AWS 決策指南

選擇 AWS 密碼編譯服務

選擇 AWS 密碼編譯服務: AWS 決策指南

Table of Contents

選擇 AWS 密碼編譯服務

採取第一步

用途	協助判斷哪些 AWS 密碼編譯服務最適合您的組織。
上次更新	2025 年 1 月 31 日
涵蓋的服務	• AWS Certificate Manager • AWS CloudHSM • AWS 資料庫加密 SDK • AWS Encryption SDK • AWS KMS • AWS 私有 CA • AWS Secrets Manager
相關指南	選擇 AWS 安全、身分和控管服務

簡介

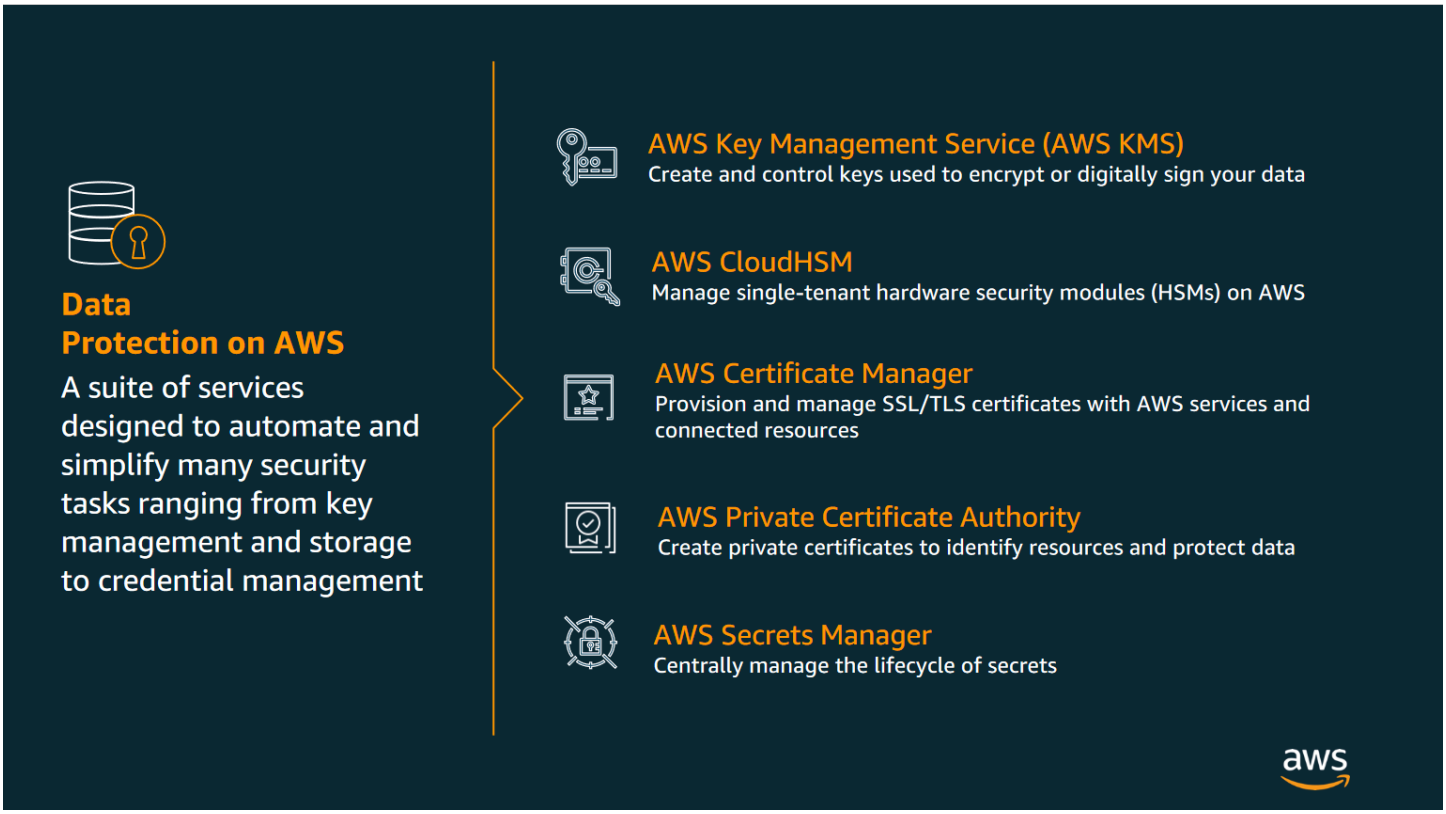
密碼編譯是雲端運算安全性的基石，有助於確保資料機密性、完整性和真實性。在雲端環境中，敏感資料可能會周遊公有網路，並位於共用基礎設施上，使得強大的密碼編譯措施對於防止未經授權的存取或竄改至關重要。

AWS 提供全方位的密碼編譯服務，以保護資料、管理加密金鑰和保護敏感資訊。這些包括用於集中式金鑰管理的 AWS Key Management Service (KMS)、 AWS CloudHSM 用於 PKCS11 應用程式和專用硬體安全模組的 ，以及 AWS Encryption SDK 用於用戶端加密的 。 AWS Secrets Manager 是一種服務，可讓您在整個生命週期安全地存放、管理和擷取敏感資訊，例如資料庫憑證、API 金鑰和其他秘密。 AWS Certificate Manager (ACM) 可簡化佈建、管理和部署可公開信任傳輸層安全 (TLS) 憑證的程序，以搭配 使用 AWS 服務。(PCA) AWS 私有憑證授權單位 可讓您為內部資源產生和分發 x509 憑證。

本指南旨在協助您選擇最適合您需求和組織的 AWS 密碼編譯服務和工具。

以下影片是介紹密碼編譯最佳實務的簡報兩分鐘區段。

了解



選擇正確的 AWS 密碼編譯服務取決於您的特定使用案例、資料安全需求、合規義務和操作偏好設定，如下表所述。

Key management

如果您需要安全地管理加密金鑰，請考慮 AWS Key Management Service (KMS)。它可讓您建立、輪換和管理與其他 整合的密碼編譯金鑰 AWS 服務。KMS 使用 FIPS 驗證HSMs 來協助您符合合規程序，並保證 KMS 公開的密碼編譯基礎實作正確性。有些應用程式需要特定密碼編譯函數或應用程式介面，這些功能僅適用於傳統 HSM，並在雲端 AWS CloudHSM 中提供專用硬體安全模組 (HSMs)，可讓您完全控制密碼編譯金鑰和操作。

Data encryption

為了加密敏感資料，例如客戶詳細資訊或智慧財產權， AWS KMS 與 AWS 儲存、資料庫和簡訊服務 （ 例如 S3、RDS 或 EBS) 緊密整合。如果您需要用戶端加密， AWS Encryption SDK 是一種開放原始碼程式庫，可讓您在將資料傳送到雲端之前，輕鬆地加密應用程式中的資料。

Secure communications

為了保護傳輸中的資料， AWS Certificate Manager (ACM) 簡化了公開信任 TLS 憑證的管理。使用它來宣告面向網際網路的應用程式身分，並促進應用程式、使用者和雲端服務之間的加密通訊，而不必擔心憑證續約。對於內部應用程式，您可以使用 AWS 私有憑證授權機構 (PCA) 為您的內部資源產生和分配 x509 憑證，包括用戶端和伺服器。

Secrets and credentials management

若要安全地存放和擷取應用程式秘密，例如資料庫登入資料、API 金鑰或憑證，請考慮 AWS Secrets Manager。它提供自動秘密輪換和精細存取控制。或者， AWS Systems Manager 參數存放區是管理非敏感組態的低成本選項，可與 整合 AWS Secrets Manager。

Compliance and auditing

對於法規合規工作，請考慮 AWS KMS 和 AWS CloudHSM ，以協助確保符合加密標準。 AWS Artifact 是一種自助式入口網站，可讓您隨需存取 ISO 認證和 SOC 報告等 AWS安全和合規報告，以及檢閱和接受商業夥伴增補合約 (BAA) 等協議的能力。您也可以使用 AWS Config 等服務 AWS Security Hub CSPM來 AWS Audit Manager 監控合規性，並產生適當的成品供您自己使用或利益相關者使用。

在 AWS 密碼編譯服務之間進行選擇時，請考慮下列要求。

需求	服務
工作量低、全受管	AWS KMS 或 AWS Secrets Manager
需要 KMS 不支援的特定應用程式界面或密碼編譯演算法	AWS CloudHSM
加密/解密應用程式中的資料	AWS Encryption SDK
簡化的公有 TLS 憑證管理	AWS Certificate Manager
秘密管理	AWS Secrets Manager

透過將您的需求與這些選項保持一致，您可以實作專為您的安全和操作需求量身打造的密碼編譯解決方案。

考慮

選擇正確的 AWS 密碼編譯服務涉及了解您的特定安全、操作和合規需求。 AWS 提供各種密碼編譯服務，每個服務旨在解決不同的使用案例，從金鑰管理到資料加密和安全通訊。若要做出明智的決策，您應該根據數個關鍵條件來評估您的需求，包括您的使用案例、控制和彈性需求、合規義務、成本考量以及與 的整合 AWS 服務。這些條件將協助您將選擇與組織的安全目標和操作工作流程保持一致。

Use case

考慮您需要的密碼編譯服務用途：資料加密、金鑰管理、安全通訊或秘密管理。例如， AWS KMS 非常適合整合到 的加密 AWS 服務，而 AWS CloudHSM 適合需要特定密碼編譯功能、應用程式界面或單一租用戶 HSM 的組織，通常是由於嚴格的合規或特定應用程式需求。釐清用途可確保您選擇適合您需求的服務，同時最佳化功能和成本。

Control and flexibility

評估您需要對密碼編譯操作的控制層級。受管服務，例如透過多租用戶 HSM AWS KMS 以最少的管理開銷提供易用性，同時保持對金鑰材料的完全控制。相反地， 為特定應用程式、密碼編譯或合規需求 AWS CloudHSM 提供單一租戶模型。

Compliance requirements

如果您在受管制的產業中營運，請確保服務符合 GDPR、PCI DSS 或 HIPAA 等標準， AWS KMS 並且 AWS CloudHSM 都通過 FIPS 140-2 第 3 級認證。選擇符合您非功能需求的服務有助於維持信任，並可能避免潛在的法律或財務處罰。

Cost considerations

根據服務的定價模型來評估您的預算。 AWS KMS 符合一般加密需求的成本效益，同時因為專用硬體而 AWS CloudHSM 產生更高的成本。了解成本影響可協助您最佳化安全支出。

Integration with AWS ecosystem

如果您大量使用 AWS 服務，請優先考慮與 S3、RDS AWS KMS 或 Lambda 無縫整合的密碼編譯解決方案，例如 或 ACM。這可確保更順暢的工作流程並減少開發工作。整合功能可以大幅提升營運效率。

選擇

選擇正確的 AWS 密碼編譯服務涉及了解您的特定安全、操作和合規需求。 AWS 提供各種密碼編譯服務，每個服務旨在解決不同的使用案例，從金鑰管理到資料加密和安全通訊。若要做出明智的決策，您

應該根據數個關鍵條件來評估您的需求，包括您的使用案例、控制和彈性需求、合規義務、成本考量以及與 的整合 AWS 服務。這些條件將協助您將選擇與組織的安全目標和操作工作流程保持一致。

目標使用案例	您會何時使用它？	建議的服務
金鑰管理	安全地建立、輪換和管理與其他 整合的密碼編譯金鑰 AWS 服務	AWS KMS
金鑰管理	對於特定應用程式整合或密碼編譯基本概念	AWS CloudHSM
資料加密	實作用戶端加密來保護敏感資料，例如客戶詳細資訊或智慧財產權。	AWS Encryption SDK AWS 資料庫加密 SDK
安全通訊	保護傳輸中的資料，並簡化 SSL/TLS 憑證的管理。	AWS Certificate Manager AWS 私有 CA
秘密和登入資料管理	安全地存放和擷取應用程式秘密，例如資料庫登入資料、API 金鑰或憑證。	AWS Secrets Manager AWS 參數存放區

使用

您現在應該清楚了解每個 AWS 密碼編譯服務的功能，以及哪些功能可能適合您。

為了探索如何使用和進一步了解每個可用的 AWS 密碼編譯服務，我們提供了途徑來探索每個服務的運作方式。下列各節提供深入文件、實作教學課程和其他資源的連結，協助您開始使用。

AWS Certificate Manager

- 開始使用 AWS Certificate Manager

  開始使用 AWS Certificate Manager，包括使用公有和私有憑證。

  探索指南
- 的最佳實務 AWS Certificate Manager

檢閱可協助您更有效地使用 AWS Certificate Manager 的建議。

探索指南

- AWS Certificate Manager 常見問答集

  檢閱 AWS Certificate Manager (ACM) 常見問答集頁面，以取得有關 ACM 功能和用量常見問題的詳細解答。它涵蓋諸如 ACM 管理的憑證類型、與其他 整合 AWS 服務，以及佈建和管理 SSL/TLS 憑證的指引等主題。

  探索FAQs

AWS CloudHSM

- 開始使用 AWS CloudHSM

  了解如何在 中建立、初始化和啟用叢集 AWS CloudHSM。完成這些程序之後，您就能管理使用者、管理叢集，以及使用隨附的軟體程式庫執行密碼編譯操作。

  探索指南

- 的最佳實務 AWS CloudHSM

  探索管理和監控叢集 AWS CloudHSM 的最佳實務。

  探索指南

- AWS CloudHSM 定價

  檢閱定價頁面以了解 AWS CloudHSM 定價。無需預付費用即可使用 AWS CloudHSM。使用 時 AWS CloudHSM，您需要為啟動的每個 HSM 支付每小時費用，直到您終止 HSM 為止。本指南提供每個 AWS 區域的每小時費率。

  探索定價頁面

- AWS CloudHSM 常見問答集

  檢閱 AWS CloudHSM 常見問答集頁面以取得常見問題的詳細解答 AWS CloudHSM，包括其功能、定價、佈建、安全性、合規性、效能，以及與第三方應用程式的整合。

  探索FAQs

AWS Encryption SDK

- 開始使用 AWS Encryption SDK

  了解如何 AWS Encryption SDK 搭配 使用 AWS KMS。

  探索指南

- 的最佳實務 AWS Encryption SDK

  檢閱 AWS Encryption SDK 最佳實務頁面，以取得有效使用 AWS Encryption SDK 來保護資料的指導方針。遵守這些最佳實務有助於確保加密資料的機密性和完整性。

  探索指南

- AWS Encryption SDK 常見問答集

  檢閱 AWS Encryption SDK 常見問答集頁面以取得有關 的常見問題解答 AWS Encryption SDK，包括其功能、支援的程式設計語言，以及實作的最佳實務。

  探索常見問答集

AWS Database Encryption SDK

- 資料庫 AWS 加密 SDK 入門

  了解如何搭配 AWS 資料庫加密 SDK 使用 AWS KMS。

  探索指南

- 設定 AWS 資料庫加密 SDK

  了解如何設定 AWS 資料庫加密 SDK，包括選取程式設計語言和包裝金鑰。

  探索指南

AWS KMS

- 開始使用 AWS KMS

  了解如何建立 KMS 金鑰，包括對稱和非對稱加密金鑰。

  探索指南

- 的最佳實務 AWS KMS

  了解 的加密最佳實務 AWS KMS。

  探索指南

- AWS KMS 定價

  檢閱 AWS Key Management Service (KMS) 定價頁面，以了解與使用 相關的成本 AWS KMS，包括金鑰儲存、API 請求和自訂金鑰存放區等選用功能的費用。

  探索定價頁面

- AWS KMS 常見問答集

  AWS Key Management Service (KMS) 常見問答集頁面提供常見問題的詳細解答 AWS KMS，包括其功能、安全措施、帳單實務、金鑰管理選項，以及與其他 整合 AWS 服務。

  探索FAQs

AWS 私有 CA

- 的最佳實務 AWS 私有 CA

  檢閱可協助您有效使用 AWS 私有 CA 的建議。

  探索指南

- 開始使用 AWS 私有 CA

  了解如何以程式設計方式建立和啟用根 CA。

  探索指南

- AWS 私有 CA 定價

  檢閱與操作私有 CAs和發行私有憑證相關的成本。

  探索定價頁面

- AWS 私有 CA 常見問答集

  取得有關 的常見問題的詳細解答 AWS 私有 CA，包括其功能、定價、佈建、安全性、合規、效能，以及與其他 整合 AWS 服務。

探索FAQs

AWS Secrets Manager

- 開始使用 AWS Secrets Manager

  了解如何建立 AWS Secrets Manager 秘密。

  探索指南
- 的最佳實務 AWS Secrets Manager

  了解使用 時應考慮的最佳實務 AWS Secrets Manager。

  探索指南
- AWS Secrets Manager 定價

  檢閱 AWS Secrets Manager 定價頁面，以了解與安全儲存、管理和擷取資料庫登入資料和 API 金鑰等秘密相關的成本。

  探索定價頁面
- AWS Secrets Manager 常見問答集

  檢閱 AWS Secrets Manager 常見問答集頁面以取得常見問題的詳細解答 AWS Secrets Manager，包括其功能、安全措施、定價和整合功能。

  探索FAQs

探索

- 研究和資源

  探索密碼編譯的 AWS 部落格、影片和工具。

  檢閱資源
- 影片

  從 YouTube 上的 AWS 開發人員頻道觀看這些影片，以進一步開發和完善您的密碼編譯策略。

  探索密碼編譯影片

文件歷史記錄

下表說明此決策指南的重要變更。如需有關本指南更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	指南首先發佈。	2025 年 1 月 31 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。