AWS Guide de décision

Choisir un service de AWS cryptographie

Choisir un service de AWS cryptographie: AWS Guide de décision

Table of Contents

Choisir un service de AWS cryptographie

Faire le premier pas

Objectif	Aidez à déterminer les services de AWS cryptographie les mieux adaptés à votre entreprise.
Dernière mise à jour	31 janvier 2025
Services couverts	• AWS Certificate Manager • AWS CloudHSM • AWS SDK de chiffrement de base de données • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
Guides associés	Choix des services AWS de sécurité, d'identité et de gouvernance

Introduction

La cryptographie est la pierre angulaire de la sécurité dans le cloud computing, car elle contribue à garantir la confidentialité, l'intégrité et l'authenticité des données. Dans un environnement cloud, les données sensibles peuvent traverser les réseaux publics et résider sur une infrastructure partagée. Des mesures cryptographiques robustes sont donc essentielles pour se protéger contre les accès non autorisés ou les falsifications.

AWS propose une gamme complète de services cryptographiques pour sécuriser les données, gérer les clés de chiffrement et protéger les informations sensibles. Il s'agit notamment de AWS Key Management Service (KMS) pour la gestion centralisée des clés, AWS CloudHSM pour PKCS11 les applications et les modules de sécurité matériels dédiés, ainsi que AWS Encryption SDK pour le chiffrement côté client. AWS Secrets Manager est un service qui vous permet de stocker, de gérer et

de récupérer en toute sécurité des informations sensibles telles que les informations d'identification des bases de données, les clés d'API et d'autres informations secrètes tout au long de leur cycle de vie. AWS Certificate Manager (ACM) simplifie le processus de provisionnement, de gestion et de déploiement de certificats TLS (Transport Layer Security) approuvés par le public à utiliser avec. Services AWS Le AWS Private Certificate Authority (PCA) vous permet de générer et de distribuer des certificats x509 pour vos ressources internes.

Le guide est conçu pour vous aider à choisir les services et outils de AWS cryptographie les mieux adaptés à vos besoins et à ceux de votre organisation.

La vidéo suivante est un segment de deux minutes d'une présentation présentant les meilleures pratiques en matière de cryptographie.

Comprendre

Le choix des services de AWS cryptographie appropriés dépend de votre cas d'utilisation spécifique, des exigences de sécurité des données, des obligations de conformité et des préférences opérationnelles, comme indiqué dans les tableaux suivants.

Key management

Si vous devez gérer les clés de chiffrement en toute sécurité, envisagez le service de gestion des AWS clés (KMS). Il vous permet de créer, de faire pivoter et de gérer des clés cryptographiques intégrées à d'autres Services AWS. KMS utilise la certification FIPS pour vous aider HSMs à répondre aux exigences de conformité et à garantir l'exactitude de l'implémentation des primitives cryptographiques exposées par KMS. Certaines applications nécessitent certaines fonctions cryptographiques ou interfaces d'application qui ne sont disponibles qu'avec un HSM traditionnel et AWS CloudHSM fournissent des modules de sécurité matériels dédiés (HSMs) dans le cloud qui vous permettent de contrôler totalement vos clés et opérations cryptographiques.

Data encryption

Pour le chiffrement des données sensibles telles que les informations sur les clients ou la propriété intellectuelle, AWS KMS il est étroitement intégré aux services AWS de stockage, de base de données et de messagerie (par exemple S3, RDS ou EBS). Si vous avez besoin d'un chiffrement côté client, il AWS Encryption SDK s'agit d'une bibliothèque open source qui permet de chiffrer facilement les données de votre application avant de les envoyer dans le cloud.

Secure communications

Pour protéger les données en transit, AWS Certificate Manager (ACM) simplifie la gestion des certificats TLS approuvés par le public. Utilisez-le pour affirmer l'identité de vos applications connectées à Internet et faciliter le chiffrement des communications entre votre application, les utilisateurs et les services cloud sans vous soucier du renouvellement des certificats. Pour les applications internes, vous pouvez utiliser l'autorité de certification AWS privée (PCA) pour générer et distribuer des certificats x509 pour vos ressources internes, y compris les clients et les serveurs.

Secrets and credentials management

Pour stocker et récupérer en toute sécurité les secrets des applications tels que les informations d'identification de base de données, les clés d'API ou les certificats, pensez AWS Secrets Managerà Il fournit une rotation secrète automatisée et des contrôles d'accès précis. Par ailleurs, AWS Systems Manager Parameter Store est une option moins coûteuse pour gérer des configurations non sensibles et peut s'intégrer à. AWS Secrets Manager

Compliance and auditing

Pour les travaux de conformité réglementaire, prenez en compte AWS KMS les normes de chiffrement et aidez-les AWS CloudHSM à vous assurer qu'elles sont respectées. AWS Artifact

est un portail en libre-service qui fournit un accès à la demande aux rapports AWS de sécurité et de conformité, tels que les certifications ISO et les rapports SOC, ainsi que la possibilité de consulter et d'accepter des accords tels que le Business Associate Addendum (BAA). Vous pouvez également utiliser des services tels que AWS Config AWS Security Hub, et AWS Audit Manager pour surveiller la conformité et produire les artefacts appropriés pour votre propre usage ou pour la consommation par vos parties prenantes.

Lorsque vous choisissez entre les services de AWS cryptographie, tenez compte des exigences suivantes.

Exigence	Service
Faible effort, entièrement géré	AWS KMS ou AWS Secrets Manager
Nécessite des interfaces d'application spécifiques ou des algorithmes cryptographiques non pris en charge par KMS	AWS CloudHSM
Encrypting/decrypting données dans vos applications	AWS Encryption SDK
Gestion simplifiée des certificats TLS publics	AWS Certificate Manager
Gestion des secrets	AWS Secrets Manager

En alignant vos exigences sur ces options, vous pouvez mettre en œuvre des solutions cryptographiques adaptées à vos besoins opérationnels et de sécurité.

Tenez compte

Pour choisir le bon service de AWS cryptographie, il faut comprendre vos besoins spécifiques en matière de sécurité, d'exploitation et de conformité. AWS propose une variété de services cryptographiques, chacun étant conçu pour répondre à différents cas d'utilisation, de la gestion des clés au chiffrement des données et aux communications sécurisées. Pour prendre une décision éclairée, vous devez évaluer vos exigences en fonction de plusieurs critères essentiels, notamment votre cas d'utilisation, vos besoins en matière de contrôle et de flexibilité, les obligations de conformité, les considérations financières et l'intégration avec Services AWS. Ces critères vous

aideront à aligner votre choix sur les objectifs de sécurité et les flux de travail opérationnels de votre organisation.

Use case

Réfléchissez aux raisons pour lesquelles vous avez besoin du service cryptographique : chiffrement des données, gestion des clés, communication sécurisée ou gestion des secrets. Par exemple, AWS KMS il est idéal pour le chiffrement intégré Services AWS, mais AWS CloudHSM convient aux entreprises qui ont besoin de certaines fonctionnalités cryptographiques, d'interfaces applicatives ou d'un HSM à locataire unique, souvent pour des raisons de conformité strictes ou de besoins spécifiques des applications. La clarification de l'objectif vous permet de sélectionner un service adapté à vos besoins, en optimisant à la fois les fonctionnalités et les coûts.

Control and flexibility

Évaluez le niveau de contrôle dont vous avez besoin pour vos opérations cryptographiques. Les services gérés tels que le HSM multi-tenant AWS KMS offrent une facilité d'utilisation avec un minimum de frais de gestion, tout en gardant un contrôle total sur vos informations clés. En revanche, AWS CloudHSM propose un modèle à locataire unique pour des besoins spécifiques en matière d'application, de cryptographie ou de conformité.

Compliance requirements

Si vous opérez dans un secteur réglementé, assurez-vous que le service est conforme aux normes telles que le RGPD, la norme PCI DSS ou la loi HIPAA. AWS KMS et AWS CloudHSM sont tous deux certifiés FIPS 140-2 niveau 3. Le choix d'un service qui répond à vos exigences non fonctionnelles contribue à maintenir la confiance et peut éviter d'éventuelles sanctions juridiques ou financières.

Cost considerations

Évaluez votre budget par rapport au modèle de tarification du service. AWS KMS est rentable pour les besoins généraux de chiffrement, tout en AWS CloudHSM entraînant des coûts plus élevés en raison du matériel dédié. Comprendre les implications financières vous aide à optimiser vos dépenses de sécurité.

Integration with AWS ecosystem

Si vous en utilisez beaucoup Services AWS, privilégiez une solution de cryptographie telle AWS KMS qu'ACM qui s'intègre parfaitement à S3, RDS ou Lambda. Cela garantit des flux de travail plus fluides et réduit les efforts de développement. Les capacités d'intégration peuvent améliorer considérablement l'efficacité opérationnelle.

Choix

Pour choisir le bon service de AWS cryptographie, il faut comprendre vos besoins spécifiques en matière de sécurité, d'exploitation et de conformité. AWS propose une variété de services cryptographiques, chacun étant conçu pour répondre à différents cas d'utilisation, de la gestion des clés au chiffrement des données et aux communications sécurisées. Pour prendre une décision éclairée, vous devez évaluer vos exigences en fonction de plusieurs critères essentiels, notamment votre cas d'utilisation, vos besoins en matière de contrôle et de flexibilité, les obligations de conformité, les considérations financières et l'intégration avec Services AWS. Ces critères vous aideront à aligner votre choix sur les objectifs de sécurité et les flux de travail opérationnels de votre organisation.

Cas d'utilisation cible	Quand l'utiliseriez-vous ?	Service recommandé
Gestion des clés	Pour créer, faire pivoter et gérer en toute sécurité des clés cryptographiques intégrées à d'autres Services AWS	AWS KMS
Gestion des clés	Pour des intégrations d'applications ou des primitives cryptographiques spécifiques	AWS CloudHSM
Chiffrement des données	Mettre en œuvre le chiffrement côté client afin de protéger les données sensibles telles que les informations sur les clients ou la propriété intellectuelle.	AWS Encryption SDK AWS SDK de chiffrement de base de données
Communications sécurisées	Pour protéger les données en transit et simplifier la gestion des SSL/TLS certificats.	AWS Certificate Manager AWS Private CA
Gestion des secrets et des informations d'identification	Pour stocker et récupérer en toute sécurité les secrets des applications tels que les informations d'identification	AWS Secrets Manager AWS Magasin de paramètres

Cas d'utilisation cible	Quand l’utiliseriez-vous ?	Service recommandé
	de base de données, les clés d'API ou les certificats.	

Utiliser

Vous devriez maintenant avoir une idée claire de ce que fait chaque service de AWS cryptographie et de ceux qui pourraient vous convenir le mieux.

Pour découvrir comment utiliser et en savoir plus sur chacun des services de AWS cryptographie disponibles, nous avons fourni un moyen d'explorer le fonctionnement de chacun d'entre eux. Les sections suivantes fournissent des liens vers une documentation détaillée, des didacticiels pratiques et d'autres ressources pour vous aider à démarrer.

AWS Certificate Manager

- Commencez avec AWS Certificate Manager

  Commencez à utiliser AWS Certificate Manager, notamment à travailler avec des certificats publics et privés.

  Explorer le guide
- Les meilleures pratiques pour AWS Certificate Manager

  Passez en revue les recommandations qui peuvent vous aider à les utiliser AWS Certificate Manager plus efficacement.

  Explorer le guide
- AWS Certificate Manager FAQ

  Consultez la page FAQ AWS Certificate Manager (ACM) pour obtenir des réponses détaillées aux questions courantes sur les fonctionnalités, les capacités et l'utilisation d'ACM. Il couvre des sujets tels que les types de certificats gérés par ACM, l'intégration avec d'autres Services AWS certificats, ainsi que des conseils sur le provisionnement et la gestion des SSL/TLS certificats.

  Découvrez le FAQs

AWS CloudHSM

- Commencez avec AWS CloudHSM

  Découvrez comment créer, initialiser et activer un cluster dans AWS CloudHSM. Une fois que vous aurez suivi ces instructions, vous serez prêt à gérer des utilisateurs et des clusters, et à effectuer des opérations de chiffrement à l'aide des bibliothèques de logiciels incluses.

  Explorer le guide

- Les meilleures pratiques pour AWS CloudHSM

  Découvrez les meilleures pratiques en matière de gestion et de surveillance de votre AWS CloudHSM cluster.

  Explorer le guide

- AWS CloudHSM tarification

  Consultez la page de tarification pour en savoir plus sur AWS CloudHSM les tarifs. Son utilisation AWS CloudHSM n'entraîne aucun coût initial. Avec AWS CloudHSM, vous payez un tarif horaire pour chaque HSM que vous lancez jusqu'à ce que vous mettiez fin au HSM. Ce guide fournit le taux horaire pour chaque AWS région.

  Explorez la page de tarification

- AWS CloudHSM FAQ

  Consultez la page AWS CloudHSM FAQ pour obtenir des réponses détaillées aux questions les plus fréquemment posées AWS CloudHSM, notamment sur ses fonctionnalités, sa tarification, son approvisionnement, sa sécurité, sa conformité, ses performances et son intégration avec des applications tierces.

  Découvrez le FAQs

AWS Encryption SDK

- Commencez avec le AWS Encryption SDK

  Apprenez à utiliser le AWS Encryption SDK avec AWS KMS.

  Explorer le guide

- Les meilleures pratiques pour le AWS Encryption SDK

  Consultez la page AWS Encryption SDK Bonnes pratiques pour obtenir des conseils sur l'utilisation efficace AWS Encryption SDK de afin de sécuriser vos données. Le respect de ces meilleures pratiques permet de garantir la confidentialité et l'intégrité de vos données chiffrées.

  Explorer le guide
- AWS Encryption SDK FAQ

  Consultez la page AWS Encryption SDK FAQ pour obtenir des réponses aux questions les plus fréquemment posées sur le AWS Encryption SDK, notamment ses fonctionnalités, les langages de programmation pris en charge et les meilleures pratiques en matière de mise en œuvre.

  Explorez la FAQ

AWS Database Encryption SDK

- Commencez avec le SDK de chiffrement AWS de base de données

  Découvrez comment utiliser le SDK de chiffrement AWS de base de données avec AWS KMS.

  Explorer le guide
- Configuration du SDK de chiffrement AWS de base de données

  Découvrez comment configurer le SDK de chiffrement AWS de base de données, notamment en sélectionnant un langage de programmation et en sélectionnant des clés d'encapsulation.

  Explorer le guide

AWS KMS

- Commencez avec AWS KMS

  Découvrez comment créer des clés KMS, notamment des clés de chiffrement symétriques et asymétriques.

  Explorer le guide
- Les meilleures pratiques pour AWS KMS

  Découvrez les meilleures pratiques de chiffrement pour AWS KMS.

Explorer le guide

- AWS KMS tarification

  Consultez la page de tarification AWS Key Management Service (KMS) pour en savoir plus sur les coûts associés à l'utilisation AWS KMS, notamment les frais de stockage des clés, les demandes d'API et les fonctionnalités optionnelles telles que les magasins de clés personnalisés.

  Explorez la page de tarification

- AWS KMS FAQ

  La page FAQ AWS Key Management Service (KMS) fournit des réponses détaillées aux questions courantes concernant notamment ses fonctionnalités AWS KMS, ses mesures de sécurité, ses pratiques de facturation, ses options de gestion des clés et son intégration avec d'autres Services AWS.

  Découvrez le FAQs

AWS Private CA

- Les meilleures pratiques pour AWS Private CA

  Passez en revue les recommandations qui peuvent vous aider à AWS Private CA les utiliser efficacement.

  Explorer le guide

- Commencez avec AWS Private CA

  Découvrez comment créer et activer une autorité de certification root par programmation.

  Explorer le guide

- AWS Private CA tarification

  Passez en revue les coûts associés à l'exploitation du secteur privé CAs et à l'émission de certificats privés.

  Explorez la page de tarification

- AWS Private CA FAQ

Obtenez des réponses détaillées aux questions les plus fréquemment posées AWS Private CA, notamment sur ses fonctionnalités, sa tarification, son approvisionnement, sa sécurité, sa conformité, ses performances et son intégration avec d'autres Services AWS.

Découvrez le FAQs

AWS Secrets Manager

- Commencez avec AWS Secrets Manager

  Apprenez à créer un AWS Secrets Manager secret.

  Explorer le guide
- Les meilleures pratiques pour AWS Secrets Manager

  Découvrez les meilleures pratiques à prendre en compte lors de l'utilisation AWS Secrets Manager.

  Explorer le guide
- AWS Secrets Manager tarification

  Consultez la page de AWS Secrets Manager tarification pour en savoir plus sur les coûts associés au stockage, à la gestion et à la récupération sécurisés de secrets tels que les informations d'identification de base de données et les clés d'API.

  Explorez la page de tarification
- AWS Secrets Manager FAQ

  Consultez la page AWS Secrets Manager FAQ pour obtenir des réponses détaillées aux questions les plus fréquemment posées AWS Secrets Manager, notamment sur ses fonctionnalités, ses mesures de sécurité, ses prix et ses capacités d'intégration.

  Découvrez le FAQs

Explorez

- Recherche et ressources

Explorez AWS des blogs, des vidéos et des outils sur la cryptographie.

Ressources de révision

- Vidéos

Regardez ces vidéos de la chaîne AWS Developers YouTube pour développer et affiner votre stratégie de cryptographie.

Découvrez les vidéos de cryptographie

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide de décision. Pour recevoir des notifications concernant les mises à jour de ce guide, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Publication initiale	Guide publié pour la première fois.	31 janvier 2025

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.