Azure.

Analyse de la timeline et reconstruction de l'attaque

L'analyse forensique cloud repose principalement sur la **corrélation des logs** pour reconstruire la chronologie de l'attaque. La timeline commence par l'identification du *patient zéro* : le premier événement anormal qui marque le début de la compromission. Sur AWS, les événements

CloudTrail permettent de tracer chaque appel API avec le timestamp, l'identité de l'appelant, l'action effectuée, les paramètres et la réponse. La corrélation entre les **événements d'authentification** (ConsoleLogin, AssumeRole, GetSessionToken), les **événements de modification** (CreateUser, PutRolePolicy, RunInstances) et les **événements d'accès aux données** (GetObject, GetItem) reconstitue la chaîne d'attaque complète.

Les techniques d'analyse incluent la recherche d'**activité depuis des IP inconnues**, l'identification d'**actions inhabituelles** pour un utilisateur donné (analyse comportementale), la détection de **création de persistance** (nouveaux utilisateurs, rôles, clés d'accès, Lambda, règles EventBridge) et la recherche d'**exfiltration** (accès S3 volumétrique, copie de snapshots vers des comptes externes, transfert de données via des canaux non habituels). Les outils comme **aws-incident-response** de Mozilla et **Prowler** en mode forensique automatisent certaines de ces vérifications. La corrélation avec les findings GuardDuty ou Defender for Cloud contextualise les événements avec les indicateurs de menace détectés automatiquement. Notre article sur Cloud Network Security Vpc Waf Ddos explore les techniques avancées de détection applicables à la forensique cloud. Les ressources du ANSSI fournissent des informations complémentaires sur l'investigation dans GCP.

Source de preuves	AWS	Azure	Type d'information
API Logs	CloudTrail	Activity Log	Toutes les actions API avec contexte
Auth Logs	CloudTrail (console/API)	Sign-in Logs	Authentifications, MFA, localisation
Network Logs	VPC Flow Logs	NSG Flow Logs	Flux réseau source/destination/port
Storage Logs	S3 Access Logs	Storage Analytics	Accès aux données stockées
DNS Logs	Route 53 Resolver	DNS Analytics	Résolutions DNS (C2, exfiltration)
Threat Detection	GuardDuty	Defender Alerts	Findings de menaces détectées

Investigation de scénarios d'incidents cloud typiques

Les scénarios d'incidents cloud les plus fréquents suivent des patterns d'investigation spécifiques. La **compromission de credentials** est le scénario le plus courant : un attaquant obtient des clés d'accès IAM (via phishing, fuite de code, compromission d'une instance) et les utilise pour accéder aux ressources. L'investigation trace l'origine des credentials, les actions effectuées, les données accédées et les mécanismes de persistance mis en place. Le **cryptominage** se manifeste par la création d'instances EC2/VMs de grande taille dans des régions inhabituelles, souvent détecté par les alertes de coûts anormaux. L'**exfiltration de données** via S3/Blob Storage se détecte par l'analyse des volumes d'accès, les copies de snapshots vers des comptes externes et les modifications de bucket policies.

La **persistance** est la phase la plus critique à investiguer car elle détermine si l'attaquant conserve un accès après la remédiation initiale. Les mécanismes de persistance cloud incluent la création de nouveaux utilisateurs IAM, la génération de clés d'accès supplémentaires, la modification de rôles de confiance, le déploiement de fonctions Lambda déclenchées par des événements, la configuration de règles EventBridge et la mise en place de reverse proxies dans

des instances EC2. L'*éradication complète* nécessite l'identification et la suppression de tous ces mécanismes, suivie d'une rotation complète des credentials potentiellement compromis. Notre article sur Cloud Disaster Recovery Pra Resilience détaille les techniques de persistance et les méthodes de détection applicables au cloud.

Mon avis : la préparation forensique est l'investissement le plus sous-estimé en sécurité cloud. Trop d'organisations découvrent lors d'un incident que leurs logs sont insuffisants, mal configurés ou déjà expirés. Le coût de la configuration proactive du logging et de la rétention étendue est négligeable comparé au coût d'une investigation aveugle qui ne peut pas déterminer l'étendue de la compromission. Je recommande un exercice de simulation forensique annuel pour valider la couverture des logs et les procédures de collecte avant qu'un incident réel ne survienne.

Comment mener une investigation forensique dans le cloud ?

L'investigation forensique cloud suit une méthodologie en cinq phases adaptée des standards NIST et SANS. **Phase 1 : Identification et triage.** Analysez l'alerte initiale (GuardDuty finding, alerte de coûts, signalement utilisateur) pour déterminer la portée potentielle et la sévérité de l'incident. **Phase 2 : Préservation.** Créez des snapshots des instances suspectées, exportez les logs pertinents et documentez les métadonnées des ressources impliquées. Activez la rétention étendue des logs si ce n'est pas déjà fait. **Phase 3 : Collecte.** Extrayez les logs CloudTrail, VPC Flow Logs, Access Logs et findings de détection pour la période couvrant l'incident. Utilisez des requêtes ciblées basées sur les indicateurs initiaux (IP, identité, ressource). **Phase 4 : Analyse.** Construisez la timeline de l'attaque en corrélant les événements de toutes les sources, identifiez le point d'entrée initial, les mouvements latéraux, les actions sur les objectifs et les mécanismes de persistance. **Phase 5 : Rapport.** Documentez la chaîne d'attaque complète avec les preuves associées, les impacts identifiés et les recommandations de remédiation et de prévention. Notre article sur Oauth Oidc Abus Consent Securite fournit des outils complémentaires pour l'analyse forensique.

Pourquoi la forensique cloud diffère-t-elle de la forensique traditionnelle ?

La forensique cloud présente des différences fondamentales avec la forensique traditionnelle sur cinq axes. **L'accès physique** : impossible d'accéder aux disques durs physiques, à la mémoire vive des hyperviseurs ou aux logs système de l'infrastructure du provider. Toute la collecte passe par les APIs et les services du provider. **L'éphéméralité** : les instances auto-scaled, les conteneurs et les fonctions serverless peuvent être créés et détruits en quelques secondes, emportant les preuves avec eux si aucune préservation proactive n'est en place. **La distribution** : les données d'un seul incident peuvent être réparties sur plusieurs régions, comptes et services, nécessitant une collecte multi-sources coordonnée. **La dépendance au provider** : la qualité et la complétude des logs disponibles dépendent de la configuration du logging et des fonctionnalités offertes par le provider. **Les contraintes contractuelles** : l'accès aux données du provider (logs d'infrastructure, metadata d'hyperviseur) est limité par les

accords de niveau de service et les politiques de confidentialité. Ces différences imposent une méthodologie adaptée et des outils spécialisés que les analystes forensiques traditionnels doivent acquérir.

Quelles sont les sources de preuves disponibles sur AWS et Azure ?

Les sources de preuves cloud sont riches mais nécessitent une activation préalable et une configuration de rétention adéquate. Sur **AWS**, les sources principales sont CloudTrail (événements API avec identité, action, paramètres et réponse), VPC Flow Logs (flux réseau avec IP source/destination, ports et protocoles), S3 Access Logs (accès aux objets avec détail des opérations), GuardDuty Findings (détections de menaces automatisées), CloudWatch Logs (logs applicatifs et système), Route 53 Resolver Logs (requêtes DNS), Lambda Execution Logs (invocations et erreurs des fonctions), et ELB Access Logs (requêtes HTTP vers les load balancers). Sur **Azure**, les sources incluent Activity Log (opérations sur les ressources), Sign-in Logs et Audit Logs d'Entra ID (authentifications et modifications d'identité), NSG Flow Logs (trafic réseau), Defender for Cloud Alerts (détections de menaces), Storage Analytics (accès aux données), Azure Monitor (métriques et logs personnalisés), et Key Vault Audit Logs (accès aux secrets et clés). La corrélation de ces sources multiples est ce qui permet la reconstruction complète d'un incident et l'identification de tous les impacts.

À retenir : la forensique cloud repose sur la préparation proactive (logging complet avec rétention étendue), une méthodologie de collecte structurée via les APIs cloud, l'analyse de timelines corrélant multiple sources de logs et un processus d'éradication couvrant tous les mécanismes de persistance cloud. La simulation forensique annuelle valide la capacité d'investigation avant qu'un incident réel ne la mette à l'épreuve.

Seriez-vous capable de reconstruire la timeline complète d'un incident sur vos environnements cloud avec les logs actuellement configurés, ou des angles morts subsistent-ils ?

Sources et références : CISA · Cloud Security Alliance

Perspectives et prochaines étapes

L'évolution de la forensique cloud est portée par l'émergence de services natifs d'investigation (AWS Detective, Azure Sentinel Investigation) qui automatisent la corrélation et la visualisation des chaînes d'attaque. L'intégration de l'IA dans les outils forensiques accélère le triage initial et l'identification des patterns d'attaque connus. Les organisations doivent investir dans la formation de leurs analystes aux spécificités forensiques de chaque cloud provider et dans l'automatisation des procédures de préservation pour réduire le délai entre la détection et la première collecte de preuves, qui reste le facteur critique de succès de toute investigation.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr