AYI NEDJIMI Consultants

Sécuriser les comptes de service : rotation et vault

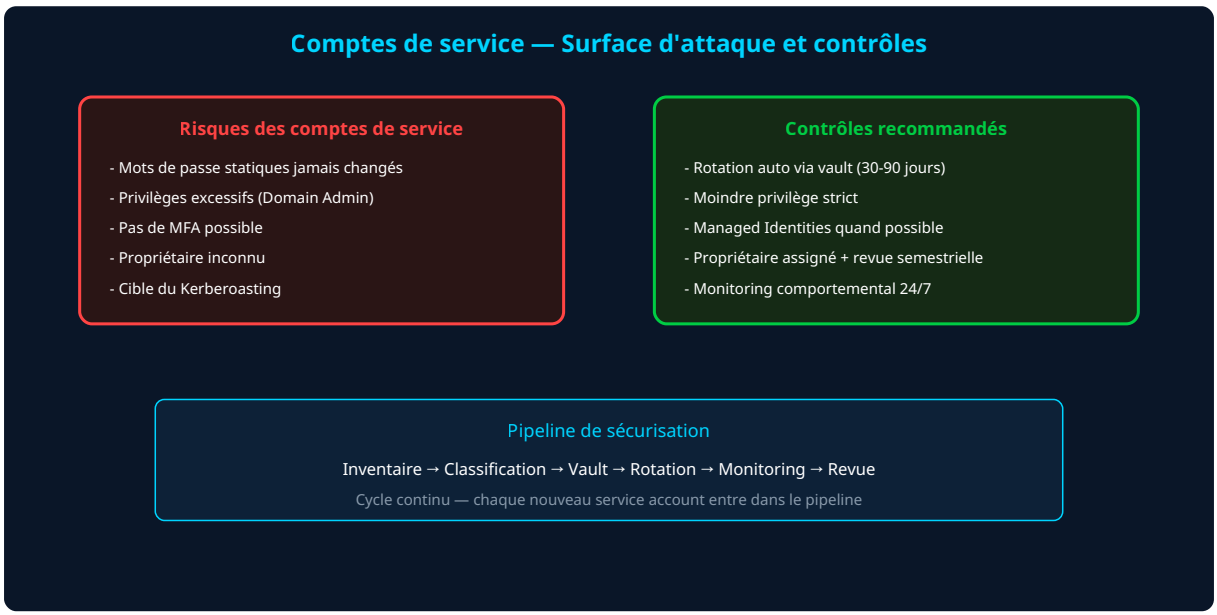
Catégorie : IAM et Gestion des Identités Lecture : 7 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Sécurisez vos comptes de service Active Directory et cloud : rotation automatique, intégration vault, monitoring et bonnes pratiques de gestion des.

Les comptes de service sont les identités oubliées de la sécurité. Personne ne les connaît vraiment, personne ne les maintient, et pourtant ils disposent souvent de privilèges considérables sur le système d'information. Un compte de service SQL Server avec des droits Domain Admin, un API key AWS avec la politique AdministratorAccess, un service principal Entra ID avec Directory.ReadWrite.All — ces configurations existent dans la majorité des organisations et représentent des vecteurs d'attaque silencieux. Contrairement aux comptes utilisateurs protégés par le MFA et les politiques d'accès conditionnel, les comptes de service échappent généralement aux contrôles de sécurité standards. Ce guide vous fournit une méthodologie complète pour reprendre le contrôle de ces identités non-humaines. De l'inventaire à la rotation automatique, de l'intégration vault au monitoring comportemental, chaque étape est détaillée avec des exemples concrets tirés d'environnements Active Directory, Azure et AWS. L'objectif est clair : transformer vos comptes de service d'un angle mort sécuritaire en un périmètre maîtrisé et auditable.

Points clés à retenir

- Les **comptes de service** représentent en moyenne 60% des identités d'une organisation
- 78% des comptes de service AD ont des mots de passe inchangés depuis plus d'un an
- La **rotation automatique** via vault réduit le risque de credential compromise de 95%
- Les **Managed Identities** Azure et les **IAM Roles** AWS éliminent le besoin de credentials statiques
- Le monitoring comportemental détecte les usages anormaux des comptes de service en temps réel



Inventaire des comptes de service : découverte et classification

L'inventaire est la première étape et souvent la plus révélatrice. Dans Active Directory, les comptes de service se répartissent en trois catégories. Les *comptes de service standard* sont des comptes utilisateur normaux utilisés par des applications (type : userAccountControl sans l'attribut NORMAL_ACCOUNT). Les *Managed Service Accounts* (MSA) et **Group Managed Service Accounts** (gMSA) sont des comptes gérés automatiquement par AD avec rotation de mot de passe intégrée. Les *Service Principals* dans Entra ID sont l'équivalent cloud des comptes de service.

Pour découvrir tous les comptes de service AD, combinez plusieurs approches : requête LDAP sur les attributs servicePrincipalName (SPN), analyse des services Windows installés sur les serveurs, audit des tâches planifiées et des pools d'applications IIS. BloodHound identifie les comptes de service avec des chemins d'attaque vers les Domain Admins — ces comptes sont vos priorités de remédiation. En moyenne, une organisation de 2000 utilisateurs découvre entre 500 et 1500 comptes de service lors de cet inventaire.

Kerberoasting : la menace spécifique aux comptes de service AD

Le **Kerberoasting** est l'attaque la plus répandue contre les comptes de service Active Directory. Tout utilisateur authentifié peut demander un ticket de service (TGS) pour n'importe quel SPN enregistré dans l'AD. Ce ticket est chiffré avec le hash du mot de passe du compte de service. L'attaquant exporte le ticket et le craque hors ligne avec des outils comme **Hashcat** ou **John the Ripper**. Si le mot de passe est faible (< 25 caractères), le craquage prend quelques heures. Si le mot de passe n'a pas changé depuis 3 ans, l'attaquant a tout son temps.

Les techniques de cracking de mots de passe évoluent rapidement. Avec les GPU modernes, un mot de passe de 14 caractères se craque en quelques jours. La défense : des mots de passe de 30 caractères minimum générés aléatoirement et stockés dans un vault, une rotation tous les 30

jours et la migration vers les gMSA partout où c'est techniquement possible. Les gMSA utilisent des mots de passe de 240 caractères gérés automatiquement par AD — incraquables en pratique.

Intégration avec un vault de secrets

Le coffre-fort de secrets est le pilier technique de la sécurisation des comptes de service. **HashiCorp Vault**, **Azure Key Vault**, **AWS Secrets Manager** et les vaults PAM (CyberArk, BeyondTrust) assurent le stockage sécurisé et la rotation automatique des credentials. L'application ne connaît jamais le mot de passe réel : elle s'authentifie auprès du vault, qui lui fournit un credential temporaire.

L'architecture de référence fonctionne ainsi : l'application s'authentifie au vault via une *managed identity* (Azure), un **IAM role** (AWS) ou un token AppRole (Vault). Le vault vérifie l'identité, applique la politique d'accès et retourne le secret demandé avec une durée de vie limitée (TTL de 1 à 24 heures). À l'expiration, l'application redemande un nouveau secret. Ce modèle élimine les credentials statiques et crée un audit trail complet de chaque accès aux secrets.

Solution vault	Rotation AD	Rotation cloud	API REST	Coût
HashiCorp Vault	Oui (plugin AD)	AWS, Azure, GCP	Oui	Open source / Enterprise
Azure Key Vault	Non natif	Azure natif	Oui	Inclus Azure
AWS Secrets Manager	Non natif	AWS natif	Oui	0.40$/secret/mois
CyberArk CPM	Oui (natif)	Oui (connecteurs)	Oui	Licence PAM

Managed Identities et IAM Roles : éliminer les credentials

La meilleure façon de sécuriser un credential, c'est de ne pas en avoir. Les **Managed Identities** Azure permettent aux ressources Azure (VM, App Service, Function) de s'authentifier auprès d'autres services Azure sans aucun credential stocké. L'identité est gérée automatiquement par la plateforme : pas de mot de passe à stocker, pas de rotation à planifier, pas de secret à protéger. C'est l'approche recommandée pour toute communication service-to-service dans Azure.

L'équivalent AWS est le **IAM Role** avec instance profile : une instance EC2 assume un rôle IAM et reçoit des credentials temporaires (STS) renouvelés automatiquement. Pour les workloads multi-cloud, les *workload identity federation* permettent à un service AWS de s'authentifier dans Azure (et vice versa) sans credentials statiques. Ces mécanismes couvrent environ 70% des cas d'usage de comptes de service cloud. Pour les 30% restants (applications legacy, intégrations tierces), le vault reste nécessaire.

Monitoring comportemental des comptes de service

Les comptes de service ont des patterns d'utilisation prévisibles : mêmes heures de connexion, mêmes IP sources, mêmes ressources accédées. Cette prévisibilité est un atout pour la détection d'anomalies. Un compte de service SQL qui se connecte habituellement depuis le serveur applicatif entre 6h et 23h et qui soudain s'authentifie depuis un poste de travail à 3h du matin, c'est un signal d'alerte fort.

Configurez des **baselines comportementales** pour vos comptes de service critiques dans votre SIEM. Les indicateurs à surveiller : IP source, horaires de connexion, volume d'opérations, types de requêtes, destinations réseau. Microsoft Defender for Identity propose un tagging spécifique des comptes de service avec détection automatique des anomalies. Pour les environnements AWS, **CloudTrail** combiné à **GuardDuty** remplit le même rôle. L'intégration avec votre SOC garantit une réponse rapide aux alertes.

Migration vers les gMSA dans Active Directory

Les **Group Managed Service Accounts** (gMSA) sont la réponse Microsoft au problème des comptes de service AD. Un gMSA utilise un mot de passe de 240 caractères généré et renouvelé automatiquement tous les 30 jours par les contrôleurs de domaine. Aucun humain ne connaît ni ne gère ce mot de passe. Le gMSA ne peut être utilisé que par les serveurs autorisés dans sa configuration, ce qui empêche son utilisation depuis un poste compromis.

La migration vers les gMSA couvre les services Windows, les tâches planifiées, les pools IIS et les instances SQL Server. Le processus : créez la clé KDS root (une seule fois par forêt), créez le gMSA avec `New-ADServiceAccount`, assignez les serveurs autorisés et reconfigurez le service pour utiliser le gMSA au lieu du compte de service classique. Les bonnes pratiques de sécurisation AD recommandent la migration systématique vers les gMSA. Pour les applications qui ne supportent pas les gMSA (applications legacy, agents tiers), le vault avec rotation automatique reste l'alternative.

Gouvernance et revue périodique

La gouvernance des comptes de service nécessite un processus dédié distinct de la gouvernance des identités humaines. Chaque compte de service doit avoir un **propriétaire identifié** (le responsable de l'application) et un **contact technique** (l'équipe qui maintient le service). Une revue semestrielle vérifie trois points : le compte est-il encore nécessaire, ses privilèges sont-ils proportionnés à son usage, et les contrôles de sécurité sont-ils en place (rotation, monitoring, principe du moindre privilège).

Intégrez la gestion des comptes de service dans votre solution IGA pour un suivi centralisé. Les solutions comme **Silverfort** et **Astrix Security** se spécialisent dans la découverte et la protection des identités non-humaines, comblant un gap que les solutions IAM traditionnelles adressent mal. Le guide ANSSI sur Active Directory consacre une section entière aux comptes de service avec des recommandations directement applicables.

Questions fréquentes sur les comptes de service

Comment identifier les comptes de service à risque en priorité ?

Trois critères de priorisation : les comptes avec des SPN enregistrés et un mot de passe ancien (cibles Kerberoasting), les comptes membres de groupes à privilèges élevés (Domain Admins, Schema Admins) et les comptes dont le propriétaire est inconnu ou a quitté l'organisation. BloodHound et PingCastle génèrent des rapports priorisés automatiquement. Concentrez-vous d'abord sur les comptes qui combinent deux ou trois de ces critères.

Peut-on appliquer le MFA aux comptes de service ?

Non, par définition un compte de service fonctionne sans interaction humaine. Le MFA n'est donc pas applicable. Les contrôles compensatoires sont : la restriction par IP source (seuls les serveurs autorisés peuvent utiliser le compte), la rotation automatique fréquente des credentials, le monitoring comportemental et l'utilisation de managed identities ou gMSA quand possible. Ces contrôles combinés offrent un niveau de sécurité comparable au MFA pour les identités humaines.

Quelle fréquence de rotation pour les mots de passe des comptes de service ?

La fréquence dépend du niveau de risque. Pour les comptes à privilèges élevés : rotation tous les 30 jours via vault automatisé. Pour les comptes standards : rotation tous les 90 jours. Pour les gMSA : rotation automatique tous les 30 jours par défaut (configurable). Pour les tokens et API keys cloud : durée de vie maximale de 1 heure (credentials temporaires STS). Toute rotation doit être testée en environnement de pré-production avant application en production pour éviter les interruptions de service.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et plan d'action immédiat

La sécurisation des comptes de service est un chantier de fond qui commence par la visibilité. Lancez l'inventaire cette semaine, identifiez les comptes à risque, assignez des propriétaires et démarrez la migration vers les gMSA et les managed identities. Chaque compte de service sécurisé réduit votre surface d'attaque. Chaque credential statique éliminé supprime un vecteur d'exploitation. Traitez vos comptes de service avec la même rigueur que vos comptes d'administration — ils le méritent.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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