



為靜態資料建立企業加密策略

AWS 規範指引



AWS 規範指引: 為靜態資料建立企業加密策略

Copyright © 2024 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
目標業務成果	1
限制	2
關於資料加密	3
關於加密金鑰	3
關於加密演算法	3
關於封加密	3
加密策略階段	5
政策	5
標準	6
成本與效能	7
金鑰存取控制	7
加密類型	7
加密金鑰規格	7
金鑰儲存位置	8
架構	8
資料分類	8
環境分類	9
變更事件和程序	9
實作	10
成本，便利性和控制	11
效能和加密類型	11
金鑰儲存位置	12
存取控制	12
稽核與記錄	13
常見問答集	14
我什麼時候需要對稱加密？	14
何時需要非對稱加密？	14
我什麼時候需要信封加密？	14
什麼時候需要使用 HSM？	14
為什麼要集中管理加密金鑰？	15
我是否需要使用專門建置的加密基礎架構？	15
如何AWS KMS幫助？	15

資源	16
AWS 服務 文件	16
AWS行銷	16
AWS驗證與 Well-Architected	16
哈希和令牌化	16
影片	17
文件歷史紀錄	18
詞彙表	19
#	19
A	19
B	22
C	23
D	26
E	29
F	31
G	32
H	33
I	34
L	36
M	37
O	41
P	43
Q	45
R	46
S	48
T	51
U	52
V	53
W	53
Z	54
.....	iv

為靜態資料建立企業加密策略

文基斯里瓦扎夫，安德烈·迪法比奧和維克拉馬迪亞·巴哈特納加爾，亞馬 Amazon Web Services (AWS)

2022 年九月 ([文件歷史記錄](#))

許多企業都擔心數據洩露的網絡安全威脅。發生數據洩露時，未經授權的人可以訪問您的網絡並竊取企業數據。防火牆和反惡意程式碼服務可協助防範此威脅。您可以實作的另一個保護是資料加密。在本指南的「關於資料加密」一節中，您可以進一步瞭解資料加密的運作方式以及可用的類型。

一般來說，當您討論加密時，有兩種類型的數據。傳輸中的資料是指在網路中主動移動的資料，例如在網路資源之間移動。靜態資料是指靜止且處於休眠狀態的資料，例如儲存中的資料。此策略著重靜態資料。如需加密傳輸中資料的詳細資訊，請參閱[保護傳輸中的資料](#) (AWS Well-Architected 的架構)。

加密策略由您按順序開發的四個部分組成。加密政策由高級管理層決定，概述了加密的法規，合規性和業務要求。加密標準可幫助實施政策的人了解並遵守它。標準可以是技術或程序性的。該框架是支持標準實施的標準操作程序，結構和護欄。最後，架構是加密標準的技術實作，例如您使用的環境、服務和工具。本文件的目的是協助您建立符合您業務、安全性和合規性需求的加密策略。其中包含有關如何檢閱和實作靜態資料安全標準的建議，以便您能夠以整體方式滿足合規性和業務需求。

此策略使用 AWS Key Management Service (AWS KMS) 來協助您建立和管理有助於保護資料的加密金鑰。AWS KMS 與許多 AWS 服務集成以加密所有靜態數據。即使您選擇不同的加密服務，您仍然可以採用本指南中的建議和階段。

目標對象

該策略旨在針對以下受眾：

- 為企業制定政策的執行官，例如 CEO、技術長 (CTO)、資訊長 (CIO) 和資訊安全長 (CIO)，以及資訊安全長 (CISO)
- 負責制定技術標準的技術人員，例如技術副總裁和董事
- 負責監察遵守合規政策 (包括法定和自願遵循制度) 的合規和治理人員

目標業務成果

- Data-at-rest 加密策略 — 決策者和政策制定者可以創建加密策略並了解影響策略的關鍵因素。

- Data-at-rest 加密標準 — 技術領導者可以根據加密策略開發加密標準。
- 加密框架 — 技術領導者和實施者可以創建一個框架，作為決定策略者和創建標準的人之間的橋樑。架構，在此內容中，意味著識別適當的流程和工作流程，可協助您在原則的範圍內實作標準。架構類似於用於變更政策或標準的標準作業程序或變更管理程序。
- 技術架構和實作 — 實作實作者 (例如開發人員和架構師) 都知道可用的架構參考，協助他們實作加密策略。

限制

本文件旨在協助您制定最適合企業需求的自訂加密策略。它本身不是加密策略，也不是合規性檢查清單。下列主題不包含在本文件中：

- 傳輸中加密
- 字符化
- 雜湊
- 合規性與資料控管
- 為您的加密程序編列預算

如需上述個別主題的詳細資訊，請參閱以下[資源](#)部份。

關於資料加密

本節包含加密概念和術語的高階概觀。如需詳細資訊，請參閱[密碼編譯概念](#) (AWS密碼編譯服務和工具指南)。資料加密協助您強制執行資料機密性。透過實作加密和存取控制，您可以協助保護企業中的資料。

關於加密金鑰

加密服務會使用加密金鑰來加密資料。加密金鑰是由加密演算法所產生的隨機位元組成的加密字串。按鍵的長度可能有所不同，每個按鍵的設計都是不可預測且獨一無二的。加密的強度通常取決於兩個因素：密鑰的長度和使用的算法。通常，較長的金鑰可提供更強的加密。

關於加密演算法

有兩種類型的算法用於生成加密密鑰，對稱和非對稱。

對稱加密用於加密資料的金鑰。這種類型的加密通常速度較快，因此對於大量資料而言更有效率。這種類型的加密被廣泛使用，普遍接受是安全的。由於單一密鑰同時用於加密和解密，因此最佳做法是經常變更密鑰，以防止未經授權的人取得密鑰。如需建議何時建議使用對稱加密的詳細資訊，請參閱「常見問題集」一節[我什麼時候需要對稱加密？](#)中的。

非對稱加密使用一對密鑰、一個公開密鑰進行加密，以及用於解密的私密密鑰。您可以共享公鑰，因為它不用於解密，但對私鑰的訪問應該受到高度限制。非對稱加密通常被認為比對稱加密更安全，但速度較慢，因為它使用的密鑰長度較長且需要更複雜的加密計算。如需建議何時建議使用非對稱加密的詳細資訊，請參閱[何時需要非對稱加密？](#)常見問題集一節。

關於封加密

當您加密資料時，只要您的加密金鑰保持機密，資料才會受到保護。用於加密資料金鑰的密鑰被稱為資料金鑰。信封加密是使用另一個加密金鑰 (稱為金鑰加密密鑰) 加密資料金鑰的做法。您甚至可以使用另一個加密金鑰來加密該密鑰，依此類推。最終，一個密鑰必須保留為純文本，以便您可以解密密鑰和數據。這個最上層的純文字密鑰加密密鑰稱為根密鑰。

封套加密提供多種優勢：

- 方便 — 由於您的數據密鑰已加密，因此您可以將其與加密數據一起存儲。

- 效率 — 加密作業可能非常耗時，尤其是當資料量龐大時。這時您可以捨棄使用不同金鑰來多次重新加密原始資料的做法，改成只重新加密負責保護原始資料的資料金鑰。這可讓您在重新加密資料的情況下提供兩層以上的加密保護。
- 效能 — 您可以結合加密演算法。例如，您可以對原始資料使用對稱加密，但是對資料金鑰使用非對稱加密，結合了兩種加密演算法的優點。

如需信封加密的詳細資訊，請參閱[信封加密](#) (AWS Key Management Service文件)。如需決定是否需要信封加密的詳細資訊，請參閱「常見問題集」一節[我什麼時候需要信封加密？](#)中的。

建立加密策略的階段

建立企業級加密策略需要多階段的方法。每個階段都會定義一組控制項，以協助您達成所需的實際結果。本文件會引導您完成這些階段，並詢問您特定問題，以協助您自訂加密策略。

建置靜態資料的加密策略包含下列順序階段：

1. [加密政策](#)— 建立定義企業加 data-at-rest 密目標的原則。
2. [加密標準](#)— 定義技術和程序標準，以幫助您實現企業政策。
3. [加密框架構](#)— 構建框架，以幫助所有利益相關者了解，更改和實施您的加密標準。
4. [實作](#)— 部署您的加密基礎架構。

加密政策

加密原則的目的是在高級管理層級上建立組織所需要符合的業務和合規性期望。此原則可作為定義合適加密策略的起點。這項政策應具有足夠的抽象性，以便為實施提供自由和靈活性。同時，它必須具有足夠的特定性，才能定義符合組織目標的可接受實作範圍。一般而言，原則與技術無關，而且很少變更，因為它們定義了企業加密策略的基本特性。

一般而言，加密原則包含 (但不限於) 下列項目：

- 您的企業必須符合的任何法規或合規制度
- 對資料加密的任何業務承諾或期望
- 必須加密的資料類型
- 何時使用加密以外的資料保護技術的準則，例如雜湊或標記化

組織的最高管理層級，例如 CIO、CTO 和 CISO，通常會定義並核准加密原則。

建立加密政策時，應考量下列事項：

- 您的業務範圍決定了您需要遵守的合規性和監管制度。這些制度決定了資料加密需求。將業務擴展到新區域或擴展產品方案的執行層級決策可能會影響您的資料適用的法規。例如，如果銀行決定向客戶提供信用卡，則他們可能需要遵守 [支付卡行業數據安全標準 \(PCI-DSS\)](#)，該標準需要數據加密。
- 您的政策應指定需要加密的資料類型。這會根據您企業的合規要求和資料處理目標而有所不同。例如，您的政策可能會聲明企業捕獲或擁有的任何數據必須在靜態時加密。

- 您的加密政策必須符合您的內部資料分類標準。要制定有效的加密政策，需要確定元數據級別的數據類別。例如，您的類別可能包括公開、內部、機密、機密或客戶資料。
- 包含如何判斷哪些資料應該加密，以及應使用其他技術 (例如 Token 化或雜湊) 來保護哪些資料的準則。例如，您的政策可能會聲明任何進入稽核、追蹤或應用程式記錄的個人識別資訊 (PII) 都必須標記化。

加密標準

標準是從您的政策衍生出來的。這些範圍較窄，有助於定義實施的框架和架構。例如，如果貴組織的政策是在靜態時加密資料，則標準會定義所需的加密類型，並提供有關如何遵守原則的一般方向。

加密標準通常指定以下內容：

- 應使用的加密類型
- 加密金鑰的最低規格
- 誰可以存取加密金鑰
- 應儲存加密金鑰的位置
- 選擇加密或雜湊技術時，挑選適當金鑰強度的準則
- 金鑰輪換頻率

雖然您很少需要更新加密原則，但加密標準可能會有所變更。網路安全產業不斷發展，以滿足不斷變化的威脅格局。因此，您的標準應該變更為採用最新技術和最佳實務，以便為您的企業資料提供最佳保護。

在企業組織中，副總裁、董事或資料管理員通常會定義加密標準，而合規主管通常會審核和核准這些標準。

在組織中定義和維護加密標準時，請考慮下列幾類因素：

- [成本與效能考量](#)
- [金鑰存取控制](#)
- [加密類型](#)
- [加密金鑰規格](#)
- [金鑰儲存位置](#)

成本與效能考量

決定靜態資料的加密標準時，請考量下列作業因素：

- 可用的硬體資源必須能夠大規模支援您的標準。
- 加密的成本會根據金鑰的長度、資料量以及執行加密所需的時間而有所不同。例如，與對稱式加密相比，非對稱加密會使用較長的金鑰，而且需要更多時間。
- 考慮企業應用程式的效能需求。如果您的應用程式需要低延遲和高輸送量，則您可能需要使用對稱加密。

金鑰存取控制

根據「最低權限原則」識別加密金鑰政策管理政策。最小權限是授與使用者執行其工作職能所需的最低存取權限的安全性最佳作法。在您的標準中，定義存取控制原則：

- 識別管理金鑰加密金鑰和資料金鑰的角色。
- 定義金鑰權限並將其對應至角色。例如，它會定義誰擁有金鑰管理員權限，以及誰擁有金鑰使用者權限。金鑰管理員可以建立或修改金鑰加密金鑰，金鑰使用者可以加密和解密資料以及產生資料金鑰。

加密類型

在您的標準中，定義哪些加密類型和功能適合您的組織：

- 記錄使用對稱和非對稱加密演算法的使用時機記錄。如需詳細資訊，請參閱 < 常見問題集 > 一節[何時需要非對稱加密？](#)中的[我什麼時候需要對稱加密？](#)和。
- 決定是否應使用信封加密，並定義情況。如需詳細資訊，請參閱[我什麼時候需要信封加密？](#)常見問題集一節。
- 定義何時使用加密替代方案的準則，例如權杖化和雜湊。

加密金鑰規格

定義加密金鑰的必要規格，例如金鑰強度和演算法。這些規格必須符合政策中定義的法規和合規制度。請考慮定義下列規格：

- 定義對稱和非對稱加密類型的最低金鑰強度和演算法。關鍵強度的因素包括長度，隨機性和唯一性。

- 定義何時要實作新版本的加密演算法。例如，您的標準可能會在發行後 30 天內說明實作最新版本的演算法，或者永遠使用比最新版本舊的一個版本。
- 定義輪換加密金鑰的間隔。

金鑰儲存位置

在您的標準中，決定儲存加密金鑰的位置時，請考慮下列事項：

- 合規性和法規要求可能會決定加密金鑰的儲存位置。
- 決定您要將金鑰儲存在集中位置，還是儲存金鑰對應的資料。如需詳細資訊，請參閱[為什麼要集中管理加密金鑰？](#)常見問題集一節。
- 如果您選擇集中式儲存，請決定要將金鑰儲存在企業管理的基礎結構中，例如硬體安全性模組 (HSM) 或受管服務提供者 (例如)AWS Key Management Service。如需詳細資訊，請參閱[何時需要使用硬體安全模組 \(HSM\)？](#)常見問題集一節。

加密框架結構

在此內容中，架構是指修改加密標準或原則時需要遵循的一組標準作業程序。該框架是幫助您實現標準的腳手架。它有助於將單詞轉換為動作。該框架將定義標準的人與實施標準的人聯繫起來。

框架通常包括以下主題：

- [資料分類](#)
- [環境分類](#)
- [變更事件和程序](#)

資料分類

資料分類在建立加密策略中扮演著至關重要的角色。數據分類是根據數據的敏感性將數據分配給類別的過程。以下是常見的資料分類類別，以提高敏感度的順序：公開、私人、內部、機密和受限制。

您的加密架構應包含下列有關資料分類的資訊：

- 您企業的資料分類類別。
- 用於將資料分類為適當類別的分類標準。例如，公司的貿易配方可以歸類為受限制，員工 PII 可能是機密的，員工之間通過官方渠道進行內部溝通可能是內部的。

- 用於在品類之間升級和降級資料的程序。
- 每個資料分類類別的存取準則。
- 每個類別所需的加密金鑰種類。

環境分類

您的企業可能會有多个環境，例如開發、測試、生產與生產。每個環境都可以包含不同類型的資料，並具有不同的加密需求。

您的加密架構應該包含以下有關環境的資訊：

- 定義您的企業環境。
- 定義每個環境的加密要求。例如，您可以針對開發環境中的所有資料類別使用單一加密金鑰，而在生產環境中，您可能會針對每個商務應用程式或資料分類類別使用不同的加密金鑰。

變更事件和程序

加密標準會經常變更，因此您可以隨時掌握最新技術、最佳實務和創新。以下是常見的變更事件，可能會啟動您的加密標準修訂：

- 加密金鑰最小長度的變更
- 加密演算法強度的變化
- 變更可存取加密金鑰的使用者或如何存取
- 更改按鍵的旋轉間隔
- 刪除金鑰程序的變更
- 金鑰儲存位置或原則的變更
- 備份和還原金鑰程序變更

您的加密架構應包含下列項目，以協助您的組織準備好管理、實作和傳達加密標準或原則的變更：

- 變更控制流程 — 此流\ 'b5\ '7b 的目的是為即將到來的變更進行計劃和準備。當您需要變更加密標準或原則時，這個可重複且可擴充的程序旨在定義：
 - 貴組織如何評估變更的影響
 - 誰可以啟動變更
 - 誰負責實施變更

- 誰負責核准變更
- 如有必要，您的組織將如何回滾更改
- 變更稽核性和可追蹤性流程 — 此程序定義組織如何在中繼資料層級和資料層級稽核和追蹤變更。它應該定義您如何保留和訪問以下記錄：
 - 什麼改變了
 - 當它被改變
 - 啟動、核准和實行變更的人員

例如，如果您的組織變更了最低加密金鑰強度，您應該能夠判斷原始和新需求、變更的生效時間，以及變更流程涉及的人員。

- 變更推出流程 — 此程序的目的是定義組織在決定進行變更之後如何實作變更。這個過程定義：
 - 誰是利益相關者
 - 您是否應該完成飛行員或概念驗證
 - 您應該如何以及何時溝通變更的狀態
 - 如何回滾更改，如果必要的話。
 - 實施更改後的觀察期應該是多少。
 - 觀察過程將是什麼來監控變化的影響，包括如何收集有關變化的反饋並評估有效性
- 處分處理 — 此處理的目的是定義貴組織如何處理與加密相關的資源與資訊的處分。它包括實際退休的指示以及退休的溝通流程。

實作

在此策略中，架構是指加密標準的技術實作。本節包含有關如何AWS 服務根據您的政策和標準來協助您實作 data-at-rest 加密策略的資訊 [AWS CloudHSM](#)，例如 [AWS Key Management Service\(AWS KMS\)](#) 和。

AWS KMS是一種受管服務，可協助您建立和控制用來保護資料的加密金鑰，並控制用來保護資料的加密金鑰。KMS 金鑰絕對不會在未加密狀態下離開服務 若要使用或管理 KMS 金鑰，您必須與其互動 AWS KMS，而且許多金鑰AWS 服務都與之整合AWS KMS。

AWS CloudHSM是一種密碼編譯服務，用於在您的AWS環境中建立和維護硬體安全模組 (HSM)。HSM 是處理密碼編譯作業並為加密金鑰提供安全儲存的運算裝置。如果您的標準要求您使用 FIPS 140-2 第 3 級驗證的硬體，或者您的標準要求使用業界標準 API，例如 PKCS #11、Java 加密延伸功能 (JCE) 和微軟加密通訊 (CNG)，則您可以考慮使用AWS CloudHSM。

您可以配置AWS CloudHSM為的自訂金鑰存放區AWS KMS。此解決方案結合的便利性AWS KMS與服務整合，以及AWS CloudHSM在您的AWS 帳戶。如需詳細資訊，請參閱[自訂金鑰存放區](#) (AWS KMS文件)。

本文件討論高階的AWS KMS功能，並說明如AWS KMS何處理您的政策和標準。

成本，便利性和控制

AWS KMS提供不同類型的按鍵。有些由客戶擁有或管理AWS，另一些則由客戶創建和管理。您可以根據主要考量和成本考量的控制層級，在這些選項之間進行選擇：

- **AWS擁有的金鑰** — AWS 擁有和管理這些金鑰，且可用於多個金鑰AWS 帳戶。一些AWS 服務支持AWS擁有的密鑰。您可以免費使用這些鑰匙。此金鑰類型可減輕您管理金鑰生命週期及其存取的成本和管理額外負荷。如需有關此類型金鑰的詳細資訊，請參閱[AWS擁有的金鑰](#) (AWS KMS說明文件)。
- **AWSManaged Key** — 如果與整合AWS KMS，它可以代表您建立、管理和使用這種類型的金鑰，以保護您在該服務中的資源。AWS 服務這些密鑰在您的中創建AWS 帳戶，並且只AWS 服務能使用它們。AWS受管金鑰沒有月費用。它們可能需要支付超過免費方案的使用費，但有些費用會為您支AWS 服務付這些費用。您可以使用身分識別原則來控制這些金鑰的檢視和稽核存取，但AWS管理金鑰生命週期。如需有關此類型金鑰的詳細資訊，請參閱[AWS受管理金鑰](#) (AWS KMS說明文件)。如需與之整合的AWS 服務完整清單AWS KMS，請參閱[AWS 服務整合](#) (AWS行銷)。
- **客戶管理金鑰** — 您可以建立、擁有和管理這類金鑰，而且您可以完全控制金鑰生命週期。對於職責劃分，您可以使用身分型政策和資源型政策控制對金鑰的存取。您也可以設定自動[金鑰輪換](#)。客戶受管金鑰會衍生每月費用，如果超出免費方案部分的使用費用費用。如需此類型金鑰的詳細資訊，請參閱[客戶管理金鑰](#) (AWS KMS說明文件)。

如需金鑰儲存和使用方式的詳細資訊，請參閱[AWS Key Management Service定價](#) (AWS行銷)。

效能和加密類型

根據標準中選擇的加密類型，您可以使用兩種類型的 KMS 金鑰。

- **對稱** — 所有類AWS KMS key型都支援對稱加密。加密客戶受管金鑰時，您可以使用單一強度金鑰，透過 AES-256-GCM 進行加密和解密。
- **非對稱** — 客戶代管金鑰支援非對稱式加密。您可以根據您的預期用途在不同的關鍵優勢和算法之間進行選擇。非對稱金鑰可以使用 RSA 加密和解密，並且可以使用 RSA 或 ECC 簽署和驗證操作。非對稱金鑰演算法本質上就是提供角色分離，並簡化金鑰管理。搭配使用非對稱加密時AWS KMS，不支援某些作業，例如旋轉金鑰和匯入外部金鑰材料。

如需有關對稱和非對稱金鑰支援之AWS KMS作業的詳細資訊，請參閱[金鑰類型參考](#) (AWS KMS說明文件)。

封套加密

信封加密內建於中AWS KMS。在中AWS KMS，您可以使用純文字或加密格式產生資料金鑰。加密資料金鑰會透過 KMS 金鑰進行加密金鑰。您可以將 KMS 金鑰存放區中的自訂金鑰存放區中存放 KMS 金鑰存AWS CloudHSM放區。如需信封加密優點的詳細資訊，請參閱[關於封加密](#)。

金鑰儲存位置

您可以使用政策管理對AWS KMS資源的存取。政策描述誰可以存取哪些資源。附加至AWS Identity and Access Management (IAM) 主體的政策稱為身分型政策或 IAM 政策。附加至其他類型資源的策略稱為資源策略。AWS KMS的資源策略稱AWS KMS keys為關鍵策略。每個 KMS 金鑰政策政策。

金鑰原則提供彈性，可將加密金鑰儲存在中央位置，或以分散式方式將其儲存在靠近資料的位置。當您決定將 KMS 金鑰存放在哪裡時，請考量下列AWS KMS功能AWS 帳戶：

- 單一區域基礎結構支援 — 根據預設，KMS 金鑰是區域特定的，而且永遠不會保留AWS KMS未加密的狀態。如果您的標準對於控制特定地理位置中的金鑰有嚴格的要求，請探索使用單一區域金鑰。
- 多區域基礎架構支援 — AWS KMS 也支援稱為「多區域金鑰」的特殊用途金鑰類型。將數據存儲在多個中AWS 區域是災難恢復的常見配置。透過使用多區域金鑰，您可以在不重新加密區域之間傳輸資料，而且您可以像在每個區域擁有相同的金鑰一樣管理資料。如果您的標準要求您的加密基礎結構在主動-主動配置中跨越多個區域，則此功能非常有用。如需詳細資訊，請參閱[多區域金鑰](#) (AWS KMS文件集)。
- 集中式管理 — 如果您的標準要求您將金鑰儲存在集中位置，您可以使用AWS KMS將所有加密金鑰儲存在一個單一位置AWS 帳戶。您可以使用金鑰原則來授與其他應用程式的存取權，這些應用程式可能位於相同區域的不同帳戶中。集中式金鑰管理可減少管理金鑰生命週期和金鑰存取控制的管理額外負荷。
- 外部金鑰材料 — 您可以將外部產生的金鑰材料匯入到中AWS KMS。單一和多區域對稱金鑰可 Support 此功能。由於對稱金鑰的材料是由外部產生的，因此您必須負責保護產生的金鑰材料。若要取得更多資訊，請參閱[匯入的金鑰材料](#) (AWS KMS文件)。

存取控制

在中AWS KMS，您可以使用下列政策機制來實作精細層級的存取控制：[金鑰政策](#)、[IAM 政策](#)和[授權](#)。使用這些控制項，您可以根據角色 (例如管理員、可以加密資料的金鑰使用者、可以解密資料的金鑰使

用者)，以及可以加密和解密資料的金鑰使用者來設定職責分離。如需詳細資訊，請參閱[驗證和存取控制](#) (AWS KMS文件集)。

稽核與記錄

AWS KMS與亞馬遜集AWS CloudTrail成以 EventBridge 進行日誌記錄和監控目的。所有AWS KMS API 操作都記錄在 CloudTrail 日誌中並可審核。您可以使用 Amazon CloudWatch EventBridge、和設AWS Lambda定自訂監控解決方案，以設定通知和自動修復。如需詳細資訊，請參閱[記錄和監控](#) (AWS KMS文件)。

常見問答集

本節提供定義加密標準或在實作階段建立加密基礎結構時常見問題的解答。

我什麼時候需要對稱加密？

在以下情況下，您可以使用對稱加密：

- 速度，成本和較低的計算開銷是優先事項。
- 您需要加密大量資料。
- 加密的資料不會離開組織網路的界限。

何時需要非對稱加密？

您可以在以下情況使用非對稱加密

- 您需要在組織外部共享數據。
- 法規或治理禁止共享密鑰。
- 不可否認性是必要的。（不可否認性可防止用戶拒絕先前的承諾或行為。）
- 您需要根據組織角色嚴格隔離對加密金鑰的存取權限。

我什麼時候需要信封加密？

如果您的加密原則需要金鑰輪替，則需要支援並實作信封加密。某些治理和合規制度需要金鑰輪替，否則您的政策可能會要求其滿足業務需求。

何時需要使用硬體安全模組 (HSM)？

如果您的原則指定符合下列條件，則可能需要 HSM：

- 聯邦資訊處理標準 (FIPS) 140-2 3 級加密標準。如需詳細資訊，請參閱 [FIPS 驗證](#) (AWS CloudHSM 文件)。
- 業界標準 API，例如 PKCS #11、Java 密碼編譯延伸 (JCE) 或微軟密碼編譯 API：下一代 (CNG)

為什麼要集中管理加密金鑰？

以下是集中式金鑰管理的常見優點：

- 由於金鑰會在不同的位置使用和管理，因此您可以重複使用金鑰，進而降低成本。
- 您可以更好地控制加密金鑰的存取權。
- 將金鑰儲存在單一位置可讓您在標準變更時更輕鬆地檢視、檢核和更新金鑰。

我是否需要針對靜態資料使用專用的加密基礎架構？

如果符合以下任一情況，則您的企業需要加密基礎結構：

- 您的企業會處理並儲存公開以外的任何分類資料。
- 您的企業會擷取並儲存有關員工或客戶的資料。
- 您的企業會處理 PII 資料。
- 您的企業必須符合需要加密資料的法規或治理制度。
- 您的企業高階主管已強制加密所有靜態資料。

如何AWS KMS協助我的組織達成靜態資料的加密目標？

除了許多其他功能外，還AWS Key Management Service可以幫助您：

- 使用加密。
- 控制加密金鑰存取，例如將金鑰管理與金鑰使用分開。
- 在多個AWS 區域和之間共用金鑰AWS 帳戶。
- 集中化金鑰管理。
- 自動化並授權金鑰輪換。

資源

AWS 服務 文件

- [AWS KMS加密詳細資料](#)
- [AWS KMS 開發人員指南](#)
 - [AWS KMS 概念](#)
 - [特殊用途按鍵](#)
 - [的身分驗證與存取控制AWS KMS](#)
 - [的安全性AWS KMS](#)
 - [如何AWS 服務使用AWS KMS](#)
- 《[AWS CloudHSM 使用者指南](#)》
- [AWS加密服務和工具指南](#)
 - [如何選擇加密工具或服務](#)
 - [密碼學概念](#)

AWS行銷

- [AWS KMS 定價](#)
- [AWS KMS與其他整合AWS 服務](#)

AWS驗證與 Well-Architected

- [保護傳輸中的資料](#)
- [保護靜態資料](#)

哈希和令牌化

- [如何使用令牌化來提高數據安全性並減少審計範圍](#) (AWS博客文章)
- [建議使用核准雜湊演算法的應用程式](#) (NIST 出版物)

影片

- [加密的運作方式AWS](#)
- [保護您的區塊儲存AWS](#)
- [實現安全目標AWS CloudHSM](#)
- [實作的最佳實務AWS Key Management Service](#)
- [深入探討AWS加密服務](#)

文件歷史紀錄

下表說明本指南的重大變更。如果您想收到有關 future 更新的通知，您可以訂閱 [RSS 摘要](#)。

變更	描述	日期
初始出版	—	2022 年 9 月 15 日

AWS 規範指引詞彙表

以下是 AWS Prescriptive Guidance 所提供策略、指南和模式的常用術語。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：將您的內部部署 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：將您的內部部署 Oracle 資料庫遷移至 中的 Oracle 的 Amazon Relational Database Service (Amazon RDS) 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：將內部部署 Oracle 資料庫遷移至 中的 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至相同平台的雲端服務。範例：遷移 Microsoft Hyper-V 應用程式 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、一致性、隔離、持久性](#)。

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，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。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。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、無效或效果不如替代方案。

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侵害。

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。如需如何在遷移策略中使用 AWS 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、一致性、隔離、持久性 (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 ([ABAC](#)) 文件中的 [Word for AWS](#)。IAM

權威性資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將資料從權威資料來源複製到其他位置，以處理或修改資料，例如匿名化、修訂或擬匿名化資料。

可用區域

與其他可用區域中的故障 AWS 區域 隔離的不同位置，並對相同區域中的其他可用區域提供便宜的低延遲網路連線。

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 將指導方針整理成六個重點領域：業務、人員、治理、平台、安全和操作。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。為此，AWS CAF 提供人員開發、訓練和通訊的指引，協助組織準備好成功採用雲端。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估算的工具。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。您可以搭配 Amazon Detective 使用行為圖表來檢查失敗的登入嘗試、可疑的 API 呼叫和類似的動作。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[端點](#)。

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。此策略可協助您在影響最小的情況下快速復原。

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。有些機器人很有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。某些其他稱為不良機器人的機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到[惡意軟體](#)感染且由單一方控制的[機器人](#)網路，稱為機器人繼承者或機器人運算子。Botnet 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，以及透過核准的程序，使用者取得其通常無權存取 AWS 帳戶之存取權的快速方法。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS [實作碎片程序](#) 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。您可以使用 CDC 進行各種用途，例如稽核或複寫目標系統中的變更以維持同步。

混亂工程

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 \(AWS FIS\)](#) 來執行實驗，以強調 AWS 工作負載並評估其回應。

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。

Cloud Center of Excellence (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、建立操作模型）
- 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

這些階段由 Stephen Orban 在部落格文章 [The Journey Toward Cloud-First](#) 和企業策略部落格上的 [採用階段](#) 中定義。AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱 [遷移準備指南](#)。

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。每個版本的程式碼都稱為分支。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

很少存取且通常為歷史資料的資料。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價格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映像和影片等視覺化格式分析和擷取資訊的 [AI](#) 欄位。例如，AWS Panorama 提供將 CV 新增至內部部署攝影機網路的裝置，而 Amazon SageMaker 則提供 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。您通常會在遷移的產品組合探索和分析階段使用來自 CMDB 的資料。

一致性套件

您可以組合的 AWS Config 規則和修復動作集合，以自訂合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶和區域中或跨組織的單一實體。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)

自動化軟體發程序的來源、建置、測試、暫存和生產階段的程序。CI/CD is commonly described as a pipeline. CI/CD 可協助您自動化程序、提高生產力、改善程式碼品質，以及更快交付。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化。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

架構架構架構，提供分散式、分散式的資料擁有權，並具有集中式的管理和治理。

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，可協助確保只有受信任的身分才能從預期的網路存取受信任的資源。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 and 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。

資料庫操作語言 (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。

defense-in-depth

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 AWS 上採用此策略時，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，a defense-in-depth 方法可能會結合多重重要素驗證、網路分割和加密。

委派的管理員

在 AWS Organizations 中，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶並管理該服務的許可。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)

用於識別和排定限制的流程，這些限制會對軟體開發生命週期中的速度和品質產生不利影響。DVSM 延伸了最初為精實生產實務設計的價值串流映射程序。它著重於透過軟體開發程序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、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 [星狀結構描述](#) 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為文字欄位或像文字那樣行為的離散數字。這些屬性通常用於查詢限制、篩選和結果集標籤。

災難

阻止工作負載或系統在其主要部署位置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，例如意外錯誤組態或惡意軟體攻擊。

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 [上的工作負載災難復原 AWS：雲端中的復原](#)。

DML

請參閱[資料庫操作語言](#)。

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。如需有關如何搭配 strangler fig 模式使用網域驅動設計的資訊，請參閱[使用容器和 Amazon ASMX Gateway 逐步現代化舊版 Microsoft ASP.NET \(API\) Web 服務](#)。

DR

請參閱[災難復原](#)。

漂移偵測

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[偵測可能會影響對治理要求合規性的登陸區域中的變更](#)。 <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縮短回應時間。

電子資料交換 (EDI)

組織之間的商業文件自動交換。如需詳細資訊，請參閱[什麼是電子資料交換](#)。

加密

將純文字資料轉換為人類可讀取的運算程序。

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) 主體。這些帳戶或主體可以透過建立介面 VPC 端點，私下連線至您的端點服務。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)

可自動化和**管理企業關鍵業務流程**（例如會計、[MES](#) 和專案管理）的系統。

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 安全特徵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。EDA 是透過計算摘要統計資料和建立資料視覺化來執行。

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：包含量值的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

使用頻繁且增量測試來縮短開發生命週期的哲學。這是敏捷方法的關鍵部分。

故障隔離界限

在中 AWS 雲端，邊界，例如可用區域 AWS 區域、控制平面或資料平面，這些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。這通常表示為數值分數，可透過各種技術計算，例如 Shapley 累加解釋 (SHAP) 和整合漸層。如需詳細資訊，請參閱[使用的機器學習模型可解釋性：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。

幾下提示

在請求 [LLM](#) 執行類似任務之前，提供少量示範任務和所需輸出的範例。此技術是內文學習的應用，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式設定、推理或網域知識的任務，少量擷取提示非常有效。另請參閱[零擷取提示](#)。

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，以及以自然語言進行交談。如需詳細資訊，請參閱[什麼是基礎模型](#)。

G

生成式 AI

經過大量資料訓練的 [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)

在 Amazon CloudFront 中，此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 [Word 文件中的限制內容的地理分佈](#)。CloudFront

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 工作流程被視為舊版，而以[中繼線為基礎的工作流程](#)是現代的首選方法。

金色影像

系統或軟體的快照，用作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

高階規則，可協助管理跨組織單位 (OUs) 的資源、政策和合規性。預防性防護機制會強制執行政策，以確保符合合規標準。其實作方式是使用服務控制政策和 IAM 許可界限。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、AWS Trusted Advisor、Amazon Inspector 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)

工作負載在遇到挑戰或災難時持續運作的能力，無需介入。HA 系統設計為自動容錯移轉、持續提供高品質效能，以及處理不同的負載和故障，且對效能的影響最小。

歷史現代化

一種用於現代化和升級操作技術 (OT) 系統的方法，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠的不同來源收集和存放資料。

保留資料

從用來訓練機器學習模型的資料集中保留的歷程記錄、已標記資料的一部分。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。

常用資料

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，修正程式通常在典型的 DevOps 發行工作流程之外建立。

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

將[基礎設施視為程式碼](#)。

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

在 90 天內的平均 CPU 和記憶體用量介於 5% 到 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、修補或修改現有基礎設施。與可變基礎設施相比，不可避免的[基礎設施](#)本質上更一致、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的部署](#)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 Security Reference Architecture](#) 建議使用傳入、傳出和檢查 VPCs 設定您的網路帳戶，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

由 [Klaus Schwab](#) 於 2016 年推出的術語，指透過連線能力、即時資料、自動化、分析和 AI/ML 的進步來現代化製造程序。

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[建置工業物聯網 \(IIoT\) 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 (在相同或不同的 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。[AWS Security Reference Architecture](#) 建議使用傳入、傳出和檢查 VPCs 設定您的 Network 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[AWS 的機器學習模型可解釋性](#)。

IoT

請參閱[物聯網](#)。

IT 資訊程式庫 (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 提供 ITSM 的基礎。

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。如需整合雲端操作與 ITSM 工具的相關資訊，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，其中每個使用者和資料本身都會明確指派安全標籤值。使用者安全標籤與資料安全標籤之間的交集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、彙整文件、將文字翻譯為其他語言，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[端點](#)。

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 服務可 AWS 操作基礎設施層、作業系統和平台，而且您可以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)

用於追蹤、監控、記錄和控制生產程序的軟體系統，可將原物料轉換為工廠的成品。

MAP

請參閱[遷移加速計畫](#)。

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。機制是在運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

除了屬於組織的管理帳戶 AWS 帳戶之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

MES

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

小型的獨立服務，透過定義明確的 APIs 進行通訊，通常由小型、獨立的團隊擁有。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 APIs 透過定義明確的界面進行通訊。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[在上實作微服務 AWS](#)。

遷移加速計畫 (MAP)

提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎以遷移至雲端，並協助抵銷遷移的初始成本的 AWS 計畫。MAP 包含以系統化方式執行舊版遷移的遷移方法，以及一組可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操作、業務分析師和擁有者、遷移工程師、開發人員，以及從事衝刺工作的 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。

遷移產品組合評估 (MPA)

線上工具，提供驗證商業案例以遷移至的資訊 AWS 雲端。MPA 提供詳細的產品組合評估（伺服器大小調整、定價、TCO 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、遷移優先順序和波規劃）。[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。

遷移就緒狀態評估 (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

用於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，並請參閱將[組織動員以加速大規模遷移](#)。

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 [中的應用程式現代化策略 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[不可變的基礎設施](#)作為最佳實務。

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[開啟程序通訊 - Unified Architecture](#)。

開放程序通訊 - Unified Architecture (OPC-UA)

工業自動化的 A machine-to-machine (M2M) 通訊協定。OPC-UA 提供具有資料加密、身分驗證和授權方案的互通性標準。

操作層級協議 (OLA)

闡明哪些功能性 IT 群組承諾交付給彼此的協議，以支援服務層級協議 (SLA)。

操作預備檢閱 (ORR)

問題及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[操作就緒審核 \(ORR\)](#)。

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 [Industry 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 AWS CloudTrail 的追蹤會記錄 AWS 帳戶組織中所有的事件 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[為組織建立追蹤](#)。

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 透過加速變革採用、解決轉型問題，以及推動文化和組織變革，協助組織準備和轉換至新系統和策略。在 AWS 遷移策略中，由於雲端採用專案所需的變更速度，因此此架構稱為人員加速。如需詳細資訊，請參閱[OCM 指南](#)。

原始存取控制 (OAC)

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

原始存取身分 (OAI)

In CloudFront，用於限制存取以保護您的 Amazon S3 內容的選項。當您使用 OAI 時，CloudFront 會建立 Amazon S3 可以驗證的主體。已驗證的主體只能透過特定 CloudFront 分佈存取 S3 儲存貯體中的內容。另請參閱[OAC](#)，它提供更精細和增強的存取控制。

ORR

請參閱[操作準備檢閱](#)。

OT

請參閱[操作技術](#)。

傳出 (傳出) 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 Security Reference Architecture](#) 建議使用傳入、傳出和檢查 VPCs 設定您的 Network 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

連接至 IAM 主體的 IAM 管理政策，用於設定使用者或角色可擁有的最大許可。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)

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

可以定義許可 (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最大許可的物件 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

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

容器，其中包含有關您希望 Amazon Route 53 如何回應一個或多個 DNS 內網域及其子網域的 VPCs 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](#)，並參閱在實作安全[控制項中的主動](#)控制項。 AWS

產品生命週期管理 (PLM)

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

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。此技術用於將複雜的任務分解為子任務，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關聯性，並允許更精細、更個人化的結果。

擬匿名化

將資料集中的個人識別碼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。

publish/subscribe (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以訂閱的頻道。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、知情 \(RACI\)](#)。

RAG

請參閱[擷取增強型生成](#)。

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、已諮詢、知情 \(RACI\)](#)。

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 Rs](#)。

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)

服務中斷和服務還原之間的可接受延遲上限。

重構

請參閱 [7 Rs](#)。

區域

地理區域 AWS 的資源集合。每個 AWS 區域 都獨立於其他，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 Rs](#)。

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 Rs](#)。

轉譯形式

請參閱 [7 Rs](#)。

回購

請參閱 [7 Rs](#)。

彈性

應用程式抵抗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](#)是常見的考量因素 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、負責、諮詢、知情 (RACI) 矩陣

定義所有涉及遷移活動和雲端操作之各方的角色和責任的矩陣。矩陣名稱衍生自矩陣中定義的責任類型：責任 (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，如果您排除該矩陣，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 Rs](#)。

淘汰

請參閱 [7 Rs](#)。

擷取增強產生 (RAG)

在產生回應之前，[LLM](#) 參考其訓練資料來源外之權威資料來源的 [生成 AI](#) 技術。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，讓攻擊者更難存取憑證。

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 由資料列許可和資料欄遮罩組成。

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 (IdPs) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必在 IAM 中為組織中的每個人建立使用者。如需 SAML 2.0 型聯合的詳細資訊，請參閱 [SAML 文件中的關於 Word 2.0 型聯合](#)。IAM

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，例如密碼或使用憑證。它由秘密值及其中繼資料組成。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。

安全資訊和事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具和服務。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，並產生警示。

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 執行個體或輪換憑證。

伺服器端加密

由接收資料的 AWS 服務 加密其目的地的資料。

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。SCPs 會定義管理員可委派給使用者或角色之動作的防護機制或設定限制。您可以使用 SCPs 作為允許清單或拒絕清單，以指定允許或禁止的服務或動作。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](#)。

服務層級協議 (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。

服務層級指示器 (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)

目標指標，代表服務的運作狀態，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](#)。

單一失敗點 (SPOF)

應用程式的單一關鍵元件發生故障，可能會中斷系統。

SLA

請參閱[服務層級協議](#)。

SLI

請參閱[服務層級指示器](#)。

SLO

請參閱[服務層級目標](#)。

split-and-seed 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[單一失敗點](#)。

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。此結構專為在[資料倉儲](#)中使用或用於商業智慧目的而設計。

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。如需如何套用此模式的範例，請參閱 [使用容器和 Amazon ASP Gateway 逐步現代化舊版 Microsoft ASMX.NET \(API\) Web 服務](#)。

子網

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

提供內容、指示或指引給 [LLM](#) 以指示其行為的技術。系統提示可協助設定內容，並建立與使用者互動的規則。

T

標籤

作為中繼資料的鍵值對，用於組織您的 AWS 資源。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

可用來互連 VPCs 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，以代表您在組織中執行任務 AWS Organizations，並在其帳戶中執行任務。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 [AWS Organizations 搭配使用其他 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。

雙披薩團隊

一個小型 DevOps 團隊，您可以使用兩個披薩來饋送。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

也稱為繁重型，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。未區分的任務範例包括採購、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

兩個 VPCs 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 Word 對等](#)。VPC

漏洞

損害系統安全性的軟體或硬體缺陷。

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，通常可接受中等慢的查詢。

視窗函數

SQL 函數，對以某種方式與目前記錄相關聯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 and 應用程式。

WORM

請參閱 [寫入一次，讀取許多](#)。

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

零時差漏洞

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。威脅實施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。

零擷取提示

為 [LLM](#) 提供執行任務的指示，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。零擷取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

平均 CPU 和記憶體用量低於 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。