的加密最佳實務和功能 AWS 服務

AWS 方案指引

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 方案指引: 的加密最佳實務和功能 AWS 服務

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介 1
目標對象 1
密碼編譯方法 2
AWS 密碼編譯基礎 2
密碼編譯演算法 2
中的建議密碼編譯演算法 AWS 3
非對稱密碼編譯 3
對稱密碼編譯 4
其他密碼編譯函數 4
在 中使用的密碼編譯 AWS 服務 5
一般加密最佳實務 6
資料分類 6
加密傳輸中的資料 6
靜態資料加密 7
的加密最佳實務 AWS 服務 8
AWS CloudTrail 8
Amazon DynamoDB 9
Amazon EC2 和 Amazon EBS 10
Amazon ECR 11
Amazon ECS 12
Amazon EFS 13
Amazon EKS 14
AWS Encryption SDK 15
AWS KMS 16
AWS Lambda 18
Amazon RDS 19
AWS Secrets Manager 20
Amazon S3 21
Amazon VPC 22
資源 24
文件歷史紀錄 25
..... xxvi

的加密最佳實務和功能 AWS 服務

Kurt Kumar，Amazon Web Services

2026 年 2 月 (文件歷史記錄)

加密是保護數位時代敏感資料的基本網路安全工具。隨著組織越來越依賴資料來推動其操作，包括生成式 AI 部署，透過強大的加密實務保護此寶貴資訊是全面資料保護策略的重要組成部分。本指南可協助您了解 提供的 AWS 加密原則和加密功能。

現代網路安全威脅包括資料外洩的風險，也就是未經授權存取您的資訊資產會導致資料遺失的情況。資料是每個組織唯一的商業資產。它可以包括客戶資訊、業務計畫、設計文件或程式碼。保護企業意味著保護資料。

即使發生違規，資料加密也有助於保護您的商業資料。它提供一層防禦，防止意外洩露。若要存取 AWS 雲端中的加密資料，使用者需要使用金鑰進行解密的許可，並且需要使用資料所在服務的許可。如果沒有這兩個許可，使用者將無法解密和檢視資料。

一般而言，您可以加密三種類型的資料。傳輸中的資料是在您的網路中主動移動的資料，例如在網路資源之間移動。靜態資料是靜止且處於休眠狀態的資料，例如儲存中的資料。範例包括區塊儲存、物件儲存、資料庫、存檔和物聯網 (IoT) 裝置。使用中的資料是指應用程式或服務正在積極處理或使用的資料。透過在使用點保護資料，組織可以協助降低意外揭露的風險。

本指南討論加密傳輸中資料和靜態資料的考量事項和最佳實務。它也會檢閱許多 中可用的加密功能和控制項 AWS 服務。您可以在 AWS 雲端 環境中的服務層級實作這些加密建議。

目標對象

本指南可供公共和私營部門的小型、中型和大型組織使用。無論您的組織處於評估和實作資料保護策略的初始階段，還是旨在增強現有安全控制，本指南中概述的建議最適合下列受眾：

- 為企業制定政策的執行官，例如執行長 (CEO)、技術長 (CTO)、資訊長 (CIO) 和資訊安全長 (CISO)
- 負責制定技術標準的技術官，例如技術副總裁和總監
- 負責下列事項的企業利害關係人和應用程式擁有者：
  - 評估風險狀態、資料分類和保護需求
  - 監控既定組織標準的合規情況
- 合規、內部稽核和治理官，負責監控合規政策的遵守情況，包括法定和自願合規管轄範圍

AWS 密碼編譯的方法

密碼編譯演算法是數學建構，旨在提供安全服務，例如機密性（加密）、真實性（訊息驗證碼和數位簽章）和不可否認性（數位簽章）。如果您是初次使用密碼編譯、加密和相關術語，建議您先閱讀關於資料加密，然後再繼續本指南。

AWS 密碼編譯基礎

密碼編譯是 for. AWS 服務 support 安全的重要部分 AWS。支援傳輸中、靜態或記憶體中資料的加密。 您可以在我們的部落格文章中，進一步了解對創新 AWS 的承諾，以及投資對主權和加密功能的額外控制，宣布AWS 數位主權承諾。

AWS 遵循共同責任模型來保護您的資料。 AWS 服務 使用符合業界標準的受信任密碼編譯演算法，並促進互通性。這些演算法由公有標準機構和學術研究進行審核。政府、產業和學術界廣泛接受相關標準。

AWS 預設為高保證密碼編譯實作，並偏好有效率的硬體最佳化解決方案。我們的密碼編譯核心程式庫 AWS-LC 可作為透明度和整個產業重複使用的開放原始碼。LC AWS中的許多密碼編譯演算法實作都經過正式驗證，以提高對數個不同平台中實作正確性和安全性的保證。此程式庫也經過 NIST 的 FIPS-140 程式驗證。

密碼編譯演算法

我們定義三種類型的密碼編譯演算法：

- 非對稱密碼編譯使用一對金鑰：用於加密（或驗證）的公有金鑰，以及用於解密（或簽署）的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰的存取應該受到高度限制。 AWS 服務 支援或計劃支援量子後演算法，例如 ML-KEM 和 ML-DSA。 AWS 服務 也支援傳統的密碼編譯演算法，例如 RSA 和橢圓曲線密碼編譯 (ECC)。
- 對稱密碼編譯使用相同的金鑰來加密和解密，或驗證和驗證資料。 AWS 服務 通常會與 AWS Key Management Service (AWS KMS) 整合，以加密使用 AES-256 模式的靜態資料。
- 其他密碼編譯函數會與非對稱和對稱密碼編譯搭配使用，以針對機密性、完整性、身分驗證和不可否認應用程式建置安全、實用的通訊協定。範例包括雜湊函數和金鑰衍生函數。

中的建議密碼編譯演算法 AWS

下表摘要說明 AWS 視為適合跨其服務進行部署以保護資料的加密演算法、模式和金鑰大小。隨著密碼編譯標準演進，本指南將隨著時間演進。

服務中可用的演算法可能會有所不同，並會在每個服務的文件中說明。如果您需要適用於已核准演算法的軟體程式庫實作，請檢查它是否包含在最新版本的 AWS-LC 程式庫中。

演算法已核准在下列兩種類別之一 AWS 下用於 ：

- 偏好的演算法符合 AWS 安全性和效能標準。
- 可接受的演算法可用於某些應用程式的相容性，但不建議使用。

非對稱密碼編譯

下表列出適合 AWS 在 內用於加密、金鑰協議和數位簽章的非對稱演算法。

類型	演算法	狀態
加密	RSA-OAEP (≥2048 位元模數)	可接受
加密	HPKE (P-256 或 P-384、HKF 和 AES-GCM)	可接受
金鑰協議	ML-KEM-768 或 ML-KEM-1024	偏好 （ 抗量子 ）
金鑰協議	ECDH(E) 搭配 P-256, P-384, P-521 或 X25519	可接受
金鑰協議	ECDH(E) 搭配 brainpool P256r1, brainpoolP384r1 或 brainpoolP512r1	可接受
Signatures (簽章)	ML-DSA-65 或 ML-DSA-87	偏好 （ 抗量子 ）
Signatures (簽章)	SLH-DSA	可接受 （ 抗量子 ）

Signatures (簽章)	ECDSA 搭配 P-256, P-384, P-521 或 Ed25519	可接受
Signatures (簽章)	RSA (≥2048 位元模數）	可接受

對稱密碼編譯

下表列出適合在 內用於加密、已驗證加密和金鑰包裝 AWS 的對稱演算法。

類型	演算法	狀態
已驗證的加密	AES-GCM-256	偏好
已驗證的加密	AES-GCM-128	可接受
已驗證的加密	ChaCha20/Poly1305	可接受
加密模式	AES-XTS-256 （用於區塊儲存）	偏好
加密模式	AES-CBC/CTR （未驗證模式）	可接受
金鑰包裝	AES-GCM-256	偏好
金鑰包裝	具有 256 位元金鑰的 AES-KW 或 AES-KWP	可接受

其他密碼編譯函數

下表列出視為適合在 內用於雜湊、金鑰衍生和訊息身分驗證 AWS 的演算法。

類型	演算法	狀態
雜湊	SHA-384	偏好
雜湊	SHA-256	可接受

雜湊	SHA3	可接受
金鑰衍生	HKDF_Expand 或 HKDF 搭配 SHA-256	偏好
金鑰衍生	使用 HMAC-SHA-256 的計數器模式 KDF	可接受
訊息驗證碼	HMAC-SHA-384	偏好
訊息驗證碼	HMAC-SHA-256	可接受
訊息驗證碼	KMAC	可接受
密碼雜湊	使用 SHA384 加密	偏好
密碼雜湊	PBKDF2	可接受

在 中使用的密碼編譯 AWS 服務

AWS 服務 倚賴經審核演算法的安全、開放原始碼實作來保護您的資料。演算法的特定選擇和組態會因服務而異。有些 AWS 工具和服務使用特定的演算法。在其他情況下，您可以在支援的演算法和金鑰長度之間進行選擇，也可以使用建議的預設值。

AWS 密碼編譯服務符合各種密碼編譯安全標準，因此您可以符合政府或產業法規。如需 AWS 服務 符合資料安全標準的完整清單，請參閱AWS 合規計劃。

一般加密最佳實務

本節提供在 中加密資料時套用的建議 AWS 雲端。這些一般加密最佳實務並非專屬 AWS 服務。本節包含下列主題：

- 資料分類
- 加密傳輸中的資料
- 靜態資料加密

資料分類

資料分類是根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 Well-Architected Framework 中 AWS 安全支柱的元件。類別可能包括高度機密、機密、非機密和公有，但分類層及其名稱可能因組織而異。如需資料分類程序、考量事項和模型的詳細資訊，請參閱資料分類 (AWS 白皮書）。

將資料分類後，您可以根據每個類別所需的保護層級為您的組織建立加密策略。例如，您的組織可能會決定高度機密的資料應使用非對稱加密，且公有資料不需要加密。如需有關設計加密策略的詳細資訊，請參閱為靜態資料建立企業加密策略。雖然該指南中的技術考量事項和建議特定於靜態資料，但您也可以使用分階段方法為傳輸中的資料建立加密策略。

加密傳輸中的資料

AWS 區域 透過 AWS 全球網路在 之間傳輸的所有資料，都會 AWS 在離開 AWS 安全設施之前由 自動加密。 會 AWS 加密可用區域之間的所有流量。

對於流經工作負載的資料，下列是在 中加密傳輸中資料的一般最佳實務 AWS 雲端：

- 根據您的資料分類、組織要求以及任何適用的法規或合規標準，為傳輸中的資料定義組織加密政策。我們強烈建議您對分類為高度機密或機密的傳輸中的資料進行加密。您的政策也可能視需要指定其他類別的加密，例如非機密或公有資料。
- 對傳輸中的資料進行加密時，我們建議使用已核准的密碼編譯演算法、區塊加密模式和金鑰長度，如加密政策中定義。我們進一步建議定期檢閱與 Application Load Balancer、Amazon API Gateway 資源、Amazon CloudFront 資源和 Amazon Virtual Private Cloud (Amazon VPC) 資源相關聯的 TLS 政策，以確保它們符合您目前的加密政策。

- 使用下列其中一項，加密公司網路和 AWS 雲端 基礎設施中資訊資產和系統之間的流量：
  - AWS Site-to-Site VPN 連線
  - AWS Site-to-Site VPN 和 AWS Direct Connect連線的組合，可提供 IPsec 加密的私有連線
  - Direct Connect 支援 MAC Security (MACsec) 將資料從公司網路加密到 Direct Connect 位置的連線
- 根據最低權限原則，識別受管憑證和 TLS 政策組態的存取控制政策。最低權限是授予使用者執行工作職能所需的最低存取權的安全最佳實務。如需有關套用最低權限許可的詳細資訊，請參閱 IAM 中的安全最佳實務和 IAM 政策的最佳實務。

靜態資料加密

Amazon Simple Storage Service (Amazon S3) 和 Amazon Elastic File System (Amazon EFS) 等所有資料 AWS 儲存服務提供加密靜態資料的選項。使用 256 位元進階加密標準 (AES-256) 區塊加密和 AWS 密碼編譯服務來執行加密，例如 AWS Key Management Service (AWS KMS) 或 AWS CloudHSM。

您可以根據資料分類、端對端加密需求或阻止您使用端對端加密的技術限制等因素，使用用戶端加密或伺服器端加密來加密資料：

- 用戶端加密是在目標應用程式或服務接收資料之前在本機加密資料的行為。 AWS 服務 收到加密的資料，但在加密或解密中未扮演任何角色。對於用戶端加密，您可以使用 AWS KMS、AWS Encryption SDK 或其他第三方加密工具或服務。
- 伺服器端加密是指接收資料的應用程式或服務在目的地加密資料的行為。對於伺服器端加密，您可以使用 AWS KMS 來加密整個儲存區塊。您也可以使用其他第三方加密工具或服務 (例如 LUKS) 在作業系統 (OS) 層級加密 Linux 檔案系統。

以下是在 AWS 雲端中對靜態資料進行加密時的一般最佳實務：

- 根據您的資料分類、組織要求以及任何適用的法規或合規標準，為靜態資料定義組織加密政策。如需詳細資訊，請參閱為靜態資料建立企業加密策略。我們強烈建議您對分類為高度機密或機密的靜態資料進行加密。您的政策也可能視需要指定其他類別的加密，例如非機密或公有資料。
- 對靜態資料進行加密時，我們建議使用已核准的密碼編譯演算法、區塊加密模式和金鑰長度。
- 根據最低權限原則識別加密金鑰的存取控制政策。

的加密最佳實務 AWS 服務

本節包含下列 的最佳實務和建議 AWS 服務：

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (Amazon EC2) 和 Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (Amazon RDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (Amazon VPC)

的加密最佳實務 AWS CloudTrail

AWS CloudTrail 可協助您稽核 AWS 帳戶的監管、合規、操作和風險。

請考慮此服務的下列加密最佳實務：

- CloudTrail 日誌應使用客戶受管 AWS KMS key進行加密。選擇位在與收到您日誌檔案之 S3 儲存貯體相同區域中的 KMS 金鑰。如需詳細資訊，請參閱更新追蹤以使用您的 KMS 金鑰。
- 作為額外的安全層，啟用追蹤的日誌檔案驗證。這可協助您確定日誌檔案在 CloudTrail 交付後是否已修改、刪除或未變更。如需說明，請參閱啟用 CloudTrail 的日誌檔案完整性驗證。
- 使用介面 VPC 端點可讓 CloudTrail 與其他 VPC 中的資源進行通訊，而無需周遊公有網際網路。如需詳細資訊，請參閱將 AWS CloudTrail 與介面 VPC 端點搭配使用。
- 將 `aws:SourceArn` 條件金鑰新增至 KMS 金鑰政策，可確保 CloudTrail 僅針對特定追蹤使用 KMS 金鑰。如需詳細資訊，請參閱設定 CloudTrail AWS KMS key 的政策。

- 在 中 AWS Config，實作cloud-trail-encryption-enabled AWS 受管規則，以驗證和強制執行日誌檔案加密。
- 如果 CloudTrail 設定為透過 Amazon Simple Notification Service (Amazon SNS) 主題傳送通知，請將 `aws:SourceArn` (或選用 `aws:SourceAccount`) 條件金鑰新增至 CloudTrail 政策陳述式，以防止未經授權的帳戶存取 SNS 主題。如需詳細資訊，請參閱適用於 CloudTrail 的 Amazon SNS 主題政策。
- 如果您使用的是 AWS Organizations，請建立組織線索，記錄 AWS 帳戶 該組織中 的所有事件。這包括組織中的管理帳戶和所有成員帳戶。如需詳細資訊，請參閱為組織建立追蹤。
- 建立適用於您存放公司資料之所有 AWS 區域 的線索，以記錄這些區域中 AWS 帳戶 的活動。當 AWS 啟動新區域時，CloudTrail 會自動包含新區域，並記錄該區域中的事件。

Amazon DynamoDB 的加密最佳實務

Amazon DynamoDB 是一項全受管 NoSQL 資料庫服務，可提供快速、可預期且可擴展的效能。每當資料儲存在耐用的媒體中時，DynamoDB 靜態加密會保護加密資料表中的資料：包括其主索引鍵、本機及全域次要索引、串流、全域資料表、備份和 DynamoDB Accelerator (DAX) 叢集。

根據資料分類要求，可以透過實作伺服器端或用戶端加密來維護資料機密性和完整性：

對於伺服器端加密，當您建立新資料表時，您可以使用 AWS KMS keys 加密資料表。您可以使用 AWS 擁有的金鑰、 AWS 受管金鑰或客戶受管金鑰。我們建議使用客戶受管金鑰，因為您的組織可以完全控制金鑰，並且當您使用此金鑰類型時，資料表層級加密金鑰、DynamoDB 資料表、本機和全域次要索引以及串流都使用相同的金鑰進行加密。如需這些金鑰類型的詳細資訊，請參閱客戶金鑰和 AWS 金鑰。

> **Note**
>
> 您可以隨時在 AWS 擁有的金鑰、 AWS 受管金鑰和客戶受管金鑰之間切換。

對於靜態資料和傳輸中的資料的用戶端加密和端對端保護，您可以使用 Amazon DynamoDB Encryption Client。除了保護項目屬性值機密性的加密之外，DynamoDB Encryption Client 也會簽署項目。這透過啟用偵測對項目的未授權變更 (包括新增或刪除屬性)，或用一個加密值替換另一個加密值，來提供完整性保護。

請考慮此服務的下列加密最佳實務：

- 將停用或排程刪除金鑰的許可限制為僅需要執行這些任務的人員。這些狀態可避免所有使用者和 DynamoDB 服務可在資料表上加密或解密資料，以及執行讀取和寫入操作。
- 雖然依預設 DynamoDB 使用 HTTPS 加密傳輸中的資料，但建議使用額外安全控制。您可以使用下列任一選項：
  - AWS Site-to-Site VPN 使用 IPsec 進行加密的 連線。
  - AWS Direct Connect 連線以建立私有連線。
  - AWS Direct Connect 連線與 IPsec 加密私有 AWS Site-to-Site VPN 連線的連線。
  - 如果只需要從虛擬私有雲端 (VPC) 內存取 DynamoDB，您可以使用 VPC 閘道端點並僅允許 VPC 中的資源進行存取。這樣可防止流量周遊公有網際網路。
- 如果您使用的是 VPC 端點，請將與端點關聯的端點政策和 IAM 政策限制為僅授權使用者、資源及服務。如需詳細資訊，請參閱使用 IAM 政策控制對 DynamoDB 端點的存取和使用端點政策控制對服務的存取。
- 您可以根據加密政策，在應用程式層級對需要加密的資料實作資料欄層級資料加密。
- 設定 DAX 叢集以在設定叢集時加密靜態資料，例如快取中的資料、組態資料和日誌檔案。您無法在現有叢集上啟用靜態加密。此伺服器端加密有助於保護資料，防止透過基礎儲存進行未經授權的存取。DAX 靜態加密會自動與 AWS KMS 整合，以管理用於加密叢集的單一服務預設金鑰。如果建立加密的 DAX 叢集時，服務預設金鑰不存在，則 AWS KMS 會自動建立新的 AWS 受管金鑰。如需詳細資訊，請參閱 DAX 靜態加密。

  > **Note**
  >
  > 客戶受管金鑰無法與 DAX 叢集搭配使用。

- 設定 DAX 叢集以在設定叢集時加密傳輸中的資料。您無法在現有叢集上啟用傳輸中加密。DAX 使用 TLS 來加密應用程式與叢集之間的請求和回應，並使用叢集的 x509 憑證來驗證叢集的身分。如需詳細資訊，請參閱 DAX 傳輸中加密。
- 在 中 AWS Config，實作dax-encryption-enabled AWS 受管規則，以驗證和維護 DAX 叢集的加密。

Amazon EC2 和 Amazon EBS 的加密最佳實務

Amazon Elastic Compute Cloud (Amazon EC2) 在 AWS 雲端中提供可擴展的運算容量。您可以視需要啟動任意數量的虛擬伺服器，，並快速進行擴展或縮減。Amazon Elastic Block Store (Amazon EBS) 提供區塊層級儲存體磁碟區，可與 EC2 執行個體搭配使用。

請考慮這些服務的下列加密最佳實務：

- 使用適當的資料分類金鑰和值來標記所有 EBS 磁碟區。這可協助您根據您的政策判斷和實作適當的安全和加密要求。
- 根據您的加密政策和技術可行性，為 EC2 執行個體之間或 EC2 執行個體與內部部署網路之間傳輸中的資料設定加密。
- 您可以同時加密 EC2 執行個體的開機和資料 EBS 磁碟區。加密的 EBS 磁碟區可保護下列資料：
  - 磁碟區內的待用資料
  - 所有在磁碟區和執行個體間移動的資料
  - 所有從磁碟區建立的快照
  - 所有從那些快照建立的磁碟區

  如需詳細資訊，請參閱 EBS 加密運作方式。
- 在目前的 中，為您的帳戶預設啟用 EBS 磁碟區的加密 AWS 區域。這會強制加密任何新的 EBS 磁碟區和快照複本。不會影響現有的 EBS 磁碟區或快照。如需詳細資訊，請參閱預設啟用加密。
- 為 Amazon EC2 執行個體加密執行個體儲存體根磁碟區。這有助於保護與作業系統一起儲存的組態檔案和資料。如需詳細資訊，請參閱如何使用 Amazon EC2 執行個體存放區加密保護靜態資料 (AWS 部落格文章)
- 在 中 AWS Config，實作加密磁碟區規則來自動檢查，以驗證和強制執行適當的加密組態。

Amazon ECR 的加密最佳實務

Amazon Elastic Container Registry (Amazon ECR) 是受管容器映像登錄服務，具安全性、可擴展性和可靠性。

Amazon ECR 將映像儲存在 Amazon ECR 管理的 Amazon S3 儲存貯體中。每個 Amazon ECR 儲存庫都有一個加密組態，這是在建立儲存庫時所設定。依預設，Amazon ECR 將伺服器端加密與 Amazon S3 受管 (SSE-S3) 加密金鑰搭配使用。如需詳細資訊，請參閱靜態加密 (Amazon ECR 文件)。

請考慮此服務的下列加密最佳實務：

- 不要使用具有 Amazon S3 受管 (SSE-S3) 加密金鑰的預設伺服器端加密，而是使用儲存在 AWS KMS中的客戶受管 KMS 金鑰。此金鑰類型提供最細緻的控制選項。

> **Note**
>
> KMS 金鑰必須存在於 AWS 區域 與儲存庫相同的 中。

- 佈建儲存庫時，請勿撤銷 Amazon ECR 依預設建立的授權。這可能會影響功能，例如存取資料、加密推送至儲存庫的新映像，或在提取映像時將其解密。
- 使用 AWS CloudTrail 記錄 Amazon ECR 傳送的請求 AWS KMS。日誌項目包含加密內容金鑰，可使其更容易識別。
- 設定 Amazon ECR 政策以從特定 Amazon VPC 端點或特定 VPC 控制存取。實際上，這隔離了對特定 Amazon ECR 資源的網路存取，僅允許從特定 VPC 進行存取。透過使用 Amazon VPC 端點建立虛擬私有網路 (VPN) 連線，您可以對傳輸中的資料進行加密。
- Amazon ECR 支援以資源為基礎的政策。您可以使用這些政策，根據來源 IP 地址或特定 來限制存取 AWS 服務。

Amazon ECS 的加密最佳實務

Amazon Elastic Container Service (Amazon ECS) 是快速、可擴展的容器管理服務，可協助您執行、停止和管理叢集上的容器。

透過 Amazon ECS，您可以使用下列任何一種方法來加密傳輸中的資料：

- 建立服務網格。使用 AWS App Mesh設定已部署 Envoy 代理與網格端點之間的 TLS 連線，例如虛擬節點或虛擬閘道。您可以從 AWS 私有憑證授權單位 或客戶提供的憑證使用 TLS 憑證。如需詳細資訊和逐步解說，請參閱AWS App Mesh 使用 AWS Certificate Manager (ACM) 或客戶提供的憑證在 中的服務之間啟用流量加密 (AWS 部落格文章）。
- 如果支援，請使用 AWS Nitro Enclaves。 AWS Nitro Enclaves 是一種 Amazon EC2 功能，可讓您從 Amazon EC2 執行個體建立稱為 enclaves 的隔離執行環境。其旨在協助保護您最敏感的資料。或者，ACM for Nitro Enclaves 可讓您透過以 AWS Nitro Enclaves 在 Amazon EC2 執行個體上執行的 Web 應用程式和 Web 伺服器，使用公有和私有 SSL/TLS 憑證。如需詳細資訊，請參閱 AWS Nitro Enclaves – 處理機密資料的隔離 EC2 環境 (AWS 部落格文章）。
- 搭配 Application Load Balancer 使用伺服器名稱指示 (SNI) 通訊協定。您可以在 Application Load Balancer 的單一 HTTPS 接聽程式後方部署多個應用程式。每個接聽程式都具有自己的 TLS 憑證。您可以使用 ACM 提供的憑證，也可以使用自我簽署憑證。Application Load Balancer 和 Network Load Balancer 都支援 SNI。如需詳細資訊，請參閱 Application Load Balancer 現在支援使用 SNI 進行智慧選擇的多個 TLS 憑證 (AWS 部落格文章）。
- 為了提高安全性和彈性，請使用 AWS 私有憑證授權單位 部署具有 Amazon ECS 任務的 TLS 憑證。如需詳細資訊，請參閱維護 TLS 至您的容器第 2 部分：使用 AWS 私有 CA(AWS 部落格文章）。
- 使用機密探索服務 (Envoy) 或 ACM 中託管的憑證 (GitHub) 在 App Mesh 中實作雙向 TLS (mTLS)。

請考慮此服務的下列加密最佳實務：

- 在技術上可行的情況下，為了增強安全性，在 AWS PrivateLink中設定 Amazon ECS 介面 VPC 端點。透過 VPN 連線存取這些端點會加密傳輸中的資料。
- 安全地儲存敏感材料，例如 API 金鑰或資料庫憑證。您可以將這些參數作為加密參數儲存在 Parameter Store (AWS Systems Manager的功能) 中。不過，我們建議您使用 ， AWS Secrets Manager 因為此服務可讓您自動輪換秘密、產生隨機秘密，以及跨 共用秘密 AWS 帳戶。
- 如果資料中心的使用者或應用程式或 Web 上的外部第三方正在向 提出直接 HTTPS API 請求 AWS 服務，請使用從 AWS Security Token Service () 取得的臨時安全登入資料簽署這些請求AWS STS。

Amazon EFS 的加密最佳實務

Amazon Elastic File System (Amazon EFS) 協助您在 AWS 雲端中建立和設定共用檔案系統。

請考慮此服務的下列加密最佳實務：

- 在 中 AWS Config，實作 efs-encrypted-check AWS 受管規則。此規則會檢查 Amazon EFS 是否設定為使用 加密檔案資料 AWS KMS。
- 透過建立 Amazon CloudWatch 警報來對 Amazon EFS 檔案系統強制執行加密，該警報會監控 CloudTrail 日誌中是否存在 `CreateFileSystem` 事件，並在建立未加密的檔案系統時觸發警報。如需詳細資訊，請參閱逐步解說：在 Amazon EFS 檔案系統上強制執行靜態加密。
- 使用 EFS 掛載協助程式掛載檔案系統。這會在用戶端與 Amazon EFS 服務之間設定和維護 TLS 1.2 通道，並透過此加密通道路由所有網路檔案系統 (NFS) 流量。下列命令實作使用 TLS 進行傳輸中加密。

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  如需詳細資訊，請參閱使用 EFS 掛載協助程式掛載 EFS 檔案系統。
- 使用 AWS PrivateLink實作界面 VPC 端點，以在 VPCs和 Amazon EFS API 之間建立私有連線。透過 VPN 連線傳入和傳出端點的資料經過加密。如需詳細資訊，請參閱使用介面 VPC 端點存取 AWS 服務。
- 使用 IAM 身分型政策中的 `elasticfilesystem:Encrypted` 條件金鑰來防止使用者建立未加密的 EFS 檔案系統。如需詳細資訊，請參閱使用 IAM 強制建立加密檔案系統。
- 應使用資源型金鑰政策將用於 EFS 加密的 KMS 金鑰設定為最低權限存取。

- 在連接至 EFS 檔案系統時，使用 EFS 檔案系統政策中的 `aws:SecureTransport` 條件金鑰強制 NFS 用戶端使用 TLS。如需詳細資訊，請參閱使用 Amazon Elastic File System 加密檔案資料中傳輸中的資料加密 (AWS 白皮書）。 Amazon Elastic File System

Amazon EKS 的加密最佳實務

Amazon Elastic Kubernetes Service (Amazon EKS) 可協助您在 上執行 Kubernetes， AWS 而無需安裝或維護您自己的 Kubernetes 控制平面或節點。在 Kubernetes 中，機密可協助您管理敏感資訊，例如使用者憑證、密碼或 API 金鑰。依預設，這些機密以未加密的方式儲存在 API 伺服器的基礎資料儲存 (稱為 etcd) 中。在 Amazon EKS 上，`etcd`節點的 Amazon Elastic Block Store (Amazon EBS) 磁碟區會使用 Amazon EBS 加密進行加密。任何具有 API 存取權或存取 `etcd` 的使用者都可以擷取或修改機密。此外，任何有權在命名空間中建立 Pod 的人都可以使用該存取權來讀取該命名空間中的任何機密。您可以使用 AWS 受管金鑰或客戶受管金鑰 AWS KMS keys，在 Amazon EKS 中加密這些靜態秘密。使用 `etcd` 的另一種方法是使用 AWS Secrets and Config Provider (ASCP) (GitHub 儲存庫)。ASCP 與 IAM 和資源型政策整合，以限制和約束對叢集內部特定 Kubernetes Pod 內的機密的存取。

您可以搭配 Kubernetes 使用下列 AWS 儲存服務：

- 對於 Amazon EBS，您可以使用樹狀內儲存驅動程式或 Amazon EBS CSI 驅動程式。兩者都包括用於加密磁碟區和提供客戶受管金鑰的參數。
- 對於 Amazon Elastic File System (Amazon EFS)，您可以使用同時支援動態和靜態佈建的 Amazon EFS CSI 驅動程式。

請考慮此服務的下列加密最佳實務：

- 如果您使用的是 `etcd` (依預設儲存未加密的機密物件)，請執行下列操作以協助保護機密：
  - 加密機密靜態資料 (Kubernetes 文件)。
  - AWS KMS 用於 Kubernetes 秘密的信封加密。這可讓您使用唯一的資料金鑰來加密秘密。您可以使用 AWS KMS 金鑰加密金鑰來加密資料金鑰。您可以定期自動輪換金鑰加密金鑰。使用適用於 Kubernetes 的 AWS KMS 外掛程式，所有 Kubernetes 秘密都會以加密文字儲存在 `etcd`中。它們只能由 Kubernetes API 伺服器解密。如需詳細資訊，請參閱使用 Amazon EKS 加密提供者支援進行深度防禦，以及在現有叢集 AWS KMS 上使用 加密 Kubernetes 秘密。
  - 透過限制讀取和寫入機密的角色型存取控制 (RBAC) 規則啟用或設定授權。限制建立新機密或取代現有機密的許可。如需詳細資訊，請參閱授權概觀 (Kubernetes 文件)。

  - 如果您在 Pod 中定義多個容器，且只有其中一個容器需要存取機密，請定義磁碟區掛載，以便其他容器無法存取該機密。以磁碟區掛載的機密會具現化為 `tmpfs` 磁碟區，並在刪除 Pod 時自動從節點中移除。您也可以使用環境變數，但我們不建議使用此方法，因為環境變數的值可能會出現在日誌中。如需詳細資訊，請參閱機密 (Kubernetes 文件)。
  - 如果可能，避免授予對命名空間內的機密的 `watch` 和 `list` 請求的存取權。在 Kubernetes API 中，這些請求非常強大，因為其允許用戶端檢查該命名空間中每個機密的值。
  - 僅允許叢集管理員存取 `etcd`，包括唯讀存取權。
  - 如果存在多個 `etcd` 執行個體，請確保 `etcd` 使用 TLS 在 `etcd` 對等項之間進行通訊。
- 如果您使用的是 ASCP，請執行下列操作以協助保護機密：
  - 使用服務帳戶的 IAM 角色將機密存取權限制為僅授權的 Pod。
  - 透過使用 AWS Encryption Provider (GitHub 儲存庫) 啟用 Kubernetes 機密加密，以使用客戶受管 KMS 金鑰實作封套加密。
- 若要協助降低環境變數資料外洩的風險，建議您使用 Secret Store CSI Driver 的AWS Secrets Manager 和 Config Provider (GitHub)。此驅動程式可讓您將儲存在 Secrets Manager 中的機密和儲存在 Parameter Store 中的參數顯示為掛載在 Kubernetes Pod 中的檔案。

  > **Note**
  >
  > AWS Fargate 不支援 。

- 建立 Amazon CloudWatch 指標篩選條件和警示，以針對管理員指定的操作傳送提醒，例如機密刪除或在等待刪除期間使用機密版本。如需詳細資訊，請參閱根據異常偵測建立警報。

的加密最佳實務 AWS Encryption SDK

AWS Encryption SDK 是開放原始碼的用戶端加密程式庫。它使用產業標準和最佳實務來支援多種程式設計語言的實作和互通性。 使用安全、經過驗證的對稱金鑰演算法 AWS Encryption SDK 來加密資料，並提供遵循密碼編譯最佳實務的預設實作。如需詳細資訊，請參閱 AWS Encryption SDK中的支援演算法套件。

的其中一個主要功能 AWS Encryption SDK 是支援加密使用中的資料。透過採用encrypt-then-use方法，您可以在應用程式邏輯處理敏感資料之前對其進行加密。這有助於保護資料免受潛在的暴露或竄改，即使應用程式本身受到安全事件的影響。

請考慮此服務的下列最佳實務：

- 遵循 AWS Encryption SDK的最佳實務中的所有建議。
- 選取一或多個包裝金鑰，以協助保護您的資料金鑰。如需詳細資訊，請參閱選取包裝金鑰。
- 將 KeyId 參數傳遞給 ReEncrypt 操作以協助防止使用不受信任的 KMS 金鑰。如需詳細資訊，請參閱改善用戶端加密：明確 KeyIds 和金鑰承諾 (AWS 部落格文章）。
- AWS Encryption SDK 搭配 使用 時 AWS KMS，請使用本機KeyId篩選。如需詳細資訊，請參閱改善用戶端加密：明確 KeyIds 和金鑰承諾 (AWS 部落格文章）。
- 對於需要加密或解密大量流量的應用程式，或您的帳戶超過 AWS KMS 請求配額，您可以使用 的資料金鑰快取功能 AWS Encryption SDK。請注意資料金鑰快取的下列最佳實務：
  - 設定快取安全閾值以限制每個已快取資料金鑰可使用的時間長度，以及依據每個資料金鑰可以保護的資料數量。如需設定這些閾值時的建議，請參閱設定快取安全閾值。
  - 將本機快取限制為實現特定應用程式使用案例效能改進所需的最小資料金鑰數。如需設定本機快取限制的指示和範例，請參閱使用資料金鑰快取：逐步。

  如需詳細資訊，請參閱AWS Encryption SDK：如何判斷資料金鑰快取是否適合您的應用程式 (AWS 部落格文章）。

的加密最佳實務 AWS Key Management Service

AWS Key Management Service (AWS KMS) 可協助您建立和控制密碼編譯金鑰，以協助保護您的資料。 與大多數 AWS 服務 可以加密資料的其他 AWS KMS 整合。如需完整清單，請參閱AWS 服務 與整合 AWS KMS。 AWS KMS 也與 AWS CloudTrail 整合，以記錄 KMS 金鑰的使用情形，用於稽核、法規和合規需求。

KMS 金鑰是 中的主要資源 AWS KMS，也是密碼編譯金鑰的邏輯表示法。KMS 金鑰有三種主要類型：

- 客戶受管金鑰是您建立的 KMS 金鑰。
- AWS 受管金鑰是在帳戶中代表您 AWS 服務 建立的 KMS 金鑰。
- AWS 擁有的金鑰是 AWS 服務 擁有和管理的 KMS 金鑰，可用於多個 AWS 帳戶。

如需有關這些金鑰類型的詳細資訊，請參閱客戶金鑰和 AWS 金鑰。

在 中 AWS 雲端，政策用於控制誰可以存取資源和服務。例如，在 AWS Identity and Access Management (IAM) 中，身分型政策會定義使用者、使用者群組或角色的許可，以及連接至資源的資源型政策，例如 S3 儲存貯體，並定義哪些主體允許存取、支援的動作，以及必須符合的任何其他條件。與 IAM 政策類似， AWS KMS 會使用金鑰政策來控制對 KMS 金鑰的存取。每個 KMS 金鑰都必須具

有金鑰政策，且每個金鑰只能具有一個金鑰政策。定義允許或拒絕存取 KMS 金鑰的政策時，注意下列事項：

- 您可以控制客戶受管金鑰的金鑰政策，但無法直接控制 AWS 受管金鑰或 AWS 擁有金鑰的金鑰政策。
- 金鑰政策允許授予 內 AWS KMS API 呼叫的精細存取權 AWS 帳戶。除非金鑰政策明確允許，否則您不能使用 IAM 政策來允許存取 KMS 金鑰。如果沒有金鑰政策的許可，允許許可的 IAM 政策將不起作用。如需詳細資訊，請參閱允許 IAM 政策存取 KMS 金鑰。
- 您可以使用 IAM 政策拒絕對客戶受管金鑰的存取，而無需金鑰政策的對應許可。
- 針對多區域金鑰設計金鑰政策和 IAM 政策時，請考慮下列事項：
  - 金鑰政策不是多區域金鑰的共用屬性，且不會在相關的多區域金鑰之間複製或同步。
  - 使用 `CreateKey` 和 `ReplicateKey` 動作建立多區域金鑰時，將套用預設金鑰政策，除非在請求中指定了金鑰政策。
  - 您可以實作條件金鑰 (例如 aws:RequestedRegion)，以限制特定 AWS 區域的許可。
  - 您可以使用授予來允許多區域主要金鑰或複本金鑰的許可。但是，您無法使用單一授予來允許多個 KMS 金鑰的許可，即使這些金鑰是相關的多區域金鑰。

使用 AWS KMS 和建立金鑰政策時，請考慮下列加密最佳實務和其他安全最佳實務：

- 遵循下列資源中 AWS KMS 有關最佳實務的建議：
  - AWS KMS 授予的最佳實務 (AWS KMS 文件)
  - IAM 政策的最佳實務 (AWS KMS 文件)
- 根據職責分離最佳實務，為管理金鑰的人員和使用金鑰的人員維護個別身分：
  - 建立和刪除金鑰的管理員角色不應具有使用金鑰的能力。
  - 部分服務可能只需要加密資料，而不應授予使用金鑰解密資料的能力。
- 金鑰政策應永遠遵循最低權限的模型。請勿將 `kms:*` 用於 IAM 或金鑰政策中的動作，因為這會授予主體管理和使用金鑰的許可。
- 在金鑰政策中使用 kms:ViaService AWS 服務 條件金鑰，將客戶受管金鑰的使用限制為特定。
- 如果您可以在金鑰類型之間進行選擇，則優先客戶受管金鑰，因為其會提供最精細的控制選項，包括下列選項：
  - 管理身分驗證和存取控制
  - 啟用和停用金鑰
  - 輪換 AWS KMS keys

  - 標記金鑰
  - 建立別名
  - 刪除 AWS KMS keys
- AWS KMS 管理和修改許可必須明確拒絕給未經核准的委託人，且 AWS KMS 修改許可不應存在於任何未經授權委託人的允許陳述式中。如需詳細資訊，請參閱適用於 AWS Key Management Service的動作、資源和條件鍵。
- 為了偵測未經授權使用 KMS 金鑰，請在 中 AWS Config實作 iam-customer-policy-blocked-kms-actions 和 iam-inline-policy-blocked-kms-actions 規則。這可防止主體在所有資源上使用 AWS KMS 解密動作。
- 在 中實作服務控制政策 SCPs)， AWS Organizations 以防止未經授權的使用者或角色直接以命令或透過主控台刪除 KMS 金鑰。如需詳細資訊，請參閱使用 SCPs做為預防性控制 (AWS 部落格文章) 。
- 在 CloudTrail 日誌中記錄 AWS KMS API 呼叫。這會記錄相關的事件屬性，例如發出的請求內容、發出請求的來源 IP 地址以及發出請求的人。如需詳細資訊，請參閱使用 記錄 AWS KMS API 呼叫 AWS CloudTrail。
- 如果您使用加密內容，它不應包含任何敏感資訊。CloudTrail 將加密內容儲存在純文字 JSON 檔案中，有權存取包含此資訊的 S3 儲存貯體的任何人都可以檢視該檔案。
- 監控客戶受管金鑰的使用情況時，設定事件以在偵測特定動作 (例如建立金鑰、更新客戶受管金鑰政策或匯入金鑰材料) 時通知您。也建議您實作自動回應，例如停用金鑰或執行組織政策規定的任何其他事件回應動作的 AWS Lambda 函數。
- 多區域金鑰建議用於特定案例，例如合規、災難復原或備份。多區域金鑰的安全屬性與單一區域金鑰顯著不同。授權建立、管理和使用多區域金鑰時，採用下列建議：
  - 允許委託人只將多區域金鑰複寫至需要的 AWS 區域 中。
  - 只將多區域金鑰的許可授予需要這些金鑰的委託人，並且僅為需要這些金鑰的任務授予。

的加密最佳實務 AWS Lambda

AWS Lambda 是一項運算服務，可協助您執行程式碼，無需佈建或管理伺服器。若要保護您的環境變數，可以使用伺服器端加密來保護您的靜態資料，並使用用戶端加密來保護傳輸中的資料。

請考慮此服務的下列加密最佳實務：

- Lambda 永遠使用 AWS KMS key提供靜態伺服器端加密。根據預設，Lambda 會使用 AWS 受管金鑰。我們建議您使用客戶受管金鑰，因為您可以完全控制此金鑰，包括管理、輪換和稽核。

- 對於需要加密的傳輸中的資料，啟用協助程式，這可確保使用偏好 KMS 金鑰對環境變數進行用戶端加密，以在傳輸過程中提供保護。如需詳細資訊，請參閱保護環境變數中的傳輸中安全。
- 儲存敏感或重要資料的 Lambda 函數環境變數應在傳輸過程中進行加密，以協助保護動態傳遞至函數的資料 (通常是存取資訊) 免遭未經授權的存取。
- 若要防止使用者檢視環境變數，請將陳述式新增至 IAM 政策中的使用者許可，或新增至拒絕存取預設金鑰、客戶受管金鑰或所有金鑰的金鑰政策。如需詳細資訊，請參閱使用 AWS Lambda 環境變數。

Amazon RDS 的加密最佳實務

Amazon Relational Database Service (Amazon RDS) 可協助您在 AWS 雲端中設定、操作和擴展關聯式資料庫 (DB)。靜態加密的資料包括資料庫執行個體的基礎儲存體、其自動化備份、僅供讀取複本，以及快照。

以下是您可用於加密 RDS 資料庫執行個體中的靜態資料的方法：

- 您可以使用 受管金鑰或客戶受管金鑰 AWS KMS keys來 AWS 加密 Amazon RDS 資料庫執行個體。如需詳細資訊，請參閱本指南中的 AWS Key Management Service。
- Amazon RDS for Oracle 和 Amazon RDS for SQL Server 支援使用透明資料加密 (TDE)，來加密資料庫執行個體。如需詳細資訊，請參閱 Oracle 透明資料加密或支援 SQL Server 的透明資料加密。

  您可以同時使用 TDE 和 KMS 金鑰來加密資料庫執行個體。但是，這可能會稍微影響資料庫的效能，您必須分別管理這些金鑰。

以下是您可用於加密往返 RDS 資料庫執行個體的傳輸中的資料的方法：

- 對於執行 MariaDB、Microsoft SQL Server、MySQL、Oracle 或 PostgreSQL 的 Amazon RDS 資料庫執行個體，您可以使用 SSL 加密連線。如需詳細資訊，請參閱使用 SSL/TLS 加密資料庫執行個體的連線。
- Amazon RDS for Oracle 也支援 Oracle 原生網路加密 (NNE)，可在資料移入和移出資料庫執行個體時加密資料。無法同時使用 NNE 和 SSL 加密。如需詳細資訊，請參閱 Oracle 原生網路加密。

請考慮此服務的下列加密最佳實務：

- 在連接至 Amazon RDS for SQL Server 或 Amazon RDS for PostgreSQL 資料庫執行個體以處理、儲存或傳輸需要加密的資料時，使用 RDS 傳輸加密功能來加密連線。您可以在參數群組中將

`rds.force_ssl` 參數設定為 1 來實作此操作。如需詳細資訊，請參閱使用參數群組。Amazon RDS for Oracle 使用 Oracle 資料庫原生網路加密。

- 用於 RDS 資料庫執行個體加密的客戶受管金鑰應僅用於該用途，且不得與任何其他 AWS 服務搭配使用。
- 在加密 RDS 資料庫執行個體之前，先建立 KMS 金鑰需求。執行個體使用的金鑰以後無法變更。例如，在您的加密政策中，根據您的業務需求，定義 AWS 受管金鑰或客戶受管金鑰的使用和管理標準。
- 授權存取客戶受管 KMS 金鑰時，請在 IAM 政策中使用條件金鑰，以遵循最低權限原則。例如，若要僅允許客戶受管金鑰用於源自 Amazon RDS 的請求，請使用 kms:ViaService 條件金鑰搭配 `rds.<region>.amazonaws.com`值。此外，您可以使用 Amazon RDS 加密內容中的金鑰或值，做為使用客戶受管金鑰的條件。
- 強烈建議您為加密的 RDS 資料庫執行個體啟用備份。Amazon RDS 可能會失去對資料庫執行個體的 KMS 金鑰的存取權，例如未啟用 KMS 金鑰或撤銷 RDS 對 KMS 金鑰的存取權時。如果發生此情況，則加密的資料庫執行個體將進入可復原狀態七天。如果資料庫執行個體在七天後未重新取得對金鑰的存取權，則資料庫將變得最終無法存取，必須從備份還原。如需詳細資訊，請參閱加密資料庫執行個體。
- 如果僅供讀取複本及其加密的資料庫執行個體位於相同位置 AWS 區域，您必須使用相同的 KMS 金鑰來加密兩者。
- 在 中 AWS Config，實作 rds-storage-encrypted AWS 受管規則來驗證和強制執行 RDS 資料庫執行個體的加密，以及 rds-snapshots-encrypted 規則來驗證和強制執行 RDS 資料庫快照的加密。
- 使用 AWS Security Hub CSPM 評估您的 Amazon RDS 資源是否遵循安全最佳實務。如需詳細資訊，請參閱 Amazon RDS 的 Security Hub CSPM 控制項。

的加密最佳實務 AWS Secrets Manager

AWS Secrets Manager 可協助您將程式碼中的硬式編碼憑證 (包括密碼) 取代為 Secrets Manager 的 API 呼叫，以便透過程式設計方法來擷取機密。Secrets Manager 與 整合 AWS KMS ，使用 保護的唯一資料金鑰來加密每個秘密值的每個版本 AWS KMS key。此整合使用永遠不會 AWS KMS 保持未加密的加密金鑰來保護存放的秘密。您也可以定義 KMS 金鑰的自訂許可，以稽核產生、加密及解密用來保護儲存機密的資料金鑰的操作。如需詳細資訊，請參閱 AWS Secrets Manager中的機密加密和解密。

請考慮此服務的下列加密最佳實務：

- 在大多數情況下，我們建議使用 `aws/secretsmanager` AWS 受管金鑰來加密秘密。使用它無需付費。
- 若要能夠從另一個帳戶存取秘密，或將金鑰政策套用至加密金鑰，請使用客戶受管金鑰來加密秘密。
  - 在金鑰政策中，將值指派給 kms:ViaService `secretsmanager.<region>.amazonaws.com` 條件金鑰。這會將金鑰的使用限制為僅來自 Secrets Manager 的請求。
  - 若要進一步限制金鑰的使用僅限於具有正確內容的 Secrets Manager 請求，請使用 Secrets Manager 加密內容中的金鑰或值，作為使用 KMS 金鑰的條件，方法是建立：
    - IAM 政策或金鑰政策中的字串條件運算子
    - 授權中的授予限制條件

Amazon S3 的加密最佳實務

Amazon Simple Storage Service (Amazon S3) 是一種雲端型物件儲存服務，可協助您儲存、保護和擷取任何數量的資料。

對於 Amazon S3 中的伺服器端加密，有以下三個選項：

- 使用 Amazon S3 受管加密金鑰進行伺服器端加密 (SSE-S3)
- 使用 AWS Key Management Service (SSE-KMS) 的伺服器端加密
- 使用客戶提供加密金鑰進行伺服器端加密 (SSE-C)

Amazon S3 會使用 Amazon S3 受管金鑰 (SSE-S3) 套用伺服器端加密，做為 Amazon S3 中每個儲存貯體的基本加密層級。從 2023 年 1 月 5 日起，所有上傳到 Amazon S3 的新物件都會自動加密，無需額外費用，也不會影響效能。S3 儲存貯體預設加密組態和新物件上傳的自動加密狀態可在 AWS CloudTrail 日誌、S3 庫存、S3 Storage Lens、Amazon S3 主控台，以及 AWS Command Line Interface (AWS CLI) 和 AWS SDKs 中的其他 Amazon S3 API 回應標頭中使用。如需詳細資訊，請參閱預設加密常見問答集。

如果在上傳時使用伺服器端加密來加密物件，請將 `x-amz-server-side-encryption` 標頭新增至請求，以通知 Amazon S3 使用 SSE-S3、SSE-KMS 或 SSE-C 加密物件。以下是 `x-amz-server-side-encryption` 標頭的可能值：

- `AES256`，可通知 Amazon S3 使用 Amazon S3 受管金鑰。
- `aws:kms`，指示 Amazon S3 使用 AWS KMS 受管金鑰。
- 對於 SSE-C，將值設定為 `True` 或 `False`

如需詳細資訊，請參閱如何使用儲存貯體政策和套用深度防禦以協助保護您的 Amazon S3 資料 (AWS 部落格文章） 中的Defense-in-depth防禦需求 1：資料必須靜態加密，並在傳輸期間加密。 Defense-in-Depth Amazon S3

對於 Amazon S3 中的用戶端加密，有以下兩個選項：

- 存放在 中的金鑰 AWS KMS
- 儲存在應用程式內的金鑰

請考慮此服務的下列加密最佳實務：

- 在 中 AWS Config，實作 s3-bucket-server-side-encryption-enabled AWS 受管規則，以驗證和強制執行 S3 儲存貯體加密。
- 部署 Amazon S3 儲存貯體政策，以驗證所有正在上傳的物件是否都使用 `s3:x-amz-server-side-encryption` 條件進行加密。如需詳細資訊，請參閱使用 SSE-S3 保護資料中的範例儲存貯體政策和新增儲存貯體政策中的說明。
- 透過在 S3 儲存貯體政策中使用 `aws:SecureTransport` 條件，僅允許透過 HTTPS (TLS) 進行加密連線。如需詳細資訊，請參閱我應該使用哪些 S3 儲存貯體政策來符合 AWS Config 規則 s3-bucket-ssl-requests-only？
- 在 中 AWS Config，實作 s3-bucket-ssl-requests-only AWS 受管規則，要求 請求使用 SSL。
- 在您需要授予 Amazon S3 物件的跨帳戶存取權時，使用客戶受管金鑰。設定金鑰政策，以允許透過其他 AWS 帳戶存取。

Amazon VPC 的加密最佳實務

Amazon Virtual Private Cloud (Amazon VPC) 可協助您在已定義的虛擬網路中啟動 AWS 資源。此虛擬網路與您在自己的資料中心中操作的傳統網路相似，且具備使用 AWS可擴展基礎設施的優勢。

請考慮此服務的下列加密最佳實務：

- 使用下列其中一種方法對公司網路和 VPC 內的資訊資產與系統之間的流量進行加密：
  - AWS Site-to-Site VPN 連線
  - AWS Site-to-Site VPN 和 AWS Direct Connect 連線的組合，可提供 IPsec 加密的私有連線
  - AWS Direct Connect 支援 MAC Security (MACsec) 將資料從公司網路加密到 位置的 AWS Direct Connect 連線

- 在 中使用 VPC 端點 AWS PrivateLink ，將您的 VPCs 私下連線至支援的 ， AWS 服務 而無需使用網際網路閘道。您可以使用 AWS Direct Connect 或 Site-to-Site VPN 服務來建立此連線。您的 VPC 與其他 服務之間的流量不會離開 AWS 網路。如需詳細資訊，請參閱AWS 服務 透過 存取 AWS PrivateLink。
- 設定安全群組規則，以僅允許來自與安全協定 (例如 HTTPS over TCP/443) 關聯的連接埠的流量。定期稽核安全群組及其規則。

資源

- 為靜態資料建立企業加密策略 (AWS 規範性指導）
- (AWS KMS 文件） 的安全最佳實務 AWS Key Management Service
- AWS 服務 如何使用 AWS KMS(AWS KMS 文件）
- 安全支柱：資料保護 (AWS Well-Architected Framework)

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
密碼編譯更新	我們更新了AWS 密碼編譯章節的方法。	2026 年 2 月 19 日
演算法更新	我們更新了密碼編譯演算法區段。	2026 年 1 月 23 日
傳輸中更新的演算法和加密	我們更新了關於密碼編譯演算法章節和傳輸中資料的加密章節。	2025 年 10 月 28 日
演算法更新	我們將密碼編譯演算法的相關資訊新增至密碼編譯演算法和 AWS 服務區段。	2025 年 6 月 18 日
Amazon EKS 更新	我們更新了 Amazon Elastic Kubernetes Service (Amazon EKS) 的加密最佳實務。	2025 年 1 月 7 日
Secrets Manager 更新	我們更新了 的資訊和建議 AWS Secrets Manager。	2024 年 9 月 9 日
AWS 服務 更新	我們更新了 Amazon EKS、Amazon Relational Database Service (Amazon RDS) AWS Encryption SDK 和 Amazon Simple Storage Service (Amazon S3) 的資訊和建議。	2024 年 9 月 4 日
初次出版	—	2022 年 12 月 2 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。