AWS 决策指南

选择 AWS 加密服务

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

选择 AWS 加密服务: AWS 决策指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

选择 AWS 加密服务

迈出第一步

目的	帮助确定哪些 AWS 加密服务最适合您的组织。
上次更新	2025 年 1 月 31 日
承保服务	• AWS Certificate Manager • AWS CloudHSM • AWS 数据库加密 SDK • AWS Encryption SDK • AWS KMS • AWS Private CA • AWS Secrets Manager
相关指南	选择 AWS 安全、身份和治理服务

简介

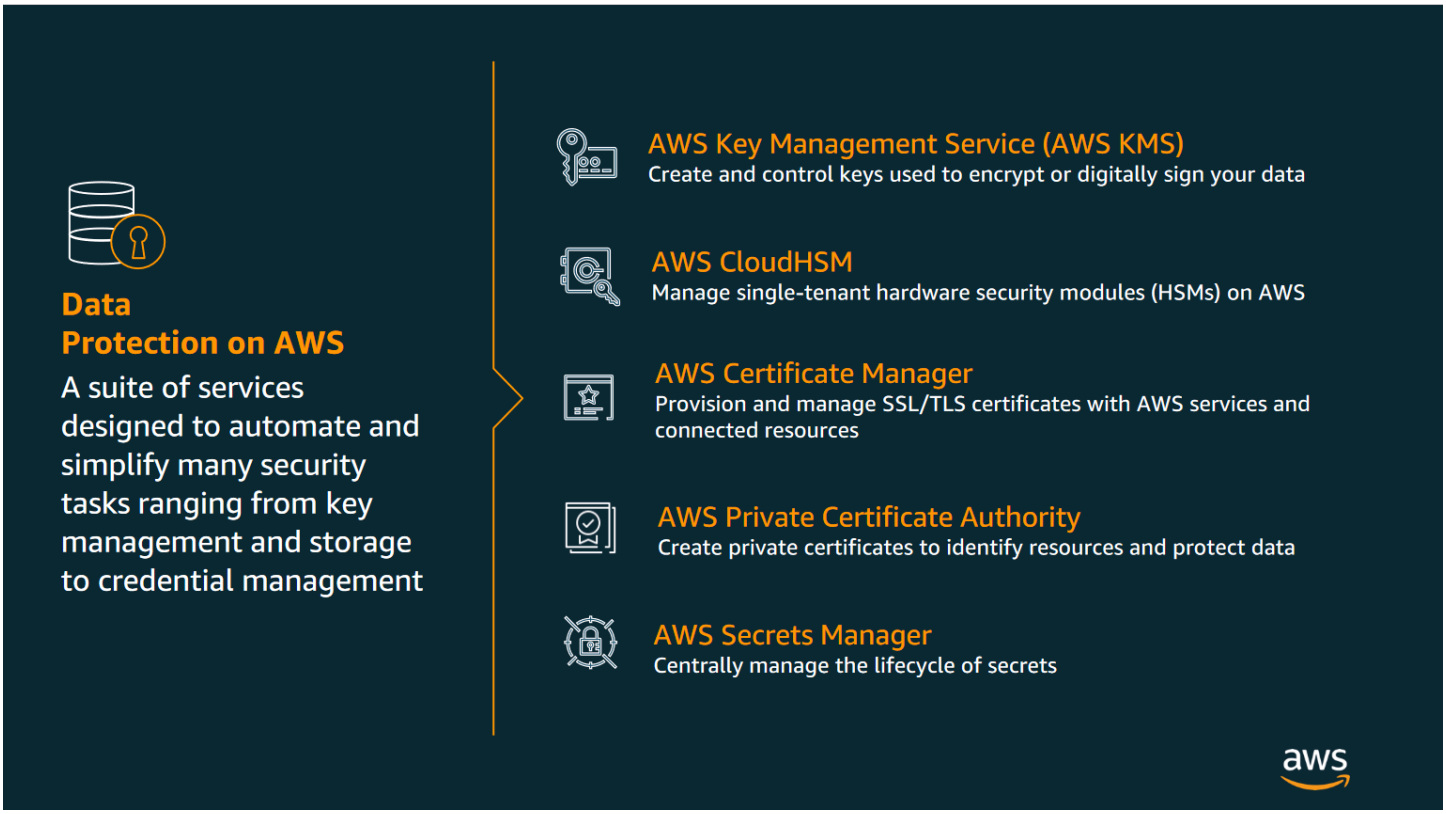
密码学是云计算安全的基石，有助于确保数据的机密性、完整性和真实性。在云环境中，敏感数据可能会穿过公共网络并驻留在共享基础设施上，这使得强大的加密措施对于防止未经授权的访问或篡改至关重要。

AWS 提供全面的加密服务，用于保护数据、管理加密密钥和保护敏感信息。其中包括用于集中密钥管理的 AWS Key Management Service (KMS)、 AWS CloudHSM 用于 PKCS11 应用程序和专用硬件安全模块，以及 AWS Encryption SDK 用于客户端加密的 (KMS)。 AWS Secrets Manager 是一项服务，使您能够在数据库凭证、API 密钥和其他密钥的整个生命周期中安全地存储、管理和检索敏感信息。AWS Certificate Manager (ACM) 简化了预置、管理和部署供使用的公开信任的传输层安全 (TLS) 证书的过程。 AWS 服务 AWS Private Certificate Authority (PCA) 允许您为内部资源生成和分发 x509 证书。

该指南旨在帮助您选择最适合您的需求和组织的 AWS 加密服务和工具。

以下视频是介绍密码学最佳实践的两分钟演示片段。

明白



选择正确的 AWS 加密服务取决于您的具体用例、数据安全要求、合规义务和操作偏好，如下表所示。

Key management

如果您需要安全地管理加密密钥，请考虑使用密 AWS 钥管理服务 (KMS)。它允许您创建、轮换和管理与其他 AWS 服务密钥集成的加密密钥。KMS 使用 FIPS 验证 HSMs 来帮助您满足合规性要求，并保证 KMS 公开的加密原语的实现的正确性。某些应用程序需要某些加密功能或应用程序接口，这些功能或应用程序接口仅适用于传统 HSM，并在云中 AWS CloudHSM 提供专用的硬件安全模块 (HSMs)，使您可以完全控制加密密钥和操作。

Data encryption

为了加密客户详细信息或知识产权等敏感数据， AWS KMS 它与 AWS 存储、数据库和消息服务（例如 S3、RDS 或 EBS）紧密集成。如果您需要客户端加密，则 AWS Encryption SDK 是一个开源库，可让您在将应用程序中的数据发送到云端之前轻松对其进行加密。

Secure communications

为了保护传输中的数据， AWS Certificate Manager (ACM) 简化了公众信任的 TLS 证书的管理。使用它来声明面向互联网的应用程序的身份，并促进对应用程序、用户和云服务之间的通信进行加

密，而不必担心证书续订。对于内部应用程序，您可以使用 AWS 私有证书颁发机构 (PCA) 为内部资源（包括客户端和服务器）生成和分发 x509 证书。

Secrets and credentials management

要安全地存储和检索应用程序密钥，例如数据库凭证、API 密钥或证书，请考虑 AWS Secrets Manager。它提供自动密钥轮换和精细的访问控制。或者， AWS Systems Manager Parameter Store 是管理非敏感配置的低成本选项，可以与集成。 AWS Secrets Manager

Compliance and auditing

对于监管合规工作，请考虑 AWS KMS AWS CloudHSM 并帮助确保加密标准得到满足。 AWS Artifactic 是一个自助服务门户，可按需访问的安全和合规报告，例如 ISO 认证和 SOC 报告，还可以查看和接受商业伙伴附录 (BAA) 等协议。 AWS您还可以使用诸如 AWS Config、 AWS Security Hub、和之类的服务 AWS Audit Manager 来监控合规性，并生成相应的工件供您自己使用或利益相关者使用。

在 AWS 加密服务之间进行选择时，请考虑以下要求。

要求	服务
省力，完全托管	AWS KMS 或者 AWS Secrets Manager
需要 KMS 不支持的特定应用程序接口或加密算法	AWS CloudHSM
Encrypting/decrypting 应用程序中的数据	AWS Encryption SDK
简化的公共 TLS 证书管理	AWS Certificate Manager
密钥管理	AWS Secrets Manager

通过将您的要求与这些选项保持一致，您可以实施针对您的安全和运营需求量身定制的加密解决方案。

考虑一下

选择正确的 AWS 加密服务需要了解您的特定安全、操作和合规需求。 AWS 提供各种加密服务，每种服务都旨在解决不同的用例，从密钥管理到数据加密和安全通信。要做出明智的决定，您应根据几个关键标准评估您的需求，包括您的用例、控制和灵活性需求、合规义务、成本考虑因素以及与的集成 AWS 服务。这些标准将帮助您将选择与组织的安全目标和操作工作流程保持一致。

Use case

考虑一下您需要加密服务的用途：数据加密、密钥管理、安全通信或机密管理。例如， AWS KMS 非常适合集成到加密中 AWS 服务，同时 AWS CloudHSM 适合需要某些加密功能、应用程序接口或单租户 HSM 的组织，通常是出于严格的合规性或特定的应用程序需求。明确目的可以确保您选择适合自己需求的服务，同时优化功能和成本。

Control and flexibility

评估您对加密操作所需的控制级别。诸如多租户 HSM 的托管 AWS KMS 服务易于使用，管理开销最小，同时保持对密钥材料的完全控制。相比之下， AWS CloudHSM 它为特定的应用程序、加密或合规性需求提供了单租户模式。

Compliance requirements

如果您在受监管的行业中运营，请确保该服务符合 GDPR、PCI DSS 或 HIPAA 等标准。 AWS KMS 并且 AWS CloudHSM 都获得了 FIPS 140-2 三级认证。选择满足您的非功能要求的服务有助于保持信任，并可能避免潜在的法律或经济处罚。

Cost considerations

根据服务的定价模型评估您的预算。 AWS KMS 在满足一般加密需求方面具有成本效益，但由于使用了专用硬件，则会 AWS CloudHSM 产生更高的成本。了解成本影响有助于您优化安全支出。

Integration with AWS ecosystem

如果您大量使用 AWS 服务，请优先考虑与 S3、RDS AWS KMS 或 Lambda 无缝集成的加密解决方案，例如或 ACM。这可确保更流畅的工作流程并减少开发工作量。集成功能可以显著提高运营效率。

选择

选择正确的 AWS 加密服务需要了解您的特定安全、操作和合规需求。 AWS 提供各种加密服务，每种服务都旨在解决不同的用例，从密钥管理到数据加密和安全通信。要做出明智的决定，您应根据几个关键标准评估您的需求，包括您的用例、控制和灵活性需求、合规义务、成本考虑因素以及与的集成 AWS 服务。这些标准将帮助您将选择与组织的安全目标和操作工作流程保持一致。

目标用例	你什么时候会用它？	推荐服务
密钥管理	安全地创建、轮换和管理与其他密钥集成的加密密钥 AWS 服务	AWS KMS
密钥管理	用于特定的应用程序集成或加密原语	AWS CloudHSM
数据加密	实施客户端加密以保护敏感数据，例如客户详细信息或知识产权。	AWS Encryption SDK AWS 数据库加密 SDK
安全通信	保护传输中的数据并简化 SSL/TLS 证书管理。	AWS Certificate Manager AWS Private CA
机密和凭据管理	安全地存储和检索应用程序密钥，例如数据库凭证、API 密钥或证书。	AWS Secrets Manager AWS 参数存储

使用

现在，您应该清楚地了解每种 AWS 加密服务的用途，以及哪些服务可能适合您。

为了探索如何使用每种可用的 AWS 密码学服务并了解有关这些服务的更多信息，我们提供了探索每种服务的工作原理的途径。以下部分提供了指向深入文档、动手教程和其他资源的链接，以帮助您入门。

AWS Certificate Manager

- 开始使用 AWS Certificate Manager

  开始使用 AWS Certificate Manager，包括同时使用公有和私有证书。

  浏览指南
- 的最佳实践 AWS Certificate Manager

  查看可以帮助您 AWS Certificate Manager 更有效地使用的建议。

浏览指南

- AWS Certificate Manager 常见问题

  查看 AWS Certificate Manager (ACM) 常见问题解答页面，详细了解有关 ACM 特性、功能和用法的常见问题。它涵盖了诸如 ACM 管理的证书类型 AWS 服务、与其他证书的集成以及配置和管理 SSL/TLS 证书的指导等主题。

  探索 FAQs

AWS CloudHSM

- 开始使用 AWS CloudHSM

  在中学习如何创建、初始化和激活集群 AWS CloudHSM。在您完成这些过程后，您即可管理用户、管理集群并使用包含的软件库来执行加密操作。

  浏览指南

- 的最佳实践 AWS CloudHSM

  探索管理和监控 AWS CloudHSM 集群的最佳实践。

  浏览指南

- AWS CloudHSM 定价

  查看定价页面以了解 AWS CloudHSM 定价。无需预付费用即可使用 AWS CloudHSM。使用 AWS CloudHSM，在终止 HSM 之前，您需要为启动的每个 HSM 支付每小时费用。本指南提供每个 AWS 地区的小时费率。

  浏览定价页面

- AWS CloudHSM 常见问题

  查看 AWS CloudHSM 常见问题解答页面，详细了解常见问题 AWS CloudHSM，包括其功能、定价、配置、安全性、合规性、性能以及与第三方应用程序的集成。

  探索 FAQs

AWS Encryption SDK

- 开始使用 AWS Encryption SDK

  了解如何 AWS Encryption SDK 搭配使用 AWS KMS。

  浏览指南
- 的最佳实践 AWS Encryption SDK

  请查看 “ AWS Encryption SDK 最佳实践” 页面，获取有关如何有效利用 AWS Encryption SDK 来保护数据的指导。遵守这些最佳实践有助于确保加密数据的机密性和完整性。

  浏览指南
- AWS Encryption SDK 常见问题

  查看 AWS Encryption SDK 常见问题解答页面，获取有关常见问题的答案 AWS Encryption SDK，包括其功能、支持的编程语言和最佳实施实践。

  浏览常见问题解答

AWS Database Encryption SDK

- 开始使用 AWS 数据库加密 SDK

  了解如何将 AWS 数据库加密 SDK 与配合使用 AWS KMS。

  浏览指南
- 配置 AWS 数据库加密 SDK

  了解如何配置 AWS 数据库加密 SDK，包括选择编程语言和选择包装密钥。

  浏览指南

AWS KMS

- 开始使用 AWS KMS

  了解如何创建 KMS 密钥，包括对称和非对称加密密钥。

  浏览指南

- 的最佳实践 AWS KMS

  了解以下方面的加密最佳实践 AWS KMS。

  浏览指南

- AWS KMS 定价

  查看 AWS Key Management Service (KMS) 定价页面，了解与使用相关的费用 AWS KMS，包括密钥存储费用、API 请求和自定义密钥存储库等可选功能。

  浏览定价页面

- AWS KMS 常见问题

  AWS Key Management Service (KMS) FAQ 页面提供了有关常见问题的详细答案 AWS KMS，包括其功能、安全措施、计费惯例、密钥管理选项以及与其他选项的集成 AWS 服务。

  探索 FAQs

AWS Private CA

- 的最佳实践 AWS Private CA

  查看可以帮助您 AWS Private CA 有效使用的建议。

  浏览指南

- 开始使用 AWS Private CA

  学习如何以编程方式创建和激活根 CA。

  浏览指南

- AWS Private CA 定价

  查看与运营私有证书 CAs 和颁发私有证书相关的成本。

  浏览定价页面

- AWS Private CA 常见问题

  获取常见问题的详细答案 AWS Private CA，包括其功能、定价、配置、安全性、合规性、性能以及与其他产品的集成 AWS 服务。

探索 FAQs

AWS Secrets Manager

- 开始使用 AWS Secrets Manager

  学习如何创建 AWS Secrets Manager 密钥。

  浏览指南
- 的最佳实践 AWS Secrets Manager

  了解使用时应考虑的最佳实践 AWS Secrets Manager。

  浏览指南
- AWS Secrets Manager 定价

  查看定 AWS Secrets Manager 价页面，了解与安全存储、管理和检索数据库凭证和 API 密钥等密钥相关的费用。

  浏览定价页面
- AWS Secrets Manager 常见问题

  查看 AWS Secrets Manager 常见问题解答页面，详细了解相关常见问题 AWS Secrets Manager，包括其功能、安全措施、定价和集成功能。

  探索 FAQs

Explore

- 研究和资源

  浏览有关密码学的 AWS 博客、视频和工具。

  查看资源
- 视频

  观看 AWS 开发者频道中的这些视频 YouTube ，进一步开发和完善您的加密策略。

  浏览密码学视频

文档历史记录

下表描述了本决策指南的重要更改。要获取有关本指南更新的通知，您可以订阅 RSS feed。

变更	说明	日期
初次发布	指南首次出版。	2025 年 1 月 31 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。