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的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 中將這些帳戶管理為單一組織AWS Organizations。有兩種廣泛的方法來 AWS KMS keys 管理多帳戶環境中的 。

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) 中結合金鑰政策和身分型政策。

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 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. 您是否有用於佈建金鑰和資源存取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，並不需要切換 AWS 帳戶 來管理金鑰。不過，請注意，仍必須針對每個帳戶管理 IAM 角色和使用者使用金鑰的許可。

3. 您是否需要向擁有自己的 AWS 帳戶 和資源的客戶或合作夥伴提供使用 KMS 金鑰的存取權？ 對於這些金鑰，集中式方法可以減少客戶和合作夥伴的管理負擔。
4. 您是否有存取集中式或本機存取方法更好地解決之 AWS 資源的授權要求？ 例如，如果不同的應用程式或業務單位負責管理其自身資料的安全性，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費用。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。

如果您希望 AWS 服務 加密您的資料，但不希望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。它只能用於 AWS 服務 您正在操作的 內容，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 金鑰相同帳戶中的 Amazon Elastic Block Store (Amazon EBS) 磁碟區，並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。您不需要為帳戶中存在受 AWS 管金鑰付費，但您需為 AWS 服務 指派給金鑰的 對此金鑰類型的任何使用付費。

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 擁有和管理的 KMS 金鑰集合，可用於多個 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	客戶受管金鑰	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；客戶可檢視	完全受控制，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（每小時按比例分配）；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	客戶無須付費

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。還有其他程式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，請仔細考慮是否依法規或其他要求（例如內部）要求進行選擇，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。在刪除您不再打算使用的 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，您應該套用限制誰可以排程刪除金鑰的政策，並需要多重驗證 (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間七天，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，您可以選擇視需要取消刪除程序。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資料的 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，或如果其匯入的金鑰材料遭到刪除，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。您要將物件上傳至 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，請參閱監控和修復排定的 AWS KMS 金鑰刪除。

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，本節會建議如何使用 AWS Encryption SDK，這是在應用程式中實作用戶端加密的工具。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 ，是使用許可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 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，提供加密傳送至 Amazon S3 之日誌資料的選項。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AWS 帳戶 中央記錄。執行此操作時，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線索，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 儲存或處理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) – 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。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，除非您指定不同的加密選項。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 S3 文件中寫入儲存貯體的所有物件都需要 SSE-KMS。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 操作會導致大量的 `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，預設為啟用伺服器端靜態加密，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。如需此服務加密的詳細資訊，請參閱 DynamoDB 文件中的資料保護。

使用 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 ServiceAmazon 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，只有具有適當許可的 Amazon Redshift 應用程式和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，以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，應考量敏感資料欄位的用戶端加密。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 查詢或索引建立中的聯結。

使用 進行 PCI DSS 資料加密 AWS KMS

中的安全性和品質控制 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，KMS 金鑰無法從中匯出 AWS KMS，這可減少對以不安全方式存放之加密金鑰的疑慮。

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 資料存放在 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，請務必向經驗豐富、合格且經過驗證的對象取得建議。當您設計直接使用 金鑰的應用程式來保護 PCI DSS 範圍內的卡片交易資料時，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 日誌來稽核金鑰使用情況。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將您的 KMS 金鑰與某些 API 操作搭配使用，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

我們不建議 AWS Key Management Service (AWS KMS) 金鑰輪換，除非您需要輪換金鑰以符合法規。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 大幅降低金鑰輪換通常用於緩解的風險類型。如果您必須輪換 KMS 金鑰，建議您使用自動金鑰輪換，並只在不支援自動金鑰輪換時使用手動金鑰輪換。

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 和相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 AWS KMS 會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優勢。如果您在法規或其他需求要求的情況下操作工作負載，金鑰輪換機制的存在可讓您更輕鬆地輪換金鑰。

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。對於加密，請指定您建立的 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至 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中輪換並刪除。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 和相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。您也可以將它用作獨立的 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 工具文件。

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，請參閱以下內容：

- 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有用起點。

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其組態。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。Security Hub 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，以確認已設定靜態加密，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：

- 開始使用 AWS Config
- 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。

匯入的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 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。這些動作與上一節中所述的 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 （這是偵測性控制），並調查和回應 （這是回應性控制） 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
- 具有預設加密的 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 中建立的每個都會 AWS KMS 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。如需最新的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。

具有預設加密的 Amazon S3 儲存貯體金鑰

在某些情況下，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、降低應用程式對 的請求受到 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 Management Console 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。如果您提高請求率配額來擴展效能，則請求的次數會不斷增加，進而 AWS KMS 產生額外的成本。

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的 AWS KMS API 呼叫（例如用於密碼編譯操作，包括加密和解密）。在沒有可協助您組織資料、調查趨勢和搜尋異常 API 活動的工具的情況下，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，因此您可以事先免費設定資料表。資料定義語言陳述式不收取費用。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。

資料事件提供對資源上執行或在資源內執行之操作的可見性。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，您記錄這些事件會產生費用。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

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將內部部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但需要比主動-被動遷移更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。彙總函數的範例包括 SUM和 MAX。

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

永久刪除資料集中個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常用於重複性問題的解決方案，其中解決方案具有反效益、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱《 AWS Identity and Access Management (IAM) 文件》中的 ABAC for AWS。

授權資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線能力。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

評估資料庫遷移工作負載、建議遷移策略並提供工作預估值的工具。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上編製資訊索引的 Web 爬蟲程式。有些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且受單一方控制之機器人的網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，並透過核准的程序，讓使用者快速存取 AWS 帳戶 他們通常沒有存取許可的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本，並完全取代目前的版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，讓您的 AWS 工作負載承受壓力並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的 CCoE 文章。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到邊緣運算技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱建置您的雲端操作模型。

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)
- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

部落格文章中的 Stephen Orban 定義了這些階段： AWS 雲端 企業策略部落格上的邁向雲端優先之旅和採用階段。如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載變得不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

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 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的原始伺服器和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理其資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶和管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別對軟體開發生命週期中的速度和品質造成負面影響的限制並排定優先順序。DVSM 擴展了最初專為精簡製造實務設計的價值串流映射程序。它著重於在軟體開發過程中建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置中實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載的災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

將人類可讀取的純文字資料轉換為加密文字的運算程序。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱 服務端點。

端點服務

您可以在虛擬私有雲端 (VPC) 中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程 （例如會計、MES 和專案管理）。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的信封加密。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全概念包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。透過計算摘要統計並建立資料可視化來執行 EDA。

F

事實資料表

星狀結構描述中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例給 LLM。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示非常有效。另請參閱零鏡頭提示。

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程會被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為棕地。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是透過使用 AWS Config AWS Security Hub、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如，Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分，而轉換結構描述可能是一項複雜任務。AWS 提供有助於結構描述轉換的 AWS SCT。

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，以及處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

請參閱基礎設施即程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC，可管理 VPCs 之間 （在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會被明確指派安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 Rs。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

屬於組織一部分的管理帳戶 AWS 帳戶 以外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱實作微服務 AWS。

Migration Acceleration Program (MAP)

此 AWS 計畫提供諮詢支援、訓練和服務，以協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變基礎設施做為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題和相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造中，整合 OT 和資訊技術 (IT) 系統是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

由 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援所有 S3 儲存貯體、使用 AWS KMS (SSE-KMS) 的伺服器端加密 AWS 區域，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (PII)

當直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（請參閱身分型政策）、指定存取條件（請參閱資源型政策），或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱服務控制政策）。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則

可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱在微服務中啟用資料持久性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE` 子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

設計隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

產品整個生命週期的資料和程序管理，從設計、開發和啟動，到成長和成熟，再到拒絕和移除。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出作為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強生成。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

Region

地理區域中的 AWS 資源集合。每個 AWS 區域 都會獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 Rs。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有參與遷移活動和雲端操作之各方的角色和責任。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、已諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能可啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而無需為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它包含秘密值及其中繼資料。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的什麼內容？。

設計安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

由接收資料的 AWS 服務 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

的進入點 URL AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

服務水準協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作

為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱 環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等速度的查詢。

視窗函數

SQL 函數，對與目前記錄在某種程度上相關的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，多次讀取。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

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。