AYI NEDJIMI Consultants

PAM multi-cloud : gérer les accès privilégiés hybrides

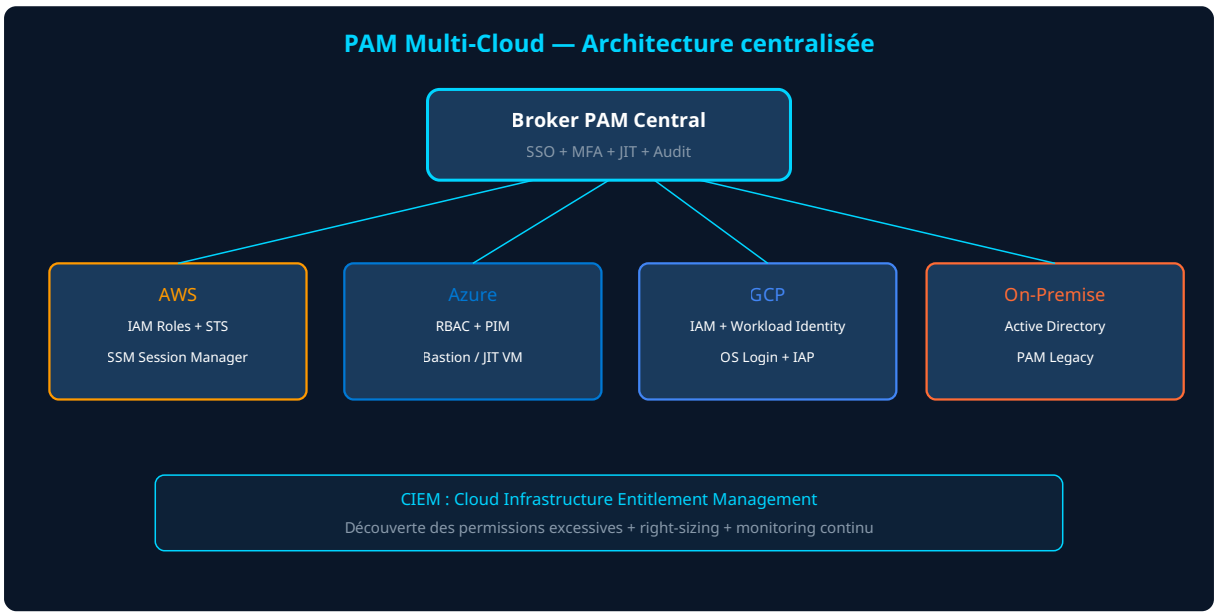
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

PAM multi-cloud : stratégies et outils pour gérer les accès privilégiés dans les environnements hybrides AWS, Azure et GCP avec CIEM et broker.

Votre infrastructure s'étend sur AWS, Azure, GCP et un datacenter on-premise. Chaque plateforme a son propre modèle IAM, ses propres rôles, ses propres mécanismes d'authentification. Résultat : vos équipes jonglent entre quatre consoles d'administration avec des comptes et des credentials différents pour chaque environnement. Cette fragmentation est un cauchemar opérationnel et un paradis pour les attaquants. Le PAM multi-cloud unifie la gestion des accès privilégiés à travers tous vos environnements cloud et on-premise dans un plan de contrôle centralisé. Ce guide vous présente les architectures de référence, les outils spécialisés et les stratégies de déploiement pour reprendre le contrôle de vos accès privilégiés dans un monde hybride. Nous aborderons les défis spécifiques de chaque cloud provider, les modèles d'intégration avec les solutions PAM existantes et l'émergence du CIEM (Cloud Infrastructure Entitlement Management) comme complément indispensable au PAM traditionnel. Des retours d'expérience concrets issus d'environnements de production multi-cloud viendront illustrer chaque recommandation.

Points clés à retenir

- 92% des organisations utilisent au moins deux cloud providers, mais seulement 30% ont un **PAM unifié**
- Le **CIEM** (Cloud Infrastructure Entitlement Management) comble le gap entre le PAM traditionnel et le cloud IAM
- Les **permissions excessives** sont le risque n°1 en cloud : 95% des identités cloud n'utilisent que 5% de leurs droits
- Un **broker d'accès centralisé** élimine la nécessité de comptes admin natifs par cloud provider
- Le Just-In-Time multi-cloud réduit la surface d'attaque à travers tous les environnements



Les défis spécifiques du PAM multi-cloud

Chaque cloud provider implémente son propre modèle IAM avec des concepts, une terminologie et des mécanismes différents. **AWS IAM** utilise des policies JSON attachées à des users, groups ou roles, avec des permissions qui se combinent par union. **Azure RBAC** utilise un modèle hiérarchique (management group > subscription > resource group > resource) avec des rôles built-in et custom. **GCP IAM** utilise des bindings entre des principals et des roles au niveau de l'organisation, du folder ou du projet.

Cette hétérogénéité crée trois problèmes majeurs. Le **manque de visibilité** : impossible de répondre à la question « qui a accès à quoi ? » à travers tous les environnements sans un outil centralisé. L'**incohérence des politiques** : une politique de moindre privilège dans Azure ne se traduit pas automatiquement dans AWS. Et la **prolifération de credentials** : chaque cloud nécessite ses propres access keys, service accounts ou certificates. Les coffres-forts de secrets adressent le stockage mais pas la gouvernance de ces credentials.

CIEM : le complément cloud-native du PAM

Le *Cloud Infrastructure Entitlement Management* (CIEM) est une catégorie d'outils spécialisée dans l'analyse et l'optimisation des permissions cloud. Là où le PAM traditionnel gère les sessions et les credentials, le CIEM se concentre sur le right-sizing des permissions. Statistique parlante : Microsoft Entra Permissions Management (ex-CloudKnox) rapporte que 95% des identités cloud n'utilisent que 5% de leurs permissions attribuées. Ce sur-provisionnement massif est une surface d'attaque dormante.

Les outils CIEM analysent l'usage réel des permissions sur une période de 90 jours, identifient les droits non utilisés et génèrent des recommandations de right-sizing. **Entra Permissions Management** couvre AWS, Azure et GCP dans une console unifiée. **Prisma Cloud** (Palo Alto) et

Wiz intègrent des fonctionnalités CIEM dans leur plateforme CNAPP. Le PAM et le CIEM sont complémentaires : le CIEM optimise les permissions statiques, le PAM gère les accès dynamiques.

Architecture du broker d'accès centralisé

Le *broker d'accès PAM* centralise tous les accès privilégiés multi-cloud dans un point d'entrée unique. L'administrateur s'authentifie au broker via SSO + MFA résistant au phishing, demande un accès JIT à une ressource spécifique (VM AWS, subscription Azure, projet GCP) et le broker génère des credentials temporaires natifs pour le cloud provider cible. L'administrateur n'a jamais de compte permanent dans aucun cloud.

Pour **AWS**, le broker utilise STS AssumeRole pour générer des credentials temporaires (1 heure). Pour **Azure**, il active le rôle PIM correspondant. Pour **GCP**, il attribue un IAM binding temporaire via l'API. Les solutions qui implémentent ce modèle : **CyberArk Privilege Cloud** avec les connecteurs multi-cloud, **BeyondTrust** avec Cloud Privilege Broker et **Teleport** (open source) qui unifie l'accès SSH, Kubernetes, bases de données et applications web. L'approche Just-In-Time est native dans cette architecture : aucun accès permanent, uniquement des activations temporaires.

Cloud	Mécanisme JIT natif	Session Recording	Intégration PAM
AWS	STS AssumeRole (1-12h)	SSM Session Manager	CyberArk, Teleport
Azure	PIM (1-8h)	Azure Bastion	CyberArk, BeyondTrust
GCP	IAM Conditions (temporel)	OS Login + IAP	Teleport, HashiCorp
Kubernetes	RBAC + token TTL	Audit logs	Teleport, CyberArk
On-Premise	PAM bastion	PAM natif	Tous

Gestion des identités machine multi-cloud

Les **identités non-humaines** (service accounts, workload identities, API keys) représentent le plus gros volume de credentials multi-cloud. Chaque pipeline CI/CD, chaque fonction serverless, chaque container a besoin d'une identité pour accéder aux ressources cloud. La bonne pratique : éliminer les credentials statiques au profit des identités fédérées. AWS IRSA (IAM Roles for Service Accounts) pour EKS, Azure Workload Identity pour AKS et GCP Workload Identity Federation pour GKE permettent aux workloads Kubernetes de s'authentifier sans secret stocké.

Pour les communications cross-cloud (un service AWS qui accède à Azure), la *workload identity federation* remplace les API keys statiques. AWS STS émet un token OIDC que Azure Entra ID accepte comme preuve d'identité via une federated credential. Zéro mot de passe, zéro secret à rotater, audit trail complet. Cette approche nécessite une architecture soigneusement planifiée mais élimine une catégorie entière de risques. Les bonnes pratiques de sécurisation des comptes de service s'appliquent avec des adaptations pour chaque cloud.

Conformité et audit multi-cloud unifié

L'audit des accès privilégiés multi-cloud est un défi majeur pour la conformité. Les régulateurs exigent une piste d'audit complète de chaque accès privilégié, indépendamment du cloud provider. La centralisation des logs d'accès dans un **SIEM unique** est indispensable. Configurez l'export des journaux IAM de chaque cloud : AWS CloudTrail, Azure Activity Log, GCP Cloud Audit Logs vers votre SIEM via des connecteurs natifs.

Créez des rapports de conformité unifiés qui couvrent les quatre domaines de contrôle : **inventaire** (combien de comptes privilégiés par cloud), **accès** (qui a accédé à quoi, quand), **permissions** (ratio permissions attribuées vs utilisées), **anomalies** (accès en dehors des patterns normaux). La conformité NIS2 et ISO 27017 impose ces contrôles pour les opérateurs de services essentiels. Un référentiel ANSSI d'administration sécurisée fournit le cadre applicable aux environnements hybrides.

Stratégie de déploiement multi-cloud progressive

Le déploiement PAM multi-cloud suit une logique d'extension progressive. Étape 1 : consolidez votre PAM on-premise existant (si ce n'est pas fait). Étape 2 : intégrez votre cloud principal (généralement Azure ou AWS) avec le broker PAM centralisé. Étape 3 : ajoutez les clouds secondaires. Étape 4 : déployez le CIEM pour le right-sizing des permissions. Étape 5 : automatisez la réponse aux anomalies via l'intégration ITDR.

Le piège classique : vouloir unifier les trois clouds simultanément. Concentrez-vous sur le cloud qui concentre le plus de workloads critiques. Les gains de visibilité et de contrôle sur un seul cloud justifient l'investissement et créent le momentum pour étendre aux autres. Un vCISO externalisé peut piloter cette transformation pour les organisations qui ne disposent pas d'expertise multi-cloud en interne.

Questions fréquentes sur le PAM multi-cloud

Peut-on utiliser le PAM natif de chaque cloud au lieu d'un outil centralisé ?

Techniquement oui, mais c'est une approche fragmentée qui ne scale pas. Chaque cloud a son propre PAM natif (AWS SSM, Azure PIM, GCP OS Login) mais sans vue unifiée, sans politiques cohérentes et sans audit centralisé. Un broker PAM centralisé n'élimine pas les mécanismes natifs — il les orchestre. Les mécanismes natifs restent les points d'application, mais le broker centralise la décision, le workflow et l'audit. Pour les organisations avec un seul cloud, le PAM natif peut suffire.

Comment gérer les comptes root AWS et Global Admin Azure ?

Ces comptes sont l'équivalent des break-glass dans le cloud. Règles strictes : changement de mot de passe après chaque utilisation (stocké dans un vault physique), MFA matériel dédié (pas un smartphone), monitoring de chaque connexion avec alerte immédiate, utilisation

uniquement pour les opérations impossibles autrement (modification de l'organisation billing, récupération d'un tenant verrouillé). En fonctionnement normal, personne n'utilise ces comptes — tout passe par des rôles délégués via le broker PAM.

Quel est le coût d'un PAM multi-cloud pour une organisation moyenne ?

Pour une organisation de 2000 utilisateurs avec AWS + Azure, comptez entre 150 et 350 k€/an pour un PAM centralisé (CyberArk Privilege Cloud ou BeyondTrust). Le CIEM ajoute 50 à 100 k€/an (Entra Permissions Management est inclus dans M365 E5 Security). Les solutions open source comme Teleport réduisent les coûts de licence mais augmentent les coûts d'exploitation interne. Le ROI se mesure en réduction de surface d'attaque et en temps d'audit économisé.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et recommandations

Le PAM multi-cloud n'est plus un luxe pour les grandes entreprises — c'est une nécessité dès que vous opérez sur deux cloud providers ou plus. La centralisation du contrôle, la visibilité unifiée et le JIT multi-cloud réduisent drastiquement la surface d'attaque de vos environnements hybrides. Commencez par le cloud principal, prouvez la valeur, puis étendez. Et n'oubliez pas le CIEM : les permissions excessives sont un risque tout aussi critique que les accès non contrôlés. Vos clouds ne méritent pas moins de sécurité que votre datacenter.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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