AYI NEDJIMI Consultants

# Sécuriser une Architecture Multi-Cloud AWS et Azure

Catégorie : Cloud Security  Lecture : 8 min  Publié le : 03/03/2026  Auteur : Ayi NEDJIMI

*Guide complet pour sécuriser une architecture multi-cloud AWS et Azure : IAM fédéré, chiffrement, réseau, monitoring et bonnes pratiques avancées en.*


### Résumé exécutif

La migration vers le multi-cloud représente une opportunité stratégique mais aussi un défi sécuritaire majeur. Ce guide détaille les architectures de référence pour fédérer la sécurité entre AWS et Azure, en couvrant IAM, chiffrement, réseau et conformité.

Quand votre COMEX vous annonce un lundi matin que la stratégie cloud évolue vers du multi-cloud AWS plus Azure, la première réaction naturelle consiste à mesurer l'ampleur du chantier sécuritaire. Après avoir accompagné plus de quinze entreprises dans cette transition, je peux affirmer que la complexité ne réside pas dans la maîtrise individuelle de chaque fournisseur, mais bien dans l'orchestration cohérente des contrôles de sécurité à travers deux écosystèmes fondamentalement différents. Les équipes sécurité doivent repenser leur approche en abandonnant la vision silotée pour embrasser une gouvernance unifiée qui couvre la gestion des identités fédérées, le chiffrement de bout en bout, la segmentation réseau cross-cloud, le monitoring centralisé et la conformité réglementaire. Ce guide technique vous livre les clés architecturales et opérationnelles pour bâtir une posture de sécurité multi-cloud robuste, pragmatique et auditable, en se fondant sur des retours d'expérience terrain concrets et des configurations éprouvées en production depuis 2024.


## Pourquoi adopter une stratégie multi-cloud en 2026 ?

Le multi-cloud n'est plus un luxe réservé aux grands groupes. Les motivations sont multiples : **éviter le vendor lock-in**, optimiser les coûts par service, répondre à des exigences de souveraineté locale, ou encore exploiter les forces spécifiques de chaque provider. AWS excelle sur le compute et le machine learning avec SageMaker, tandis qu'Azure domine sur l'intégration Microsoft 365 et Active Directory. Cependant, cette diversification multiplie la surface d'attaque. Chaque provider dispose de son propre modèle de responsabilité partagée, de ses propres primitives IAM et de ses propres mécanismes de chiffrement. Sans gouvernance unifiée, les failles se nichent précisément aux jonctions entre les deux environnements.

Pour approfondir la gestion des identités cross-cloud, consultez notre article sur escalade de privilèges IAM cloud. Les principes d'escalade de privilèges diffèrent entre AWS et Azure, ce qui nécessite une vigilance accrue lors de la fédération.

**Mon avis :** Le multi-cloud ne se justifie que si votre organisation possède la maturité DevSecOps suffisante. Trop d'entreprises se lancent dans le multi-cloud par effet de mode sans disposer des compétences nécessaires pour sécuriser ne serait-ce qu'un seul cloud correctement.

L'approche pragmatique consiste à définir un modèle de gouvernance en trois couches. La couche stratégique établit les politiques de sécurité transverses applicables aux deux clouds : classification des données, gestion des identités, standards de chiffrement, exigences de conformité. La couche tactique traduit ces politiques en configurations techniques spécifiques à chaque provider, en exploitant les services natifs plutôt que de forcer une uniformité artificielle. La couche opérationnelle déploie et supervise ces configurations via des pipelines IaC unifiés et un monitoring centralisé. Cette séparation en couches permet de maintenir la cohérence stratégique tout en exploitant les forces spécifiques de chaque provider au niveau technique. Les organisations qui tentent de forcer une couche d'abstraction unique sur les deux clouds finissent invariablement par perdre la profondeur d'intégration native qui fait la valeur ajoutée de chaque plateforme, créant un nivellement par le bas sécuritaire plutôt qu'une synergie constructive entre les deux écosystèmes.

## Comment fédérer les identités IAM entre AWS et Azure ?

La *fédération d'identités* constitue le socle de toute architecture multi-cloud sécurisée. Le principe repose sur un Identity Provider central — typiquement Azure AD (rebaptisé Entra ID) — qui authentifie les utilisateurs et émet des tokens SAML ou OIDC consommés par AWS via des rôles IAM. Concrètement, on configure un Enterprise Application dans Azure AD avec AWS comme relying party, puis on mappe les groupes Azure AD vers des rôles AWS IAM via des claims SAML. Cette approche élimine la nécessité de gérer des credentials IAM long-terme dans AWS.

**Configuration critique** : dans AWS, le trust policy du rôle IAM doit spécifier explicitement le thumbprint du certificat Azure AD et limiter les conditions d'assomption via `aws:SourceIdentity` et `sts:RoleSessionName`. Côté Azure, activez le Conditional Access pour imposer le MFA et la conformité du device avant toute authentification fédérée.

| Composant | AWS | Azure | Recommandation |
|---|---|---|---|
| Identity Provider | IAM Identity Center | Entra ID | Centraliser sur Entra ID |
| MFA | Virtual MFA / FIDO2 | Authenticator / FIDO2 | FIDO2 partout |
| Privileged Access | IAM Roles + SCP | PIM + Conditional Access | Just-in-time des deux côtés |
| Audit | CloudTrail | Azure Activity Log | Centraliser dans SIEM |
| Secret Rotation | Secrets Manager | Key Vault | Rotation automatique 90j |

Pour comprendre les risques d'escalade de privilèges spécifiques à AWS, notre article sur escalades de privilèges AWS détaille les vecteurs d'attaque les plus courants exploités lors des pentests cloud.

## Chiffrement cross-cloud et gestion des clés

Le chiffrement en multi-cloud impose de trancher un dilemme architectural : utiliser les KMS natifs de chaque provider ou centraliser la gestion des clés via une solution tierce comme **HashiCorp Vault** ou **Thales CipherTrust**. L'approche hybride s'avère souvent la plus pragmatique : on utilise AWS KMS et Azure Key Vault pour le chiffrement at-rest natif des services managés (S3, RDS, Blob Storage, SQL Database), tout en centralisant les clés applicatives dans Vault pour les workloads qui communiquent entre les deux clouds.

Le chiffrement in-transit entre AWS et Azure s'appuie sur des tunnels IPsec via AWS VPN Gateway et Azure VPN Gateway, ou mieux, sur des interconnexions privées type AWS Direct Connect peered avec Azure ExpressRoute via un point de présence commun. Le protocole **MACsec** (IEEE 802.1AE) ajoute une couche de chiffrement au niveau 2 pour les connexions dédiées. Attention : les clés de chiffrement des tunnels VPN doivent être rotées automatiquement — AWS le fait par défaut toutes les heures, Azure nécessite une configuration explicite.

Concernant l'audit de vos configurations Terraform pour le chiffrement, référez-vous à notre guide sur audit Terraform compliance.

## Segmentation réseau multi-cloud

La segmentation réseau cross-cloud requiert une approche en couches. Au niveau macro, on interconnecte les VPC AWS et les VNet Azure via des solutions de transit : AWS Transit Gateway côté AWS, Azure Virtual WAN côté Azure, reliés entre eux par des tunnels VPN site-to-site ou des connexions privées. Au niveau micro, chaque workload est isolé dans son propre subnet avec des Security Groups (AWS) et des Network Security Groups (Azure) finement configurés.

**Le piège classique** : les équipes réseau créent des règles permissives pour "faire fonctionner" la communication cross-cloud, puis ne les restreignent jamais. J'ai audité des architectures où un Security Group AWS autorisait tout le range CIDR du VNet Azure — soit des milliers d'adresses IP — au lieu de cibler uniquement les subnets nécessaires. Adoptez le principe du *moindre privilège réseau* : chaque flux doit être documenté, justifié et limité au protocole, port et plage IP strictement nécessaires.

Pour renforcer cette segmentation, les principes décrits dans notre article sur segmentation réseau VLAN firewall sont directement applicables aux architectures cloud.

Sur un projet multi-cloud pour un acteur bancaire européen, nous avons déployé un modèle hub-and-spoke bilatéral avec un hub de transit dans chaque cloud, interconnectés via deux tunnels IPsec redondants. Chaque spoke (environnement applicatif) ne pouvait communiquer qu'avec son homologue dans l'autre cloud via des routes statiques et des ACL strictes. Ce modèle a réduit la surface d'attaque latérale de 87% par rapport à l'architecture flat initiale.

## Quelles solutions de monitoring centralisé déployer ?

Le monitoring multi-cloud nécessite une plateforme capable d'ingérer et corréler les logs des deux providers. Les options principales sont : **Microsoft Sentinel** (natif Azure, connecteurs AWS), **Splunk Cloud**, **Elastic SIEM** ou **Datadog Security Monitoring**. Le choix dépend de votre écosystème existant, mais Sentinel offre l'avantage d'une intégration native avec Azure et de connecteurs AWS matures pour CloudTrail, VPC Flow Logs, GuardDuty et Security Hub.

Configurez des règles de détection cross-cloud : par exemple, une alerte si un même principal IAM effectue des actions suspectes simultanément dans AWS et Azure (impossible physiquement, donc indicateur de compromission). Les logs doivent être centralisés dans un bucket S3 ou un Storage Account immuable avec des policies de rétention alignées sur vos obligations réglementaires. Le délai acceptable entre l'événement et sa visibilité dans le SIEM ne doit pas dépasser cinq minutes pour les événements critiques.

Les ressources officielles d'AWS Security et d'Azure Defender for Cloud documentent les meilleures pratiques de logging pour chaque provider.

## Comment gérer la conformité multi-cloud ?

La conformité multi-cloud impose de maintenir une posture cohérente malgré des contrôles natifs différents. AWS propose **AWS Config** avec des Conformance Packs, Azure dispose d'**Azure Policy** avec des initiatives. Pour unifier le tout, des solutions CSPM (Cloud Security Posture Management) comme Prisma Cloud, Wiz ou Orca Security évaluent en continu la conformité des deux environnements contre des frameworks communs : CIS Benchmarks, SOC 2, ISO 27001 et désormais NIS 2.

La directive NIS 2, applicable depuis octobre 2024, impose des exigences spécifiques aux opérateurs de services essentiels utilisant le cloud. En multi-cloud, cela signifie documenter précisément la chaîne de sous-traitance, maintenir un registre des traitements par provider et démontrer la capacité de portabilité entre les deux clouds. Le référentiel *SecNumCloud* de l'ANSSI ajoute une couche d'exigences pour les données sensibles hébergées sur des clouds qualifiés.

**À retenir :** La conformité multi-cloud ne se résume pas à cocher des cases. Elle nécessite une cartographie précise des données par niveau de sensibilité, un mapping explicite des contrôles par provider, et des audits croisés réguliers pour identifier les divergences de posture entre AWS et Azure.

## Faut-il utiliser un CASB pour le multi-cloud ?

Le *Cloud Access Security Broker* (CASB) agit comme un point de contrôle entre les utilisateurs et les services cloud. En multi-cloud, un CASB comme Microsoft Defender for Cloud Apps, Netskope ou Zscaler permet d'appliquer des politiques DLP uniformes, de détecter le shadow IT et de contrôler les accès aux données sensibles indépendamment du provider. Le CASB est

particulièrement pertinent pour les scénarios SaaS multi-cloud où les utilisateurs accèdent à des services AWS et Azure depuis des appareils variés. Il complète la fédération IAM en ajoutant une couche de contrôle au niveau applicatif et données.

Notre analyse sur la sécurité offensive GCP montre comment les attaquants exploitent les configurations GCP, des techniques similaires s'appliquent aux environnements multi-cloud mal segmentés.

## Peut-on automatiser la réponse aux incidents cross-cloud ?

L'automatisation de la réponse aux incidents en multi-cloud repose sur des playbooks SOAR (Security Orchestration, Automation and Response) capables d'interagir avec les API des deux providers. Concrètement, un playbook de réponse à une compromission de clé d'accès AWS doit : révoquer la clé via l'API IAM, scanner les logs CloudTrail pour identifier les actions malveillantes, vérifier si le même utilisateur dispose de credentials Azure via la fédération, et le cas échéant, révoquer ses sessions Azure AD via l'API Microsoft Graph.

Les outils comme **Palo Alto XSOAR**, **Swimlane** ou les Logic Apps Azure combinés aux Step Functions AWS permettent de construire ces workflows cross-cloud. La clé réside dans la préparation : chaque scénario de compromission doit être documenté, testé et exécuté en conditions réelles lors de game days trimestriels. Pour approfondir les méthodologies de détection des secrets compromis, consultez notre guide sur audit Terraform compliance.

Votre équipe SOC est-elle réellement capable de corréler un incident qui traverse simultanément deux clouds en moins de trente minutes ?

## Comment gérer les coûts de sécurité multi-cloud ?

La sécurité multi-cloud a un coût significatif qu'il faut anticiper et optimiser. Les postes principaux incluent : les licences des outils de sécurité multi-cloud (CSPM, CNAPP), les coûts d'interconnexion réseau (tunnels VPN, Direct Connect, ExpressRoute), le stockage et la rétention des logs centralisés, et surtout le coût humain des compétences cross-cloud. Un ingénieur sécurité maîtrisant à la fois AWS et Azure est significativement plus rare et coûteux qu'un spécialiste mono-cloud. Optimisez en mutualisant les outils : un SIEM unique pour les deux clouds, des politiques IaC partagées, et des processus de revue de sécurité communs. Le retour sur investissement se mesure en réduction du temps de détection et de réponse aux incidents, en diminution des violations de conformité, et en évitement des compromissions coûteuses qui justifient largement l'investissement initial dans une gouvernance de sécurité multi-cloud structurée et outillée correctement.

**Sources et références :** CISA · Cloud Security Alliance

## Vers une maturité multi-cloud durable

Sécuriser une architecture multi-cloud AWS et Azure n'est pas un projet ponctuel mais un processus continu d'amélioration. Commencez par la fédération IAM, puis étendez progressivement le chiffrement, la segmentation réseau et le monitoring. Mesurez votre maturité avec le Cloud Security Maturity Model et fixez des objectifs trimestriels réalistes. Le multi-cloud sécurisé est atteignable à condition d'investir dans les compétences, les outils et surtout la gouvernance transverse.

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

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