AWS Key Management Service 最佳實務

AWS 方案指引

AWS 方案指引: AWS Key Management Service 最佳實務

Table of Contents

AWS Key Management Service 最佳實務

Amazon Web Services （貢獻者）

2025 年 3 月 (文件歷史記錄)

AWS Key Management Service (AWS KMS) 是一種受管服務，可讓您輕鬆建立和控制用來保護資料的加密金鑰。本指南說明如何有效地使用 AWS KMS 和提供最佳實務。它可協助您比較組態選項，並根據您的需求選擇最佳設定。

本指南包含有關組織如何使用 AWS KMS 來保護敏感資訊並實作多個使用案例簽署的建議。它會考慮使用下列維度的目前建議：

- 管理金鑰 – 管理和金鑰儲存選擇的委派選項
- 資料保護 – 在您自己的應用程式中加密資料，而不是代表您 AWS 服務 進行加密
- 存取管理 – 使用 AWS KMS 金鑰政策和 AWS Identity and Access Management (IAM) 政策來實作角色型存取控制 (RBAC) 或屬性型存取控制 (ABAC)。
- 多帳戶和多區域架構 – 大規模部署的建議。
- 帳單和成本管理 – 了解您的成本和用量，以及降低成本的建議。
- Detective 控制 – 監控 KMS 金鑰、加密設定和加密資料的狀態。
- 事件回應 – 更正導致不符合資料保護政策的錯誤設定。

目標業務成果

您的資料是您業務的關鍵和敏感資產。透過 AWS KMS，您可以管理用來保護和驗證資料的加密金鑰。您可以控制資料的使用方式、誰可以存取資料，以及資料的加密方式。本指南旨在協助開發人員、系統管理員和安全專業人員實作加密最佳實務，協助您保護儲存或傳輸的敏感資料 AWS 服務。透過了解並實作本指南中的建議，您可以在整個 AWS 環境中提升資料機密性和完整性。您可以滿足您的資料保護要求，無論這些要求是在內部制定，或者您有合規或驗證計劃的特定要求。如需有關 AWS KMS 如何協助您保護 AWS 環境中資料的詳細資訊，請參閱 AWS KMS 文件中的使用 AWS KMS 加密搭配 AWS 服務 。

關於 AWS KMS keys

AWS Key Management Service (AWS KMS) 可讓您建立密碼編譯金鑰，可用於您傳遞給服務的資料。主要資源類型是 KMS 金鑰，其中有三種類型：

- 進階加密標準 (AES) 對稱金鑰 – 這些是 256 位元金鑰，用於 AES 的 Galois 計數器模式 (GCM) 模式。這些金鑰提供大小小於 4 KB 的資料驗證加密和解密。這是最常見的金鑰類型。它用於保護其他資料金鑰，例如您的應用程式中使用的資料 AWS 服務 金鑰，或代表您加密資料的資料金鑰。
- RSA 或橢圓曲線非對稱索引鍵 – 這些索引鍵提供各種大小，並支援許多演算法。根據演算法，它們可用於加密和解密以及簽署和驗證操作。
- 用於執行雜湊型訊息驗證碼 (HMAC) 操作的對稱金鑰 – 這些金鑰是用於簽署和驗證操作的 256 位元金鑰。

無法從服務以純文字匯出 KMS 金鑰。它們是由 產生，並且只能在 服務使用的硬體安全模組 HSMs) 內使用。這是 的基本安全屬性 AWS KMS ，可防止金鑰遭到入侵。在中國 （北京） 和中國 （寧夏） 區域，這些 HSMs已經過 OSCCA 認證。在所有其他區域中，用於 HSMs AWS KMS 會在安全層級 3 的 NIST 內透過 FIPS 140 程式進行驗證。如需 中 AWS KMS 有助於保護金鑰之設計和控制項的詳細資訊，請參閱AWS Key Management Service 密碼編譯詳細資訊。

您可以使用 AWS KMS 各種密碼編譯 APIs 將資料提交至 ，以使用 KMS 金鑰執行加密、解密、簽署或驗證操作。您也可以選擇讓 KMS 金鑰充當金鑰加密金鑰，以保護稱為資料金鑰的金鑰類型。您可以從匯出資料金鑰 AWS KMS ，以便在本機應用程式或代表保護 AWS 服務 資料的 中使用。資料金鑰的使用在所有金鑰管理系統中都很常見，通常稱為信封加密。信封加密允許在處理您的敏感資料的遠端系統上使用資料金鑰，而不必直接將敏感資料傳送到 AWS KMS 以進行 KMS 金鑰下的加密。

如需詳細資訊，請參閱 AWS KMS 文件中的 AWS KMS keys和 AWS KMS 密碼編譯基本概念。

的金鑰管理最佳實務 AWS KMS

使用 AWS Key Management Service (AWS KMS) 時，您必須做出一些基本的設計決策。這些包括是否使用集中式或分散式模型進行金鑰管理和存取、要使用的金鑰類型，以及要使用的金鑰存放區類型。下列各節可協助您做出適合您組織和使用案例的決策。本節最後說明停用和刪除 KMS 金鑰的重要考量，包括您應該採取的動作，以協助保護您的資料和金鑰。

本節包含下列主題：

選擇集中式或分散式模型

AWS 建議您使用多個 ， AWS 帳戶 並在 中將這些帳戶做為單一組織管理AWS Organizations。在 AWS KMS keys 多帳戶環境中管理 有兩種廣泛的方法。

第一種方法是分散式方法，您可以在每個帳戶中建立使用這些金鑰的金鑰。當您將 KMS 金鑰存放在與其保護的資源相同的帳戶中時，將許可委派給了解其 AWS 委託人和金鑰存取要求的本機管理員會更容易。您可以只使用金鑰政策來授權金鑰用量，也可以在 AWS Identity and Access Management (IAM) 中結合金鑰政策和以身分為基礎的政策。

第二個方法是集中式方法，您可以在其中將 KMS 金鑰維持在一個或幾個指定的金鑰中 AWS 帳戶。您只允許其他帳戶將金鑰用於密碼編譯操作。您可以從集中式帳戶管理金鑰、其生命週期及其許可。您允許其他 AWS 帳戶 使用金鑰，但不允許其他許可。外部帳戶無法管理有關金鑰生命週期或存取許可的任何內容。此集中式模型有助於將委派管理員或使用者意外刪除金鑰或權限提升的風險降至最低。

您選擇的選項取決於幾個因素。選擇方法時，請考慮下列事項：

1. 您是否有佈建金鑰和資源存取權的自動化或手動程序？ 這包括部署管道和基礎設施即程式碼 (IaC) 範本等資源。這些工具可協助您在許多 之間部署和管理資源 （ 例如 KMS 金鑰、金鑰政策、IAM 角色和 IAM 政策） AWS 帳戶。如果您沒有這些部署工具，對於您的企業而言，集中式的金鑰管理方法可能更易於管理。
2. 您對 AWS 帳戶 包含使用 KMS 金鑰之資源的所有 是否具有管理控制權？ 如果是這樣，集中式模型可以簡化管理，無需切換 AWS 帳戶 來管理金鑰。不過，請注意，仍必須管理每個帳戶的 IAM 角色和使用者使用金鑰的許可。

3. 您是否需要提供存取權，以便擁有自己的 AWS 帳戶 和資源的客戶或合作夥伴使用您的 KMS 金鑰？ 對於這些金鑰，集中式方法可以減輕客戶和合作夥伴的管理負擔。
4. 對於透過集中式或本機存取方法更好地解決 AWS 的資源，您是否有存取的授權要求？ 例如，如果不同的應用程式或業務單位負責管理自己資料的安全性，則對金鑰管理的分散式方法會更好。
5. 您是否超過 的服務資源配額 AWS KMS？ 由於這些配額是根據 設定 AWS 帳戶，因此分散式模型會將負載分散到 帳戶，有效地乘以服務配額。

> **Note**
>
> 考慮請求配額時，金鑰的管理模型無關緊要，因為這些配額會套用至對金鑰提出請求的帳戶委託人，而不是擁有或管理金鑰的帳戶。

一般而言，建議您從分散式方法開始，除非您可以明確表達對集中式 KMS 金鑰模型的需求。

選擇客戶受管金鑰、受 AWS 管金鑰或 AWS 擁有的金鑰

您為在自己的密碼編譯應用程式中使用而建立和管理的 KMS 金鑰稱為客戶受管金鑰。 AWS 服務 可以使用客戶受管金鑰來代表您加密服務存放的資料。如果您想要完全控制金鑰的生命週期和用量，建議使用客戶受管金鑰。您的帳戶中有客戶受管金鑰需要每月成本。此外，使用或管理金鑰的請求會產生使用成本。如需詳細資訊，請參閱 AWS KMS 定價。

如果您想要 AWS 服務 加密資料，但不想要管理金鑰的額外負荷或成本，您可以使用 AWS 受管金鑰。這種類型的金鑰存在於您的帳戶中，但只能在特定情況下使用。它只能在 AWS 服務 您正在操作的 內容中使用，而且只能由包含金鑰的帳戶內的主體使用。您無法管理有關這些金鑰生命週期或許可的任何內容。有些 AWS 服務 使用 AWS 受管金鑰。 AWS 受管金鑰別名的格式為 `aws/<service code>`。例如， `aws/ebs`金鑰只能用來加密與金鑰位於相同帳戶中的 Amazon Elastic Block Store (Amazon EBS) 磁碟區，而且只能由該帳戶中的 IAM 主體使用。 AWS 受管金鑰只能由該帳戶中的使用者和該帳戶中的資源使用。您無法與其他 帳戶共用在 AWS 受管金鑰下加密的資源。如果您的使用案例有此限制，我們建議您改用客戶受管金鑰；您可以與任何其他帳戶共用該金鑰的使用。您的帳戶中存在 AWS 受管金鑰不需要付費，但您需為 AWS 服務 指派給金鑰的 使用此金鑰類型付費。

AWS 受管金鑰是自 2021 AWS 服務 年起不再為新 建立的舊版金鑰類型。反之，新的 （和舊版） AWS 服務 預設會使用 AWS 擁有的金鑰來加密您的資料。 AWS 擁有的金鑰是 AWS 服務 擁有和管理以用於多個 的 KMS 金鑰集合 AWS 帳戶。雖然這些金鑰不在您的 中 AWS 帳戶，但 AWS 服務 可以使用一個金鑰來保護您帳戶中的資源。

建議您在精細控制最重要時使用客戶受管金鑰，並在便利性最重要時使用 AWS 擁有的金鑰。

下表說明每個金鑰類型之間的金鑰政策、記錄、管理和定價差異。如需金鑰類型的詳細資訊，請參閱 AWS KMS 概念。

考量事項	客戶自管金鑰	AWS 受管金鑰	AWS 擁有的金鑰
金鑰政策	由客戶獨家控制	由服務控制；可由客戶檢視	完全控制，且只能由加密資料的 AWS 服務進行檢視
日誌	AWS CloudTrail 客戶追蹤或事件資料存放區	CloudTrail 客戶追蹤或事件資料存放區	客戶無法檢視
生命週期管理	客戶管理輪換、刪除和 AWS 區域	AWS 服務 管理輪換（每年）、刪除和區域	AWS 服務 管理輪換（每年）、刪除和區域
定價	金鑰存在的每月費用（每小時按比例）；呼叫者需支付 API 用量的費用	金鑰存在不收取費用；呼叫者需支付 API 用量的費用	不向客戶收費

選擇 AWS KMS 金鑰存放區

金鑰存放區是存放和使用密碼編譯金鑰材料的安全位置。金鑰存放區的產業最佳實務是使用稱為硬體安全模組 (HSM) 的裝置，該裝置已在安全層級 3 的 NIST 聯邦資訊處理標準 (FIPS) 140 密碼編譯模組驗證計劃下進行驗證。還有其他計劃可支援用於處理付款的金鑰存放區。 AWS Payment Cryptography 是一項服務，可用來保護與付款工作負載相關的資料。

AWS KMS 支援多種金鑰存放區類型，以協助在使用 AWS KMS 建立和管理加密金鑰時保護您的金鑰材料。提供的所有金鑰存放區選項 AWS KMS 都會在安全層級 3 的 FIPS 140 下持續驗證。它們旨在防止任何人，包括 AWS 運算子，在沒有您的許可的情況下存取您的純文字金鑰或使用它們。如需可用金鑰存放區類型的詳細資訊，請參閱 AWS KMS 文件中的金鑰存放區。

AWS KMS 標準金鑰存放區是大多數工作負載的最佳選擇。如果您需要選擇不同類型的金鑰存放區，請仔細考慮是否有法規或其他要求（例如內部）強制做出此選擇，並仔細權衡成本和利益。

刪除和停用 KMS 金鑰

刪除 KMS 金鑰可能會產生重大影響。在您刪除不再打算使用的 KMS 金鑰之前，請考慮是否足以將金鑰狀態設定為已停用。當金鑰停用時，就無法用於密碼編譯操作。它仍然存在於 中 AWS，您可以視需要在未來重新啟用它。停用的金鑰會持續產生儲存費用。建議您停用金鑰，不要刪除它們，直到您確信金鑰不會保護任何資料或資料金鑰為止。

> **Important**
>
> 必須仔細規劃刪除金鑰。如果已刪除對應的金鑰，則無法解密資料。刪除後 AWS 就無法復原已刪除的金鑰。如同 中的其他關鍵操作 AWS，您應該套用政策，限制誰可以排程刪除金鑰，並且需要多重要素驗證 (MFA) 才能刪除金鑰。

為了協助防止意外刪除金鑰， 會在`DeleteKey`呼叫執行後 AWS KMS 強制執行預設最短等待期七天，然後再刪除金鑰。您可以將等待期間設定為最大值 30 天。在等待期間，金鑰仍會 AWS KMS 以待定刪除狀態存放在 中。它無法用於加密或解密操作。任何嘗試使用處於待定刪除狀態的金鑰進行加密或解密都會記錄到 AWS CloudTrail。您可以在 CloudTrail 日誌中為這些事件設定 Amazon CloudWatch 警示。 CloudTrail 如果您收到這些事件的警示，您可以視需要選擇取消刪除程序。在等待期間到期之前，您可以從待定刪除狀態復原金鑰，並將其還原為已停用或已啟用狀態。

刪除多區域金鑰需要您在原始複本之前刪除複本。如需詳細資訊，請參閱刪除多區域金鑰。

如果您使用具有匯入金鑰材料的金鑰，您可以立即刪除匯入的金鑰材料。這與以多種方式刪除 KMS 金鑰不同。當您執行`DeleteImportedKeyMaterial`動作時， 會 AWS KMS 刪除金鑰材料，且金鑰狀態會變更為待匯入。刪除金鑰材料後，金鑰會立即無法使用。沒有等待期間。若要再次啟用 金鑰，您需要再次匯入相同的金鑰材料。KMS 金鑰刪除的等待期間也適用於具有匯入金鑰材料的 KMS 金鑰。

如果資料金鑰受到 KMS 金鑰保護且由 主動使用 AWS 服務，則如果其關聯的 KMS 金鑰已停用或將其匯入的金鑰材料刪除，則不會立即受到影響。例如，假設使用具有匯入資料的金鑰來加密具有 SSE-KMS 的物件。您正在將物件上傳至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。將物件上傳至儲存貯體之前，請將材料匯入金鑰。上傳物件之後，您可以從該金鑰刪除匯入的金鑰材料。物件會保持在加密狀態的儲存貯體中，但在刪除的金鑰材料重新匯入金鑰之前，沒有人可以存取物件。雖然此流程需要精確的自動化，才能從金鑰匯入和刪除金鑰材料，但它可以在 環境中提供額外的控制層級。

AWS 提供規範性指引，協助您監控和修復 （如有必要） 排定的 KMS 金鑰刪除。如需詳細資訊，請參閱監控和修復 AWS KMS 金鑰的排程刪除。

的資料保護最佳實務 AWS KMS

本節可協助您選擇資料保護的 AWS Key Management Service (AWS KMS) 金鑰用量，例如每個資料類型要使用的金鑰。它也提供使用 AWS KMS 搭配不同 的特定範例 AWS 服務。這些建議和範例可協助您了解可能需要多少金鑰，以及哪些委託人需要使用這些金鑰的許可。

本節也會討論金鑰輪換。金鑰輪換是將現有 KMS 金鑰取代為新金鑰，或將與現有 KMS 金鑰相關聯的密碼編譯材料取代為新材料。本指南提供如何輪換常用 KMS 金鑰的範例和指示 AWS 服務。這些建議和範例旨在協助您對金鑰輪換策略做出明智的選擇。

最後，本節會針對如何在應用程式中實作用戶端加密的工具 AWS Encryption SDK，提供如何使用 的建議。本節包含您可以根據 的功能集和功能進行的設計選擇 AWS Encryption SDK。

本節討論下列加密主題：

- 使用 加密 AWS KMS
- 影響 AWS KMS 範圍的金鑰輪換
- 使用 的建議 AWS Encryption SDK

使用 加密 AWS KMS

加密是保護敏感資訊機密性和完整性的一般最佳實務。您應該使用現有的資料分類層級，每個層級至少有一個 AWS Key Management Service (AWS KMS) 金鑰。例如，您可以為分類為機密的資料定義 KMS 金鑰，為僅限內部的資料定義 KMS 金鑰，為敏感資料定義 KMS 金鑰。這可協助您確保只有授權使用者才具有使用與每個分類層級相關聯金鑰的許可。

> **Note**
>
> 單一客戶受管 KMS 金鑰可用於儲存特定分類資料的任意組合 AWS 服務 或您自己的應用程式。在多個工作負載中使用金鑰的限制因素 AWS 服務 ，是控制一組使用者對資料的存取所需的複雜程度。 AWS KMS 金鑰政策 JSON 文件必須小於 32 KB。如果此大小限制成為限制，請考慮使用AWS KMS 授予或建立多個金鑰，以將金鑰政策文件的大小降至最低。

您也可以選擇在單一 中指派用於資料分類的 KMS 金鑰，而不是僅依賴資料分類來分割 KMS 金鑰 AWS 服務。例如，Amazon Simple Storage Service (Amazon S3) `Sensitive`中標記的所有資料都應使用名稱為 的 KMS 金鑰加密`S3-Sensitive`。您可以在定義的資料分類和 AWS 服務 /或應用程式

中，進一步將資料分散到多個 KMS 金鑰。例如，您可以刪除特定時段中的某些資料集，並在不同的時段刪除其他資料集。您可以使用資源標籤來協助您識別和排序使用特定 KMS 金鑰加密的資料。

如果您選擇 KMS 金鑰的分散式管理模型，您應該套用護欄，以確保已建立具有指定分類的新資源，並使用具有適當許可的預期 KMS 金鑰。如需如何使用自動化強制執行、偵測和管理資源組態的詳細資訊，請參閱本指南的 偵測和監控一節。

本節討論下列加密主題：

- 使用 記錄資料加密 AWS KMS
- 預設加密
- 使用 進行資料庫加密 AWS KMS
- 使用 進行 PCI DSS 資料加密 AWS KMS
- 搭配 Amazon EC2 Auto Scaling 使用 KMS 金鑰

使用 記錄資料加密 AWS KMS

許多 AWS 服務，例如 Amazon GuardDuty 和 AWS CloudTrail，提供選項來加密傳送至 Amazon S3 的日誌資料。從 GuardDuty 匯出問題清單至 Amazon S3 時，您必須使用 KMS 金鑰。我們建議您加密所有日誌資料，並僅將解密存取權授予授權委託人，例如安全團隊、事件回應者和稽核人員。

AWS 安全參考架構建議建立中央 AWS 帳戶 記錄。當您這樣做時，您也可以降低金鑰管理開銷。例如，使用 CloudTrail，您可以建立組織追蹤或事件資料存放區，以記錄整個組織的事件。當您設定組織追蹤或事件資料存放區時，您可以在指定的記錄帳戶中指定單一 Amazon S3 儲存貯體和 KMS 金鑰。此組態適用於組織中的所有成員帳戶。然後，所有帳戶都會將其 CloudTrail 日誌傳送至記錄帳戶中的 Amazon S3 儲存貯體，並使用指定的 KMS 金鑰加密日誌資料。您需要更新此 KMS 金鑰的金鑰政策，才能授予 CloudTrail 使用金鑰的必要許可。如需詳細資訊，請參閱 CloudTrail 文件中的設定 CloudTrail 的 AWS KMS 金鑰政策。

為了協助保護 GuardDuty 和 CloudTrail 日誌，Amazon S3 儲存貯體和 KMS 金鑰必須位於相同位置 AWS 區域。 AWS 安全參考架構也提供記錄和多帳戶架構的指引。在跨多個區域和帳戶彙總日誌時，請參閱 CloudTrail 文件中的為組織建立追蹤，以進一步了解選擇加入區域，並確保您的集中式日誌依設計運作。

預設加密

AWS 服務 存放或處理的資料通常會提供靜態加密。此安全功能可在不使用資料時進行加密，協助保護您的資料。授權使用者仍然可以在需要時存取它。

實作和加密選項會有所不同 AWS 服務。根據預設，許多 會提供加密。請務必了解加密如何為您使用的每個服務運作。下列是一些範例：

- Amazon Elastic Block Store (Amazon EBS) – 當您預設啟用加密時，所有新的 Amazon EBS 磁碟區和快照複本都會加密。 AWS Identity and Access Management (IAM) 角色或使用者無法使用未加密的磁碟區或不支援加密的磁碟區啟動執行個體。此功能可確保存放在 Amazon EBS 磁碟區上的所有資料都已加密，有助於安全、合規和稽核。如需此服務中加密的詳細資訊，請參閱 Amazon EBS 文件中的 Amazon EBS 加密。
- Amazon Simple Storage Service (Amazon S3) – 預設會加密所有新物件。除非您指定不同的加密選項，否則 Amazon S3 會自動將伺服器端加密與 Amazon S3 受管金鑰 (SSE-S3) 套用至每個新物件。IAM 主體仍然可以在 API 呼叫中明確指出，將未加密的物件上傳至 Amazon S3。在 Amazon S3 中，若要強制執行 SSE-KMS 加密，您必須使用具有需要加密條件的儲存貯體政策。如需範例政策，請參閱 Amazon S3 文件中寫入儲存貯體的所有物件都需要 SSE-KMS。 Amazon S3 有些 Amazon S3 儲存貯體會接收並提供大量物件。如果這些物件使用 KMS 金鑰加密，大量的 Amazon S3 操作會產生大量的 `GenerateDataKey`和 `Decrypt`呼叫 AWS KMS。這可能會增加您因 AWS KMS 使用而產生的費用。您可以設定 Amazon S3 儲存貯體金鑰，這可能會大幅降低您的 AWS KMS 成本。如需此服務中加密的詳細資訊，請參閱 Amazon S3 文件中的使用加密保護資料。
- Amazon DynamoDB – DynamoDB 是全受管的 NoSQL 資料庫服務，預設啟用靜態伺服器端加密，您無法停用它。我們建議您使用客戶受管金鑰來加密 DynamoDB 資料表。此方法透過鎖定 AWS KMS 金鑰政策中的特定 IAM 使用者和角色，協助您實作具有精細許可和職責分離的最低權限。您也可以在設定 DynamoDB 資料表的加密設定時，選擇 AWS 受管或 AWS 擁有的金鑰。對於需要高度保護的資料（其中資料應僅顯示為用戶端的純文字），請考慮搭配AWS 資料庫加密 SDK 使用用戶端加密。如需此服務中加密的詳細資訊，請參閱 DynamoDB 文件中的資料保護。

使用 進行資料庫加密 AWS KMS

您實作加密的層級會影響資料庫功能。以下是您必須考慮的權衡：

- 如果您僅使用 AWS KMS 加密，則會針對 DynamoDB 和 Amazon Relational Database Service (Amazon RDS) 加密備份資料表的儲存體。這表示執行資料庫的作業系統會將儲存體的內容視為純文字。所有資料庫函數，包括索引產生和其他需要存取純文字資料的高階函數，都會繼續如預期運作。
- Amazon RDS 建置於 Amazon Elastic Block Store (Amazon EBS) 加密以提供資料庫磁碟區的完整磁碟加密。當您使用 Amazon RDS 建立加密資料庫執行個體時，Amazon RDS 會代表您建立加密的 Amazon EBS 磁碟區來存放資料庫。存放在磁碟區、資料庫快照、自動備份和僅供讀取複本上的靜態資料都會以您在建立資料庫執行個體時指定的 KMS 金鑰進行加密。

- Amazon Redshift 與 整合， AWS KMS 並建立四層金鑰階層，用於透過資料層級加密叢集層級。啟動叢集時，您可以選擇使用 AWS KMS 加密。在記憶體中開啟（和解密）資料表時，只有 Amazon Redshift 應用程式和具有適當許可的使用者可以看到純文字。這大致上類似於某些商業資料庫中可用的透明或資料表型資料加密 (TDE) 功能。這表示所有資料庫函數，包括索引產生和其他需要存取純文字資料的高階函數，都會繼續如預期般運作。
- 透過AWS 資料庫加密 SDK（和類似工具）實作的用戶端資料層級加密，表示作業系統和資料庫都只會看到加密文字。使用者只有在從已安裝 AWS 資料庫加密 SDK 的用戶端存取資料庫，且有權存取相關金鑰時，才能檢視純文字。需要存取純文字才能如預期運作的高階資料庫函數，例如產生索引，如果導向在加密欄位上操作，則無法運作。選擇使用用戶端加密時，請務必使用強大的加密機制，協助防止對加密資料的常見攻擊。這包括使用強大的加密演算法和適當的技術，例如 salt，以協助緩解加密文字攻擊。

我們建議您使用 AWS 資料庫服務的 AWS KMS 整合加密功能。對於處理敏感資料的工作負載，敏感資料欄位應考慮用戶端加密。使用用戶端加密時，您應該考慮對資料庫存取的影響，例如 SQL 查詢內的聯結或索引建立。

使用 進行 PCI DSS 資料加密 AWS KMS

中的安全和品質控制 AWS KMS 已經過驗證和認證，符合支付卡產業資料安全標準 (PCI DSS) 的要求。這表示您可以使用 KMS 金鑰加密主要帳戶號碼 (PAN) 資料。使用 KMS 金鑰來加密資料，可免除管理加密程式庫的一些負擔。此外，無法從 匯出 KMS 金鑰 AWS KMS，這可減少對以不安全方式存放加密金鑰的疑慮。

您可以使用其他方法來 AWS KMS 滿足 PCI DSS 要求。例如，如果您使用 AWS KMS 搭配 Amazon S3，您可以將 PAN 資料儲存在 Amazon S3 中，因為每個服務的存取控制機制與其他服務不同。

一如往常，檢閱您的合規要求時，請務必從經驗豐富、合格且經過驗證的對象取得建議。當您設計直接使用 金鑰來保護 PCI DSS 範圍內卡片交易資料的應用程式時，請注意AWS KMS 請求配額。

由於所有 AWS KMS 請求都已登入 AWS CloudTrail，因此您可以透過檢閱 CloudTrail 日誌來稽核金鑰用量。不過，如果您使用 Amazon S3 儲存貯體金鑰，則沒有對應至每個 Amazon S3 動作的項目。這是因為儲存貯體金鑰會加密您用來加密 Amazon S3 中物件的資料金鑰。雖然使用儲存貯體金鑰不會消除所有 API 呼叫 AWS KMS，但會減少它們的數量。因此，Amazon S3 物件存取嘗試和 API 呼叫之間不再有one-to-one的比對 AWS KMS。

搭配 Amazon EC2 Auto Scaling 使用 KMS 金鑰

Amazon EC2 Auto Scaling 是自動化 Amazon EC2 執行個體擴展的建議服務。它可協助您確保擁有正確數量的執行個體，以處理應用程式的負載。Amazon EC2 Auto Scaling 使用服務連結角色，為服

務提供適當的許可，並授權其在您帳戶中的活動。若要搭配 Amazon EC2 Auto Scaling 使用 KMS 金鑰，您的 AWS KMS 金鑰政策必須允許服務連結角色搭配某些 API 操作使用您的 KMS 金鑰，例如 `Decrypt`，自動化才有用。如果 AWS KMS 金鑰政策未授權執行操作的 IAM 主體執行動作，則該動作將被拒絕。如需如何在金鑰政策中正確套用許可以允許存取的詳細資訊，請參閱 Amazon EC2 Auto Scaling 文件中的 Amazon EC2 Auto Scaling 中的資料保護。 Amazon EC2 Auto Scaling

影響 AWS KMS 範圍的金鑰輪換

除非您需要輪換金鑰以符合法規，否則我們不建議 AWS Key Management Service (AWS KMS) 金鑰輪換。例如，由於商業政策、合約規則或政府法規，您可能需要輪換 KMS 金鑰。的設計可 AWS KMS 大幅降低通常用於緩解金鑰輪換的風險類型。如果您必須輪換 KMS 金鑰，建議您使用自動金鑰輪換，只有在不支援自動金鑰輪換時，才使用手動金鑰輪換。

本節討論下列金鑰輪換主題：

- AWS KMS 對稱金鑰輪換
- Amazon EBS 磁碟區的金鑰輪換
- Amazon RDS 的金鑰輪換
- Amazon S3 和同區域複寫的金鑰輪換
- 使用匯入的資料輪換 KMS 金鑰

AWS KMS 對稱金鑰輪換

AWS KMS 僅支援使用 AWS KMS 建立的金鑰材料進行對稱加密 KMS 金鑰的自動金鑰輪換。對於客戶受管 KMS 金鑰，自動輪換是選用的。會每年 AWS KMS 輪換 AWS 受管 KMS 金鑰的金鑰材料。 會永久 AWS KMS 儲存所有先前版本的密碼編譯材料，因此您可以解密使用該 KMS 金鑰加密的任何資料。AWS KMS 不會刪除任何輪換的金鑰材料，直到您刪除 KMS 金鑰為止。此外，當您使用 解密物件時 AWS KMS，服務會決定用於解密操作的正確備份材料；不需要提供其他輸入參數。

由於 會 AWS KMS 保留舊版本的密碼編譯金鑰材料，而且由於您可以使用該材料來解密資料，因此金鑰輪換不會提供任何額外的安全性優勢。如果您在法規要求或其他要求的情況下操作工作負載，金鑰輪換機制可以更輕鬆地輪換金鑰。

Amazon EBS 磁碟區的金鑰輪換

您可以使用下列其中一種方法輪換 Amazon Elastic Block Store (Amazon EBS) 資料金鑰。方法取決於您的工作流程、部署方法和應用程式架構。從 AWS 受管金鑰變更為客戶受管金鑰時，您可能想要執行此操作。

使用作業系統工具將資料從一個磁碟區複製到另一個磁碟區

1. 建立新的 KMS 金鑰。如需說明，請參閱建立 KMS 金鑰。
2. 建立新的 Amazon EBS 磁碟區，其大小與原始磁碟區相同或大於原始磁碟區。針對加密，指定您建立的 KMS 金鑰。如需說明，請參閱建立 Amazon EBS 磁碟區。
3. 將新磁碟區掛載在與原始磁碟區相同的執行個體或容器上。如需說明，請參閱將 Amazon EBS 磁碟區連接至 Amazon EC2 執行個體。
4. 使用您偏好的作業系統工具，將資料從現有磁碟區複製到新磁碟區。
5. 當同步完成時，在預先排定的維護時段期間，停止執行個體的流量。如需說明，請參閱手動停止和啟動您的執行個體。
6. 卸載原始磁碟區。如需說明，請參閱從 Amazon EC2 執行個體分離 Amazon EBS 磁碟區。
7. 將新磁碟區掛載至原始掛載點。
8. 驗證新磁碟區是否正常運作。
9. 刪除原始磁碟區。如需說明，請參閱刪除 Amazon EBS 磁碟區。

使用 Amazon EBS 快照將資料從一個磁碟區複製到另一個磁碟區

1. 建立新的 KMS 金鑰。如需說明，請參閱建立 KMS 金鑰。
2. 建立原始磁碟區的 Amazon EBS 快照。如需說明，請參閱建立 Amazon EBS 快照。
3. 從快照建立新磁碟區。對於加密，請指定您建立的新 KMS 金鑰。如需說明，請參閱建立 Amazon EBS 磁碟區。

> **Note**
>
> 根據您的工作負載，您可能想要使用 Amazon EBS 快速快照還原，將磁碟區的初始延遲降至最低。

4. 建立新的 Amazon EC2 執行個體。如需說明，請參閱啟動 Amazon EC2 執行個體。
5. 將您建立的磁碟區連接到 Amazon EC2 執行個體。如需說明，請參閱將 Amazon EBS 磁碟區連接至 Amazon EC2 執行個體。
6. 將新執行個體輪換到生產環境。
7. 將原始執行個體從生產環境輪換並刪除。如需說明，請參閱刪除 Amazon EBS 磁碟區。

> **Note**
>
> 您可以複製快照並修改用於目標複製的加密金鑰。複製快照並使用您偏好的 KMS 金鑰加密快照後，您也可以從快照建立 Amazon Machine Image (AMI)。如需詳細資訊，請參閱 Amazon EC2 文件中的 Amazon EBS 加密。 Amazon EC2

Amazon RDS 的金鑰輪換

對於某些服務，例如 Amazon Relational Database Service (Amazon RDS)，資料加密發生在服務內並由 提供 AWS KMS。使用下列指示來輪換 Amazon RDS 資料庫執行個體的金鑰。

輪換 Amazon RDS 資料庫的 KMS 金鑰

1. 建立原始加密資料庫的快照。如需說明，請參閱 Amazon RDS 文件中的管理手動備份。
2. 將快照複製到新的快照。對於加密，請指定新的 KMS 金鑰。如需說明，請參閱複製 Amazon RDS 的資料庫快照。
3. 使用新的快照來建立新的 Amazon RDS 叢集。如需說明，請參閱 Amazon RDS 文件中的還原至資料庫執行個體。根據預設，叢集會使用新的 KMS 金鑰。
4. 驗證新資料庫的操作及其中的資料。
5. 將新資料庫輪換到生產環境。
6. 將舊資料庫從生產環境中輪換並刪除。如需說明，請參閱刪除資料庫執行個體。

Amazon S3 和同區域複寫的金鑰輪換

對於 Amazon Simple Storage Service (Amazon S3)，若要變更物件的加密金鑰，您需要讀取和重寫物件。當您重寫物件時，您會在寫入操作中明確指定新的加密金鑰。若要對許多物件執行此操作，您可以使用 Amazon S3 Batch Operations。在任務設定中，針對複製操作，指定新的加密設定。例如，您可以選擇 SSE-KMS 並輸入 keyId。

或者，您可以使用 Amazon S3 相同區域複寫 (SRR)。SSR 可以重新加密傳輸中的物件。

使用匯入的資料輪換 KMS 金鑰

AWS KMS 不會復原或輪換您匯入的金鑰材料。若要使用匯入的金鑰材料輪換 KMS 金鑰，您必須手動輪換金鑰。

使用 的建議 AWS Encryption SDK

AWS Encryption SDK 是在應用程式中實作用戶端加密的強大工具。程式庫適用於 Java、JavaScript、C、Python 和其他程式設計語言。它與 AWS Key Management Service (AWS KMS) 整合。您也可以將其用作獨立的 SDK，而無需參考 KMS 金鑰。

使用此工具的建議實務包括仔細考慮應用程式的需求。平衡這些需求與特定組態可能帶來的風險，例如將金鑰快取引入您的應用程式。如需資料金鑰快取的詳細資訊，請參閱 AWS Encryption SDK 文件中的資料金鑰快取。

在決定是否使用 時，請考慮下列問題 AWS Encryption SDK：

- 與 整合的 服務進行伺服器端加密時，是否有無法滿足的用戶端加密需求 AWS KMS？
- 您能否充分保護用於加密資料用戶端的金鑰，以及如何執行此操作？
- 是否有其他fit-for-purpose的加密程式庫，可能更適合您的使用案例？ 考慮替代 AWS 產品，例如 Amazon S3 用戶端加密和AWS 資料庫加密 SDK。

如需為您的使用案例選擇適當服務的詳細資訊，請參閱 AWS Crypto Tools 文件。

的身分和存取管理最佳實務 AWS KMS

若要使用 AWS Key Management Service (AWS KMS)，您必須擁有 AWS 可用於驗證和授權請求的登入資料。除非明確提供該許可且從未拒絕，否則任何 AWS 委託人都沒有任何 KMS 金鑰的許可。沒有使用或管理 KMS 金鑰的隱含或自動許可。本節中的主題定義安全最佳實務，協助您判斷應使用哪些 AWS KMS 存取控制控制來保護基礎設施。

本節討論下列身分和存取管理主題：

- AWS KMS 金鑰政策和 IAM 政策
- 的最低權限許可 AWS KMS
- 的角色型存取控制 AWS KMS
- 的屬性型存取控制 AWS KMS
- 的加密內容 AWS KMS
- 故障診斷 AWS KMS 許可

AWS KMS 金鑰政策和 IAM 政策

管理 AWS KMS 資源存取權的主要方法是使用 政策。政策是描述哪些主體可以存取哪些資源的文件。連接到 AWS Identity and Access Management (IAM) 身分 （使用者、使用者群組或角色） 的政策稱為以身分為基礎的政策。連接到資源的 IAM 政策稱為以資源為基礎的政策。KMS 金鑰的資源 AWS KMS 政策稱為金鑰政策。除了 IAM 政策和 AWS KMS 金鑰政策之外， AWS KMS 還支援授予。授予提供靈活且強大的方法來委派許可。您可以使用授予，對 AWS 帳戶 或其他 中的 IAM 主體發出有時間限制的 KMS 金鑰存取 AWS 帳戶。

所有 KMS 金鑰都擁有金鑰政策。如果您沒有提供，請為您 AWS KMS 建立一個。 AWS KMS 使用的預設金鑰政策會因您使用 AWS KMS 主控台或使用 AWS KMS API 建立金鑰而有所不同。我們建議您編輯預設金鑰政策，以符合組織對最低權限許可的要求。這也應該符合您搭配金鑰政策使用 IAM 政策的策略。如需搭配 使用 IAM 政策的更多建議 AWS KMS，請參閱 AWS KMS 文件中的 IAM 政策最佳實務。

您可以使用金鑰政策，將 IAM 主體的授權委派給身分型政策。您也可以使用金鑰政策搭配身分型政策來精簡授權。在任何一種情況下，金鑰政策和身分型政策都會決定存取，以及限制存取的任何其他適用政策，例如服務控制政策 (SCPs)、資源控制政策 RCPs) 或許可界限。如果委託人位於與 KMS 金鑰不同的帳戶中，基本上，僅支援密碼編譯和授予動作。如需此跨帳戶案例的詳細資訊，請參閱 文件中的 AWS KMS 允許其他帳戶中的使用者使用 KMS 金鑰。

您必須使用 IAM 身分型政策搭配金鑰政策來控制對 KMS 金鑰的存取。授予也可以與這些政策結合使用，以控制對 KMS 金鑰的存取。若要使用身分型政策來控制對 KMS 金鑰的存取，金鑰政策必須允許帳戶使用身分型政策。您可以指定啟用 IAM 政策的金鑰政策陳述式，也可以在金鑰政策中明確指定允許的主體。

撰寫政策時，請確保您有強大的控制，限制誰可以執行下列動作：

- 更新、建立和刪除 IAM 政策和 KMS 金鑰政策
- 從使用者、角色和群組連接和分離身分型政策
- 從 KMS AWS KMS 金鑰連接和分離金鑰政策
- 為您的 KMS 金鑰建立授予 – 無論您只使用金鑰政策控制對 KMS 金鑰的存取，還是將金鑰政策與 IAM 政策結合，都應該限制修改政策的能力。實作核准程序，以變更任何現有的政策。核准程序有助於防止下列情況：
  - 意外遺失 IAM 主體許可 – 可以進行變更，以防止 IAM 主體能夠管理金鑰或在密碼編譯操作中使用金鑰。在極端情況下，可以從所有使用者撤銷金鑰管理許可。如果發生這種情況，您需要聯絡 AWS 支援 以重新取得 金鑰的存取權。
  - 未經核准的 KMS 金鑰政策變更 – 如果未經授權的使用者取得金鑰政策的存取權，他們可以修改它，以將許可委派給非預期的 AWS 帳戶 或 委託人。
  - 未經核准的 IAM 政策變更 – 如果未經授權的使用者取得一組具有管理群組成員資格許可的登入資料，他們可以提升自己的許可，並變更您的 IAM 政策、金鑰政策、KMS 金鑰組態或其他 AWS 資源組態。

仔細檢閱與指定為 KMS 金鑰管理員的 IAM 主體相關聯的 IAM 角色和使用者。這有助於防止未經授權的刪除或變更。如果您需要變更有權存取 KMS 金鑰的主體，請確認新的管理員主體已新增至所有必要的金鑰政策。先測試其許可，再刪除先前的管理委託人。我們強烈建議遵循所有 IAM 安全最佳實務，並使用暫時登入資料而非長期登入資料。

如果您在建立政策時不知道委託人的名稱，或者需要存取的委託人經常變更，建議您透過授予發出有時間限制的存取。承授者主體可以位於與 KMS 金鑰相同的帳戶中，也可以位於不同的帳戶中。如果委託人和 KMS 金鑰位於不同的帳戶中，則除了授予之外，您還必須指定身分型政策。授予需要額外的管理，因為您必須呼叫 API 來建立授予，並在不再需要授予時淘汰或撤銷授予。

除非在金鑰政策、IAM 政策或授予中明確允許且未明確拒絕 KMS 金鑰，否則任何 AWS 委託人，包括帳戶根使用者或金鑰建立者，都沒有任何許可。延伸時，您應該考慮如果使用者取得使用 KMS 金鑰的意外存取權，會發生什麼情況，以及影響會是什麼。若要降低此類風險，請考慮下列事項：

- 您可以為不同類別的資料維護不同的 KMS 金鑰。這可協助您分隔金鑰，並維護更簡潔的金鑰政策，其中包含專門以主體存取該資料類別為目標的政策陳述式。這也表示，如果意外存取相關的 IAM 登入資料，則與該存取關聯的身分只能存取 IAM 政策中指定的金鑰，而且只有在金鑰政策允許存取該主體時。
- 您可以評估具有金鑰意外存取的使用者是否可以存取資料。例如，使用 Amazon Simple Storage Service (Amazon S3)，使用者也必須具有適當的許可才能存取 Amazon S3 中的加密物件。或者，如果使用者對具有磁碟區以 KMS 金鑰加密的 Amazon EC2 執行個體具有意外存取 （使用 RDP 或 SSH)，則使用者可以使用作業系統工具來存取資料。

> **Note**
>
> AWS 服務 使用 的 AWS KMS 不會向使用者公開加密文字 （最新的加密分析方法需要存取加密文字 ）。此外，加密文字不適用於 AWS 資料中心外部的實體檢查，因為所有儲存媒體在除役時都會根據 NIST SP800-88 要求實際銷毀。

的最低權限許可 AWS KMS

由於 KMS 金鑰會保護敏感資訊，因此建議您遵循最低權限存取的原則。當您定義金鑰政策時，委派執行任務所需的最低許可。只有在您計劃使用其他身分型政策進一步限制許可時，才允許 KMS 金鑰政策上的所有動作 (`kms:*`)。如果您計劃使用身分型政策管理許可，請限制誰能夠建立 IAM 政策並將其連接到 IAM 主體，並監控政策變更。

如果您同時允許金鑰政策和身分型政策中的所有動作 (`kms:*`)，委託人會同時擁有 KMS 金鑰的管理和使用許可。作為安全最佳實務，我們建議僅將這些許可委派給特定的委託人。考慮如何將許可指派給將管理金鑰的委託人，以及將使用您的金鑰的委託人。您可以透過在金鑰政策中明確命名主體，或限制連接身分型政策的主體來執行此操作。您也可以使用條件金鑰來限制許可。例如，如果發出 API 呼叫的委託人具有條件規則中指定的標籤，您可以使用 aws：PrincipalTag 來允許所有動作。

如需了解政策陳述式如何評估的說明 AWS，請參閱 IAM 文件中的政策評估邏輯。我們建議您在撰寫政策之前檢閱此主題，以協助降低政策產生意外效果的機會，例如提供存取權給不應存取的主體。

> **Tip**
>
> 在非生產環境中測試應用程式時，請使用 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) 協助您在 IAM 政策中套用最低權限許可。

如果您使用 IAM 使用者而非 IAM 角色，強烈建議使用AWS 多重要素驗證 (MFA) 來緩解長期憑證的漏洞。您可以使用 MFA 執行下列操作：

- 要求使用者在執行特殊權限動作之前，使用 MFA 驗證其憑證，例如排程金鑰刪除。
- 管理員帳戶密碼和 MFA 裝置在個人之間分割擁有權，以實作分割授權。

如需可協助您設定最低權限許可的範例政策，請參閱 AWS KMS 文件中的 IAM 政策範例。

的角色型存取控制 AWS KMS

角色型存取控制 (RBAC) 是一種授權策略，僅提供使用者執行其任務所需的許可，不會再提供其他許可。這是一種方法，可協助您實作最低權限原則。

AWS KMS 支援 RBAC。它可讓您透過在金鑰政策中指定精細許可來控制對金鑰的存取。金鑰政策會指定資源、動作、效果、主體和選用條件，以授予金鑰的存取權。若要在 中實作 RBAC AWS KMS，我們建議區隔金鑰使用者和金鑰管理員的許可。

對於金鑰使用者，請僅指派使用者所需的許可。使用下列問題來協助您進一步精簡許可：

- 哪些 IAM 主體需要存取金鑰？
- 每個委託人需要使用 金鑰執行哪些動作？ 例如，委託人只需要 `Encrypt`和 `Sign`許可嗎？
- 委託人需要存取哪些資源？
- 實體是人類還是 AWS 服務？ 如果是服務，您可以使用 kms:ViaService 條件金鑰，將金鑰用量限制在特定服務。

對於金鑰管理員，請僅指派管理員所需的許可。例如，管理員的許可可能會因金鑰是否用於測試或生產環境而有所不同。如果您在特定非生產環境中使用較不嚴格的許可，請在政策發佈至生產環境之前實作程序來測試政策。

如需可協助您為金鑰使用者和管理員設定角色型存取控制的範例政策，請參閱 RBAC for AWS KMS。

的屬性型存取控制 AWS KMS

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性定義許可。如同 RBAC，這是一種可協助您實作最低權限原則的方法。

AWS KMS 支援 ABAC，可讓您根據與目標資源相關聯的標籤定義許可，例如 KMS 金鑰，以及與發出 API 呼叫的委託人相關聯的標籤。在 中 AWS KMS，您可以使用標籤和別名來控制對客戶受管金鑰

的存取。例如，您可以定義使用標籤條件索引鍵的 IAM 政策，在委託人的標籤符合與 KMS 索引鍵相關聯的標籤時允許操作。如需教學課程，請參閱 文件中根據標籤定義存取 AWS 資源的許可。 AWS KMS

最佳實務是使用 ABAC 策略來簡化 IAM 政策管理。有了 ABAC，管理員可以使用標籤來允許存取新資源，而不是更新現有的政策。ABAC 需要的政策較少，因為您不必為不同的任務職能建立不同的政策。如需詳細資訊，請參閱 IAM 文件中的 ABAC 與傳統 RBAC 模型的比較。

將最低權限許可的最佳實務套用至 ABAC 模型。只為 IAM 主體提供執行其任務所需的許可。仔細控制標記 APIs存取，以允許使用者修改角色和資源上的標籤。如果您使用金鑰別名條件索引鍵在 中支援 ABAC AWS KMS，請確保您也有強大的控制項來限制誰可以建立金鑰和修改別名。

您也可以使用標籤將特定金鑰連結至商業類別，並確認指定動作正在使用正確的金鑰。例如，您可以使用 AWS CloudTrail 日誌來驗證用於執行特定 AWS KMS 動作的 金鑰是否與正在使用的資源屬於相同的業務類別。

> **Warning**
>
> 請勿在標籤金鑰或標籤值包含機密或敏感資訊。標籤不會加密。許多 都可以存取它們 AWS 服務，包括帳單。

在存取控制實作 ABAC 方法之前，請考慮您使用的其他 服務是否支援此方法。如需判斷哪些服務支援 ABAC 的說明，請參閱 AWS 服務 IAM 文件中的 與 IAM 搭配使用。

如需實作 ABAC for 的詳細資訊， AWS KMS 以及可協助您設定政策的條件金鑰，請參閱 ABAC for AWS KMS。

的加密內容 AWS KMS

所有具有對稱加密 KMS 金鑰 AWS KMS 的密碼編譯操作都接受加密內容。加密內容是一組選用的非私密金鑰/值對，可包含有關資料的其他內容資訊。最佳實務是，您可以在 中的`Encrypt`操作中插入加密內容 AWS KMS ，以增強解密 API 呼叫的授權和可稽核性 AWS KMS。 AWS KMS 會使用加密內容做為額外的驗證資料 (AAD)，以支援已驗證的加密。加密內容以密碼編譯方式繫結至加密文字，因此需要相同的加密內容才能解密資料。

加密內容不是秘密，也不被加密。它在 AWS CloudTrail 日誌中以純文字顯示，因此您可以使用它來識別和分類您的密碼編譯操作。由於加密內容不是秘密，因此您應該僅允許授權的主體存取您的 CloudTrail 日誌資料。

您也可以使用 kms:EncryptionContext：context-key 和 kms:EncryptionContextKeys 條件金鑰，根據加密內容控制對對稱加密 KMS 金鑰的存取。您也可以使用這些條件金鑰，要求加密內容用於密碼編譯操作。對於這些條件金鑰，請檢閱有關使用或ForAnyValueForAllValues設定運算子的指引，以確保您的政策反映您的預期許可。

故障診斷 AWS KMS 許可

當您撰寫 KMS 金鑰的存取控制政策時，請考慮 IAM 政策和金鑰政策如何一起運作。委託人的有效許可是所有有效政策授予（且未明確拒絕）的許可。在帳戶中，KMS 金鑰的許可可能會受到 IAM 身分型政策、金鑰政策、許可界限、服務控制政策或工作階段政策的影響。例如，如果您同時使用身分型和金鑰政策來控制對 KMS 金鑰的存取，則會評估與委託人和資源相關的所有政策，以判斷委託人執行指定動作的授權。如需詳細資訊，請參閱 IAM 文件中的政策評估邏輯。

如需故障診斷金鑰存取的詳細資訊和流程圖，請參閱 AWS KMS 文件中的故障診斷金鑰存取。

對存取遭拒錯誤訊息進行故障診斷

1. 確認 IAM 身分型政策和 KMS 金鑰政策允許存取。
2. 確認 IAM 中的許可界限未限制存取。
3. 確認 中的服務控制政策 (SCP) 或資源控制政策 (RCP) AWS Organizations 未限制存取。
4. 如果您使用的是 VPC 端點，請確認端點政策正確無誤。
5. 在身分型政策和金鑰政策中，移除限制存取金鑰的任何條件或資源參考。移除這些限制之後，請確認委託人可以成功呼叫先前失敗的 API。如果成功，請一次重新套用一個條件和資源參考，並在每個條件和資源之後驗證委託人仍然具有存取權。這可協助您識別造成錯誤的 條件或資源參考。

如需詳細資訊，請參閱 IAM 文件中的對存取遭拒錯誤訊息進行故障診斷。

的偵測和監控最佳實務 AWS KMS

偵測和監控是了解 AWS Key Management Service (AWS KMS) 金鑰可用性、狀態和用量的重要部分。監控有助於維護 AWS 解決方案的安全性、可靠性、可用性和效能。 AWS 提供數種工具來監控 KMS 金鑰和 AWS KMS 操作。本節說明如何設定和使用這些工具，以更清楚地了解您的環境，並監控 KMS 金鑰的使用情況。

本節討論下列偵測和監控主題：

- 使用 監控 AWS KMS 操作 AWS CloudTrail
- 使用 IAM Access Analyzer 監控對 KMS 金鑰的存取
- AWS 服務 使用 監控其他 的加密設定 AWS Config
- 使用 Amazon CloudWatch 警示監控 KMS 金鑰
- 使用 Amazon EventBridge 自動化回應

使用 監控 AWS KMS 操作 AWS CloudTrail

AWS KMS 已與 整合AWS CloudTrail，這項服務可記錄使用者、角色和其他 AWS KMS 對 的所有呼叫 AWS 服務。CloudTrail 會將對 的所有 API 呼叫擷取 AWS KMS 為事件，包括來自 AWS KMS 主控台、 AWS KMS APIs、 AWS CloudFormation AWS Command Line Interface (AWS CLI) 和 的呼叫 AWS Tools for PowerShell。

CloudTrail 會記錄所有 AWS KMS 操作，包括唯讀操作，例如 `ListAliases`和 `GetKeyRotationStatus`。它也會記錄管理 KMS 金鑰的操作，例如 `CreateKey`和 `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey`和 `Decrypt`。它也會記錄 為您 AWS KMS 呼叫的內部操作，例如 `DeleteExpiredKeyMaterial`、`SynchronizeMultiRegionKey`、 `DeleteKey`和 `RotateKey`。

建立 CloudTrail AWS 帳戶 時，會在您的 上啟用 CloudTrail。根據預設，事件歷史記錄會提供過去 90 天在 中記錄的管理事件 API 活動的可檢視、可搜尋、可下載和不可變記錄 AWS 區域。若要監控或稽核超過 90 天的 KMS 金鑰使用情況，建議您為 建立 CloudTrail 追蹤 AWS 帳戶。如果您已在 中建立組織 AWS Organizations，您可以建立組織追蹤或事件資料存放區，以記錄 AWS 帳戶 該組織中所有的事件。

為帳戶或組織建立追蹤之後，您可以使用其他 AWS 服務 來存放、分析和自動回應記錄於追蹤中的事件。例如，您可以執行下列動作：

- 您可以設定 Amazon CloudWatch 警示，通知您追蹤中的特定事件。如需詳細資訊，請參閱本指南中的 使用 Amazon CloudWatch 警示監控 KMS 金鑰。
- 您可以建立 Amazon EventBridge 規則，在追蹤中發生事件時自動執行 動作。如需詳細資訊，請參閱本指南中的使用 Amazon EventBridge 自動化回應。
- 您可以使用 Amazon Security Lake 從多個 收集和存放日誌 AWS 服務，包括 CloudTrail。如需詳細資訊，請參閱《Amazon Security Lake 文件》中的 AWS 服務從 Security Lake 收集資料。
- 若要增強對操作活動的分析，您可以使用 Amazon Athena 查詢 CloudTrail 日誌。如需詳細資訊，請參閱 Amazon Athena 文件中的查詢 AWS CloudTrail 日誌。

如需使用 CloudTrail 監控 AWS KMS 操作的詳細資訊，請參閱下列內容：

- 使用 記錄 AWS KMS API 呼叫 AWS CloudTrail
- AWS KMS 日誌項目的範例
- 使用 Amazon EventBridge 監控 KMS 金鑰
- CloudTrail 與 Amazon EventBridge 整合

使用 IAM Access Analyzer 監控對 KMS 金鑰的存取

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) 可協助您識別組織和帳戶中與外部實體共用的資源（例如 KMS 金鑰）。此服務可協助您識別意外或過於廣泛的資源和資料存取，這是安全風險。IAM Access Analyzer 會使用邏輯式推理來分析 AWS 環境中以資源為基礎的政策，藉此識別與外部主體共用的資源。

您可以使用 IAM Access Analyzer 來識別哪些外部實體可以存取您的 KMS 金鑰。當您啟用 IAM Access Analyzer 時，您可以為整個組織或目標帳戶建立分析器。您選擇的組織或帳戶稱為分析器的信任區域。分析器會監控信任區域內支援的資源。信任區域中的主體對資源的任何存取都會被視為受信任。

對於 KMS 金鑰，IAM Access Analyzer 會分析套用至金鑰的金鑰政策和授予。如果金鑰政策或授予允許外部實體存取金鑰，則會產生調查結果。使用 IAM Access Analyzer 來判斷外部實體是否可以存取您的 KMS 金鑰，然後驗證這些實體是否應具有存取權。

如需使用 IAM Access Analyzer 監控 KMS 金鑰存取的詳細資訊，請參閱下列內容：

- 使用 AWS Identity and Access Management Access Analyzer
- 外部存取的 IAM Access Analyzer 資源類型

- IAM Access Analyzer 資源類型： AWS KMS keys
- 外部和未使用存取的問題清單

AWS 服務 使用 監控其他 的加密設定 AWS Config

AWS Config 提供 中 AWS 資源組態的詳細檢視 AWS 帳戶。您可以使用 AWS Config 來驗證使用 KMS 金鑰 AWS 服務 的 已正確設定其加密設定。例如，您可以使用加密磁碟區 AWS Config 規則來驗證您的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是否已加密。

AWS Config 包含 受管規則，可協助您快速選擇要評估資源的規則。 AWS Config 請檢查您的 AWS 區域 ，以判斷該區域是否支援您需要的受管規則。可用的受管規則包括檢查 Amazon Relational Database Service (Amazon RDS) 快照的組態、CloudTrail 追蹤加密、Amazon Simple Storage Service (Amazon S3) 儲存貯體的預設加密、Amazon DynamoDB 資料表加密等。

您也可以建立自訂規則並套用您的商業邏輯，以判斷您的資源是否符合您的需求。GitHub 上的AWS Config 規則儲存庫提供許多受管規則的開放原始碼。這些可以是開發自訂規則的實用起點。

當資源不符合規則時，您可以啟動回應動作。 AWS Config 包含AWS Systems Manager 自動化執行的修補動作。例如，如果您已套用cloud-trail-encryption-enabled規則，且規則傳回NON_COMPLIANT結果，則 AWS Config 可以為您加密 CloudTrail 日誌，啟動可修復問題的自動化文件。

AWS Config 可讓您在佈建資源之前，主動檢查是否符合 AWS Config 規則。在主動模式下套用規則可協助您在雲端資源建立或更新之前評估這些資源的組態。在部署管道中以主動模式套用規則，可讓您在部署資源之前測試資源組態。

您也可以透過 將 AWS Config 規則實作為控制項AWS Security Hub CSPM。Security Hub CSPM 提供您可以套用至 的安全標準 AWS 帳戶。這些標準可協助您根據建議實務來評估您的環境。AWS 基礎安全最佳實務標準包含保護控制類別內的控制項，以驗證靜態加密是否已設定，且 KMS 金鑰政策遵循建議的實務。

如需使用 AWS Config 監控 中加密設定的詳細資訊 AWS 服務，請參閱下列內容：

- AWS Config入門
- AWS Config 受管規則
- AWS Config 自訂規則
- 使用 修復不合規的資源 AWS Config

使用 Amazon CloudWatch 警示監控 KMS 金鑰

Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以使用 CloudWatch 來收集和追蹤指標，這些是您可以測量的變數。

匯入金鑰材料過期或金鑰刪除，如果非預期或未適當規劃，則可能是災難性事件。建議您設定 CloudWatch 警示，以便在這些事件發生之前提醒您。我們也建議您設定 AWS Identity and Access Management (IAM) 政策 AWS Organizations 或服務控制政策 SCPs)，以防止刪除重要的金鑰。

CloudWatch 警示可協助您採取修正動作，例如取消金鑰刪除，或修補動作，例如重新匯入已刪除或過期的金鑰資料。

使用 Amazon EventBridge 自動化回應

您也可以使用 Amazon EventBridge 來通知您影響 KMS 金鑰的重要事件。EventBridge 是 AWS 服務 ，可提供近乎即時的系統事件串流，描述 AWS 資源的變更。EventBridge 會自動從 CloudTrail 和 Security Hub CSPM 接收事件。在 EventBridge 中，您可以建立回應 CloudTrail 記錄之事件的規則。

AWS KMS 事件包括下列項目：

- KMS 金鑰中的金鑰材料會自動輪換
- KMS 金鑰中匯入的金鑰材料已過期
- 已刪除已排定刪除的 KMS 金鑰

這些事件可以在 中啟動其他動作 AWS 帳戶。這些動作與上一節所述的 CloudWatch 警示不同，因為它們只能在事件發生後執行。例如，您可能想要在刪除特定金鑰之後刪除連線至特定金鑰的資源，或者您可能想要通知合規或稽核團隊該金鑰已刪除。

您也可以使用 EventBridge 來篩選在 CloudTrail 中記錄的任何其他 API 事件。這表示如果金鑰政策相關的 API 動作有特定考量，您可以篩選這些動作。例如，您可以在 EventBridge 中篩選 `PutKeyPolicy` API 動作。更廣泛地說，您可以篩選開頭為 `Disable*`或 的任何 API 動作，`Delete*`以啟動自動回應。

使用 EventBridge，您可以監控 （偵測性控制） 並調查和回應 （回應性控制） 意外或選取的事件。例如，如果建立 IAM 使用者或角色、建立 KMS 金鑰或變更金鑰政策，您可以提醒安全團隊並採取特定動作。您可以建立 EventBridge 事件規則，篩選您指定的 API 動作，然後將目標與規則建立關聯。範例目標包括 AWS Lambda 函數、Amazon Simple Notification Service (Amazon SNS) 通知、Amazon

Simple Queue Service (Amazon SQS) 佇列等。如需將事件傳送至目標的詳細資訊，請參閱 Amazon EventBridge 中的事件匯流排目標。

如需 AWS KMS 使用 EventBridge 監控和自動化回應的詳細資訊，請參閱 AWS KMS 文件中的使用 Amazon EventBridge 監控 KMS 金鑰。

的成本和帳單管理最佳實務 AWS KMS

透過廣度和深度， AWS 服務 提供彈性來管理成本，同時滿足業務需求。本節涵蓋 (AWS KMS) 中 AWS Key Management Service 金鑰儲存的定價，並提供降低成本的建議，例如透過金鑰快取。您也可以檢閱 KMS 金鑰用量，判斷是否有其他機會降低成本。

本節討論下列成本和帳單管理主題：

- AWS KMS 金鑰儲存的 定價
- 使用預設加密的 Amazon S3 儲存貯體金鑰
- 使用 快取資料金鑰 AWS Encryption SDK
- 金鑰快取和 Amazon S3 儲存貯體金鑰的替代方案
- 管理 KMS 金鑰用量的記錄成本

AWS KMS 金鑰儲存的 定價

AWS KMS key 您在 中建立的每個 AWS KMS 都會產生費用。對於對稱金鑰、非對稱金鑰、HMAC 金鑰、多區域金鑰 （每個主要金鑰和每個複本多區域金鑰）、具有匯入金鑰材料的金鑰，以及金鑰來源為 AWS CloudHSM 或外部金鑰存放區的 KMS 金鑰，每月費用相同。

對於您自動或隨需輪換的 KMS 金鑰，金鑰的第一次和第二次輪換會增加額外的每月費用 （每小時按比例分配）。在第二次輪換之後，該月的任何後續輪換都不會計費。如需最新AWS KMS 定價資訊，請參閱 定價。

您可以使用 AWS Budgets來設定用量預算。當帳戶中的花費超過特定閾值時， AWS Budgets 可以提醒您。對於與 相關的成本 AWS KMS，您可以建立用量預算，以根據 KMS 金鑰或請求發出提醒。這可以提高您對 AWS KMS 金鑰儲存和使用成本的可見性。

使用預設加密的 Amazon S3 儲存貯體金鑰

在某些使用案例中，在 Amazon Simple Storage Service (Amazon S3) 中存取或產生大量物件的工作負載可能會產生大量請求 AWS KMS，進而增加您的成本。設定 Amazon S3 儲存貯體金鑰可協助您將成本降低高達 99%。這是停用加密的建議替代方案，以協助降低與 相關的成本 AWS KMS。

使用 快取資料金鑰 AWS Encryption SDK

使用 AWS Encryption SDK執行用戶端加密時，資料金鑰快取有助於改善應用程式的效能、降低應用程式請求受到 AWS KMS 調節的風險，並協助您降低成本。 https://docs.aws.amazon.com/kms/latest/developerguide/throttling.html如需如何開始使用的詳細資訊，請參閱如何使用資料金鑰快取。

金鑰快取和 Amazon S3 儲存貯體金鑰的替代方案

如果由於資料處理需求而無法選擇金鑰快取，您也可以使用 AWS 管理主控台 或 Service Quotas API 來請求 AWS KMS 增加配額。考慮您可能進行的 API 呼叫量。您進行的 API 呼叫數量是AWS KMS 定價的重要因素。如果您增加請求率配額以擴展效能，則 產生的請求數量會增加 AWS KMS ，因而產生額外費用。

管理 KMS 金鑰用量的記錄成本

所有 AWS KMS API 呼叫都會記錄到 AWS CloudTrail。應用程式和服務可以產生大量 AWS KMS API 呼叫 （例如用於密碼編譯操作，包括加密和解密）。如果沒有可協助您整理資料、調查趨勢和搜尋異常 API 活動的工具，檢閱 CloudTrail 日誌可能具有挑戰性。Amazon Athena 提供預先定義的資料結構，可協助您快速設定 CloudTrail 日誌的資料表，並開始分析日誌資料。在事件回應期間，它對於臨機操作分析或進一步調查特別有用。如需詳細資訊，請參閱 Athena 文件中的查詢 AWS CloudTrail 日誌。

由於您按 Athena 的每個查詢付費，因此您可以免費事先設定資料表。資料定義語言陳述式不收取任何費用。當您回應事件時，這可協助您確保已符合許多先決條件。為了協助您做好準備，最佳實務是在建立資料表後撰寫查詢、進行測試，並確保它們產生您想要的結果。您可以在 Athena 中儲存查詢以供日後使用。如需如何開始使用 Athena 的詳細資訊，請參閱開始使用 Amazon Athena。

資料事件可讓您查看在資源上執行或在資源內執行的操作。這些也稱為資料平面操作。範例包括 Amazon S3 `PutObject`事件或 Lambda 函數操作 API 呼叫。資料事件通常是大量活動，您記錄它們會產生費用。為了協助控制記錄到 CloudTrail 中線索或事件資料存放區的資料事件量，您可以最佳化您的記錄以降低 CloudTrail 和 Amazon S3 的成本 AWS KMS，方法是設定進階事件選取器來限制要登入 CloudTrail 的資料事件。如需詳細資訊，請參閱如何使用進階事件選取器來最佳化 AWS CloudTrail 成本 (AWS 部落格文章）。

資源

AWS Key Management Service (AWS KMS) 文件

- AWS KMS 開發人員指南
- AWS KMS API 參考
- AWS KMS 參考中的 AWS CLI

工具

- AWS Encryption SDK

AWS 方案指引

策略

- 為靜態資料建立加密策略

指南

- 的加密最佳實務和功能 AWS 服務
- AWS 隱私權參考架構 (AWS PRA)

模式

- 自動加密 Amazon EBS 磁碟區
- 自動修復未加密的 Amazon RDS 資料庫執行個體和叢集
- 監控和修復 的排程刪除 AWS KMS keys

貢獻者

編寫

- 資深 GTM 專家解決方案架構師，Frank Phillis AWS
- Ken Beer， AWS KMS 和 Crypto 程式庫的總監， AWS
- Michael Miller，資深解決方案架構師， AWS
- Jeremy Stieglitz，首席產品經理 AWS
- Zach Miller，首席解決方案架構師， AWS
- Peter M. O'Donnell，首席解決方案架構師， AWS
- Patrick Palmer，首席解決方案架構師 AWS
- Dave Walker，首席解決方案架構師 AWS

檢閱

- Manigandan Shri，資深交付顧問， AWS

技術寫入

- 資深技術作者，Lilly AbouHarb AWS
- 資深技術作者，Kimberly Garmoe AWS

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
初次出版	—	2025 年 3 月 24 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。