



實作安全控制 AWS

AWS 規定指引



AWS 規定指引: 實作安全控制 AWS

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	2
控管架構中的安全控制	3
安全控制的類型	4
預防性控制	4
目標	4
處理	5
使用案例	5
技術	6
業務成果	7
主動性控制	7
目標	8
處理	8
使用案例	8
技術	9
業務成果	9
偵測性控制	10
目標	10
處理	10
使用案例	11
技術	11
業務成果	13
回應性控制	14
目標	14
處理	14
使用案例	15
技術	15
業務成果	15
後續步驟	16
常見問答集	17
如果我的時間和資源有限且無法實作所有這些控制類型，我應關注什麼？	17
資源	18
AWS 文件	18

AWS 部落格文章	18
其他資源	18
文件歷史紀錄	19
詞彙表	20
#	20
A	20
B	23
C	24
D	27
E	30
F	32
G	33
H	33
I	34
L	36
M	37
O	40
P	43
Q	45
R	45
S	48
T	50
U	52
V	52
W	52
Z	53
.....	liv

在 AWS 上實作安全控制

Iqbal Umair、Gurpreet Kaur Cheema、Wasim Hossain、Joseph Nguyen、San Brar 和 Lucia Vanta，Amazon Web Services (AWS)

2023 年 12 月 ([文件歷史記錄](#))

安全對每個公司都至關重要，也是 AWS Well-Architected Framework 的關鍵支柱。但是，許多人不知道如何遵循安全考量事項進行操作並為雲端環境建立全面的自動化安全測試和修復策略。透過使用 AWS 服務和工具，例如 AWS Config、Amazon GuardDuty 和 AWS CloudFormation，您可以建立安全測試策略並將其建置到您的 AWS 雲端環境。

為了協助符合公司的安全政策和標準，安全控制是技術或管理防護機制，有助於防止、偵測或降低威脅執行者利用安全漏洞的能力。其旨在保護資源和資料的機密性、完整性和可用性。以下是安全控制的範例：

- 為需要登入應用程式的使用者實作多重要素驗證
- 記錄、監控和查詢動作，以便對帳戶活動執行即時稽核
- 確保敏感資料已加密
- 確保根據公司的保留政策儲存日誌

安全控制有四種類型：預防性、主動性、偵測性以及回應式。本指南更詳細地描述了每種類型，並重點介紹如何在 AWS 雲端中實作和自動化這些控制。本指南可協助您實作持續且主動的安全控制。

目標對象

本指南面向負責在 AWS 雲端中實作安全控制的架構師和安全工程師。如果您的公司尚未定義安全政策、控制目標或標準 (如 [控管架構中的安全控制](#) 所述)，我們建議您在繼續本指南之前完成這些控管任務。

目標業務成果

公司使用安全控制來減輕 IT 系統風險或作為針對此風險的對策。控制定義了滿足 IT 程式及其安全策略的主要安全目標的要求基準。適當的控制可透過保護資料和 IT 資產的機密性、完整性和可用性，來改善公司的安全狀態。如果沒有控制，就很難知道需要在哪裡關注和投資來建立安全基準。

安全控制可用於解決各種情況。範例包括滿足源自於風險評定的要求、達到產業標準或遵守法規。滿足安全控制表明您已衡量系統的風險，確定了所需的保護層級，並主動實作了解決方案。其他因素 (例如業務、產業和地理位置) 都可以決定您所需的安全控制。

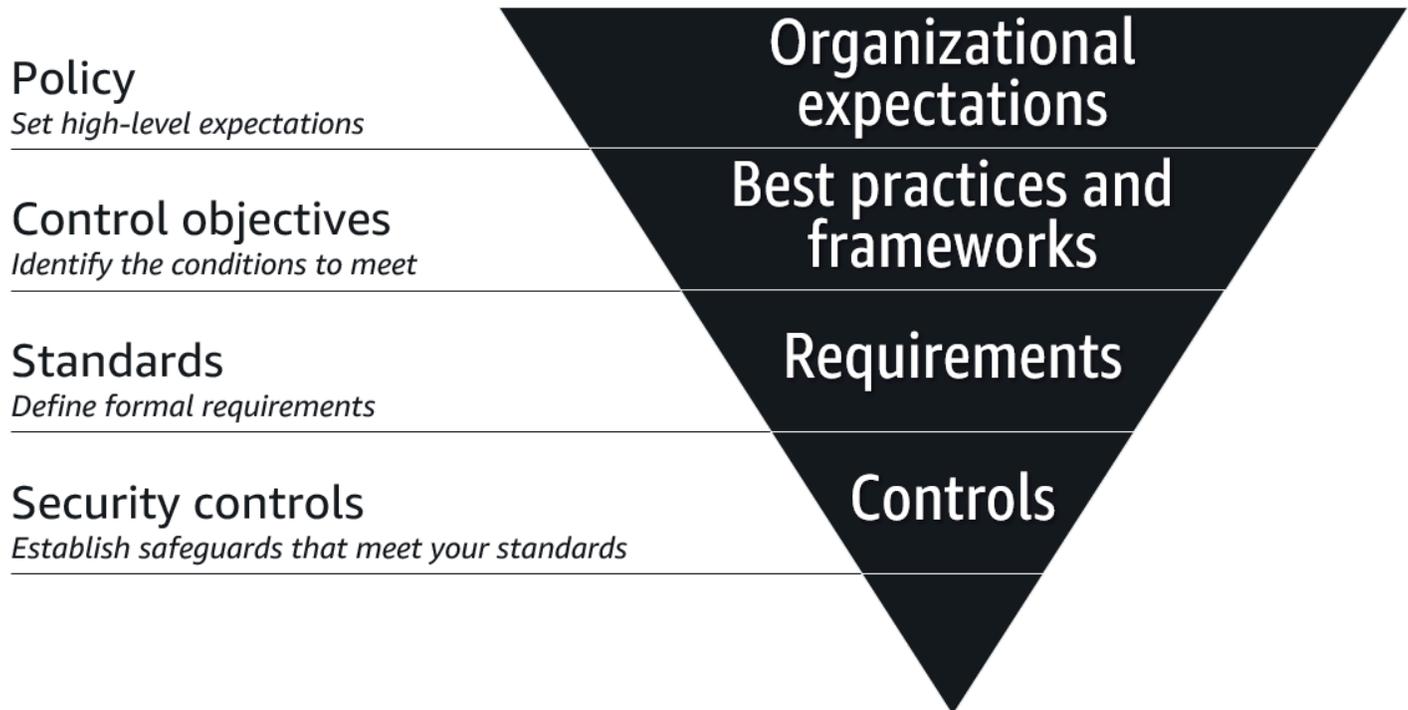
以下是實作安全控制的常見使用案例：

- 應用程式的安全評定已根據正在處理的資料敏感性識別存取控制的需求。
- 您必須遵守安全標準，例如支付卡產業資料安全標準 (PCI DSS)、HIPAA (美國健康保險流通與責任法案) 或國家標準技術研究所 (NIST)。
- 您需要保護商業交易的敏感資訊。
- 您的公司已擴展到需要安全控制的地理區域，例如需要遵守一般資料保護規範 (GDPR) 的區域。

閱讀本指南後，您應熟悉四種類型的的安全控制，了解其如何成為安全控管架構的一部分，並準備好開始在 AWS 雲端 中實作和自動化安全控制。

控管架構中的安全控制

從基礎層面進行規劃非常重要。如何開始？下圖顯示如何根據政策、控制目標、標準和安全控制建置安全控管策略。



以下是安全控管策略的階層元件：

- 政策 – 政策是任何網路安全控管策略的基礎。它是一份說明公司預期 (例如必須履行的法定、法規或合約義務) 的文件。政策可能因產業和區域而異。
- 控制目標 – 控制目標是可協助您符合政策意圖的目標，例如業界認可的最佳實務。對於雲端運算，許多公司採用 [雲端控制矩陣 \(CCM\)](#) (雲端安全聯盟網站)，這是網路安全控制目標的架構。
- 標準 – 標準是滿足控制目標的正式制定的要求。標準可能包括程序、動作或組態，並且可量化，以便您可以根據標準衡量效能。
- 安全控制 – 安全控制是您為實作標準所採取的技術或管理機制。所有安全控制都映射至標準，但並非所有標準都映射至安全控制。安全控制測試旨在監控和衡量您是否有效地滿足定義的標準。

本指南重點介紹如何在 AWS 雲端 中設計和實作常見類型的安全控制。

安全控制的類型

安全控制有以下四種主要類型：

- [預防性控制](#) – 這些控制旨在防止事件發生。
- [主動性控制](#) – 這些控制旨在防止建立不合規的資源。
- [偵測性控制](#) – 這些控制旨在事件發生後偵測、記錄和提醒。
- [回應性控制](#) – 這些控制旨在驅動不良事件或偏離安全基準的補救措施。

有效的安全策略包括所有四種類型的的安全控制。雖然預防性控制是協助防止未經授權的存取或對網路進行不必要變更的第一道防線，但請務必確保建立偵測性和回應性控制，以便您知道事件何時發生，且可以立即採取適當的措施進行修復。使用主動性控制可增加另一層安全性，因為它補充了預防性控制，而預防性控制通常在本質上更嚴格。

以下章節更詳細地描述了每種類型的控制。討論了每種控制類型的目標、實作程序、使用案例、技術考量事項和目標結果。

預防性控制

預防性控制旨在防止事件發生的安全控制。這些防護機制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。預防性控制的範例是具有唯讀存取權的 AWS Identity and Access Management (IAM) 角色，因為它有助於防止未經授權的使用者發生意外的寫入動作。

檢閱下列有關此類型控制的資訊：

- [目標](#)
- [處理](#)
- [使用案例](#)
- [技術](#)
- [業務成果](#)

目標

預防性控制的主要目的是最大限度地減少或避免威脅事件發生的可能性。此控制應有助於防止未經授權存取系統，並有助於防止意外的變更影響系統。以下是預防性控制的目標：

- 職責分離 – 預防性控制可以建立限制權限的邏輯界限，允許許可僅在指定帳戶或環境中執行特定任務。範例包括：
 - 將工作負載分段至特定服務的不同帳戶
 - 分隔並考慮獨立的生產、開發和測試環境
 - 將存取權和責任委派給多個實體以執行特定功能，例如使用 IAM 角色或擔任的角色以僅允許特定的工作職能執行某些動作
- 存取控制 – 預防性控制可以一致地授予或拒絕對環境中資源和資料的存取。範例包括：
 - 防止使用者超出預期許可，稱為權限提升
 - 僅限授權使用者和服務存取應用程式和資料
 - 保持管理員群組較小
 - 避免使用根使用者憑證
- 強制執行 – 預防性控制可以協助您的公司遵守其政策、指引和標準。範例包括：
 - 作為最低安全基準的鎖定組態
 - 實作其他安全措施，例如多重要素驗證
 - 避免由未經核准的角色執行的非標準任務和動作

處理

預防性控制映射是將控制映射至需求並使用政策透過限制、停用或封鎖來實作這些控制的程序。在映射控制時，考慮控制對環境、資源和使用者的主動影響。以下是映射控制的最佳實務：

- 禁止某項活動的嚴格控制應該映射至該動作需要審核、核准和變更程序的生產環境。
- 開發或封閉環境可能需要較少的預防性控制才能提供建置和測試的敏捷性。
- 資料的分類、資產的風險層級和風險管理政策決定了預防性控制。
- 映射至現有架構作為遵守標準和法規的證據。
- 依地理位置、環境、帳戶、網路、使用者、角色或資源實作預防性控制。

使用案例

標籤處理

建立可以存取帳戶中的所有資料的角色。如果存在敏感的加密資料，過度寬鬆的權限可能會帶來風險，這取決於可以擔任該角色的使用者或群組。透過使用 AWS Key Management Service (AWS KMS) 中的金鑰政策，您可以控制擁有金鑰存取權的人員，並可以解密資料。

權限提升

如果管理和寫入許可指派得太寬泛，則使用者可以規避其預期許可的限制並授予自己其他權限。建立和管理角色的使用者可以指派許可界限，該界限定義了角色允許的最大權限。

工作負載鎖定

如果您的企業沒有使用特定服務的可預見需求，請啟用服務控制策略，以限制哪些服務可以在組織的成員帳戶中運行，或根據 AWS 區域如果威脅行為者設法洩露和存取您組織中的帳戶，此預防性控制可以減少影響範圍。如需詳細資訊，請參閱本指南中的 [服務控制政策](#)。

對其他應用程式的影響

預防性控制可以強制使用 IAM、加密和日誌記錄等服務和功能，以符合應用程式的安全要求。您也可以使用這些控制來限制威脅行為者因意外錯誤或組態錯誤而可能利用的操作，從而協助防範漏洞。

技術

服務控制政策

在中 AWS Organizations，[服務控制策略](#) (SCP) 會定義組織中成員帳戶的最大可用權限。這些政策可協助帳戶遵守組織的存取控制指導方針。為您的組織設計 SCP 時，請注意下列事項：

- SCP 是預防性控制，因為它們會為組織成員帳戶中的 IAM 角色和使用者定義並強制執行允許的最大許可。
- SCP 只會影響組織成員帳戶中的 IAM 角色和使用者。它不會影響組織管理帳戶中的使用者和角色。

您可以透過定義每個 AWS 區域的許可上限來使 SCP 更加精細。

IAM 許可界限

在 AWS Identity and Access Management (IAM) 中，使用許可[界限](#)設定以身分為基礎的政策可授予 IAM 實體 (使用者或角色) 的最大許可。實體的許可界限可讓其僅執行由身分型政策和許可界限同時允許的動作。使用許可界限時，請注意下列事項：

- 您可以使用 AWS 受管政策或客戶受管政策來設定 IAM 實體的界限。
- 許可界限不會自行授予許可。許可界限政策會限制授予 IAM 實體的許可。

業務成果

節省時間

- 透過在設定預防性控制後新增自動化，您可以減少手動介入需求並降低錯誤頻率。
- 使用許可界限作為預防性控制有助於安全和 IAM 團隊專注於關鍵任務，例如控管和支援。

法規合規

- 公司可能需要遵守內部或產業法規。這些可以是區域限制、使用者和角色限制或服務限制。SCP 可以協助您保持合規並避免違規處罰。

降低風險

- 隨著成長，建立和管理新角色和政策的請求數量也會增加。了解為每個應用程式手動建立許可所需的內容變得更具挑戰性。建立預防性控制作為基準，有助於防止使用者執行意外動作，即使他們意外取得存取權亦如此。
- 將預防性控制套用至存取政策提供了額外層來協助保護資料和資產。

主動性控制

主動控制是旨在防止建立不合規資源的安全控制。這些控制可以減少回應式和偵測性控制處理的安全事件數量。這些控制可確保已部署的資源在部署之前符合要求；因此，不存在需要回應或修復的偵測事件。

例如，您可能具有一個偵測性控制，當 Amazon Simple Storage Service (Amazon S3) 儲存貯體變成可公開存取時通知您。您也可能具有可修復此問題的回應式控制。雖然您已具有這兩個控制，但是可以新增主動性控制來多加一道保護。透過主動控制 AWS CloudFormation，可防止建立任何已啟用公開存取權的 S3 儲存貯體的更新。威脅執行者仍可略過此控制項，並在其外部部署或修改資源 CloudFormation。在這種情況下，偵測性和回應式控制將修復安全事件。

檢閱下列有關此類型控制的資訊：

- [目標](#)
- [處理](#)
- [使用案例](#)
- [技術](#)

• [業務成果](#)

目標

- 主動性控制可協助您改進安全操作和品質程序。
- 主動性控制可以協助您遵守安全政策、標準，以及法規或合規義務。
- 主動性控制可以防止建立不合規資源。
- 主動性控制可以減少安全調查結果的數量。
- 主動性控制提供了另一層保護，防止威脅執行者繞過預防性控制並嘗試部署不合規資源。
- 主動性控制與預防性、偵測性和回應式控制相結合，可以協助您解決潛在的安全事件。

處理

主動性控制可補充預防性控制。主動性控制可降低組織的安全風險，並強制部署合規資源。這些控制會在建立或更新資源之前評估資源合規性。主動控制通常通過使用 CloudFormation 鉤子來實現。如果資源未通過主動性控制驗證，您可以選擇使資源部署失敗或顯示警告訊息。以下是建置主動性控制的一些秘訣和最佳實務：

- 確保主動性控制已映射至組織的合規要求。
- 確保主動性控制遵循關聯服務的安全最佳實務。
- 使用 CloudFormation StackSets 或其他解決方案，跨多個帳戶 AWS 區域 或帳戶部署主動式控制。
- 確保與主動性控制關聯的警告或失敗訊息明確且清晰。這可協助開發人員了解資源未通過評估的原因。
- 建置新的主動式控制項時，在觀察模式下啟動。這表示您傳送警告訊息，而非使資源部署失敗。這可協助您了解主動性控制的影響。
- 在 Amazon CloudWatch 日誌中啟用日誌記錄以獲得主動控制。
- 如果您需要監控特定主動控制的叫用，請使用 Amazon EventBridge 規則並訂閱勾點的叫用事件。
CloudFormation

使用案例

- 防止部署不合規資源
- 符合合規要求

- 透過在部署之前強制修復安全問題來提高程式碼品質
- 減少部署之後與修復安全問題關聯的營運停機時間

技術

CloudFormation 掛鉤

[AWS CloudFormation](#)協助您設定 AWS 資源、快速且一致地佈建資源，以及跨區域的整個生命週期進 AWS 帳戶行管理。[CloudFormation 掛接](#)會在部署 CloudFormation 資源之前主動評估資源的組態。如果找到不合規資源，則會傳回失敗狀態。根據掛接失敗模式，CloudFormation可能會使作業失敗或顯示警告，以允許使用者繼續部署。您可以使用可用的勾點，也可以開發自己的勾點。

AWS Control Tower

[AWS Control Tower](#)協助您設定和管理 AWS 多帳戶環境，遵循規範的最佳做法。AWS Control Tower 提供預先設定的[主動控制](#)功能，您可以在 landing zone 啟用。如果您的 landing zone 域設定為使用 AWS Control Tower，您可以使用這些選用的主動式控制項做為組織的起點。您可以視需要在中建置額外的自訂主動 CloudFormation 式控制項。

業務成果

減少人工和錯誤

主動性控制可降低導致部署不合規資源的人為錯誤風險。這些控制還可減少開發週期後期的人工，因為它們使開發人員在部署之前考慮資源安全性。這將左移實務套用於建置安全資源，因為它強制在開發生命週期的早期實現合規性。

降低了成本

在部署之後修正安全問題通常成本較高。在開發週期的早期識別並修正問題可降低開發成本。

節省時間

由於主動性控制可防止部署不合規資源，因此可以減少您用於分類和修正安全問題的時長。它們還包括安全調查結果的數量，偵測性控制將在開發週期後期識別這些安全調查結果。

法規合規

如果您的組織需要遵守內部或產業法規，主動性控制可以協助您保持合規並避免違規處罰。

降低風險

主動性控制可協助開發人員部署合規並更安全地建置資源，因此主動性控制可降低組織的安全風險。

偵測性控制

偵測性控制是安全控制，旨在事件發生後偵測、記錄和提醒。偵測性控制是控管架構的基礎部分。這些防護機制是第二道防線，通知您繞過預防性控制的安全問題。

例如，您可以套用偵測性控制來偵測 Amazon Simple Storage Service (Amazon S3) 儲存貯體是否可公開存取並通知您。雖然您可能已採取預防性控制，在帳戶層級停用對 S3 儲存貯體的公開存取，然後停用透過 SCP 的存取，但威脅行為者可以透過以管理使用者身分登入來規避這些預防性控制。在這些情況下，偵測性控制可以提醒您組態錯誤和潛在威脅。

檢閱下列有關此類型控制的資訊：

- [目標](#)
- [處理](#)
- [使用案例](#)
- [技術](#)
- [業務成果](#)

目標

- 偵測性控制可協助您改進安全操作程序和品質程序。
- 偵測性控制可協助您履行法規、法律或合規義務。
- 偵測性控制為安全營運團隊提供了回應安全問題的可見性，包括繞過預防性控制的進階威脅。
- 偵測性控制可以協助您識別對安全問題和潛在威脅的適當回應。

處理

您可以分兩個階段實作偵測性控制。首先，設定系統將事件和資源狀態記錄到集中的位置，例如 Amazon CloudWatch Logs。集中式日誌記錄到位後，您可以分析這些日誌以偵測可能表示威脅的異常狀況。每個分析都是一個映射回您的原始需求和政策的控制。例如，您可以建立偵測性控制，以在日誌中搜尋特定模式，並在符合時產生提醒。安全團隊使用偵測性控制來提高對系統可能面臨的威脅和風險的整體可見性。

使用案例

偵測可疑行為

偵測性控制有助於識別任何異常活動，例如洩露特權使用者憑證或者存取或外洩敏感資料。這些控制是重要的反應因素，可以協助您的公司識別和了解異常活動的範圍。

偵測詐欺

這些控制有助於偵測和識別公司內部的威脅，例如規避政策和執行未經授權的交易的使用者。

合規

偵測性控制可協助您符合合規要求，例如支付卡產業資料安全標準 (PCI DSS)，並有助於防止身分盜用。這些控制可以協助您探索和保護受法規合規約束的敏感資訊，例如個人身分識別資訊。

自動化分析

偵測性控制可以自動分析日誌以偵測異常狀況和未經授權活動的其他指標。

您可以自動分析來自不同來源的日誌 (例如 AWS CloudTrail 日誌、[VPC 流程日誌](#)和網域名稱系統 (DNS) 日誌)，以發現潛在惡意活動的跡象。為了協助組織，將多個安全警示或發現項目彙總 AWS 服務到一個集中位置。

技術

常見的偵測性控制是實作一或多個監控服務，這些服務可以分析資料來源 (例如日誌) 以識別安全威脅。在中 AWS 雲端，您可以分析 AWS CloudTrail 日誌、Amazon S3 存取日誌和 Amazon Virtual Private Cloud 流程日誌等來源，以協助偵測異常活動。AWS Amazon GuardDuty，Amazon Detective 和亞馬 Amazon Macie 等安全服務具有內置的監控功能。AWS Security Hub

GuardDuty 和 Security Hub

[Amazon GuardDuty](#) 使用威脅情報、機器學習和異常偵測技術，持續監控您的日誌來源是否存在惡意或未經授權的活動。儀表板提供您 AWS 帳戶 和工作負載的即時健康狀態的深入解析。您可以整合 GuardDuty 合雲端安全狀態管理服務 [AWS Security Hub](#)，以檢查是否遵守最佳實務、彙總警示並啟用自動修復。GuardDuty 將發現項目傳送至 Security Hub，作為集中資訊的一種方式。您可以進一步將 Security Hub 與安全資訊和事件管理 (SIEM) 解決方案整合，以擴展組織的監控和提醒功能。

Macie

[Amazon Macie](#) 是一種全受管資料安全和資料隱私權服務，該服務使用機器學習和模式比對來協助探索和保護 AWS 中的敏感資料。以下是 Macie 中提供的一些偵測性控制和功能：

- Macie 會檢查儲存貯體庫存和儲存在 Amazon S3 中的所有物件。此資訊可以在單一儀表板檢視中呈現，提供可見性並協助您評估儲存貯體安全性。
- 為了探索敏感資料，Macie 使用內建的受管資料識別符，並且還支援自訂資料識別符。
- Macie 與其他工具本地集 AWS 服務 成。例如，Macie 發布發現為 Amazon EventBridge 事件，這些事件會自動發送到 Security Hub。

以下是在 Macie 中設定偵測性控制的最佳實務：

- 在所有帳戶上啟用 Macie。透過使用委派的管理功能，使用 AWS Organizations 在多個帳戶上啟用 Macie。
- 使用 Macie 評估您帳戶中 S3 儲存貯體的安全狀態。這有助於透過提供資料位置和存取的可見性來防止資料遺失。如需詳細資訊，請參閱[分析您的 Amazon S3 安全狀態](#) (Macie 文件)。
- 透過執行和排程自動處理和資料探索作業，自動探索 S3 儲存貯體中的敏感資料。這會定期檢查 S3 儲存貯體中是否有敏感資料。

AWS Config

[AWS Config](#) 審計和記錄資 AWS 源的合規性。AWS Config 探索現有 AWS 資源並產生完整庫存，以及每個資源的組態詳細資料。如果存在任何組態變更，則會記錄這些變更並提供通知。這可以協助您偵測並復原未經授權的基礎設施變更。您可以使用 AWS 受管規則，也可以建立自訂規則。

以下是在 AWS Config 中設定偵測性控制的最佳實務：

- 針 AWS Config 對組織中的每個成員帳號，以及包含您要保護之資源的每個 AWS 區域 成員帳號啟用。
- 針對任何組態變更，設定 Amazon Simple Notification Service (Amazon SNS) 提醒。
- 將組態資料儲存在 S3 儲存貯體中，並使用 Amazon Athena 進行分析。
- 使用 [自動化](#) (AWS Systems Manager 的一項功能) 來自動修復不合規資源。
- 使用 EventBridge 或 Amazon SNS 設定有關不合規 AWS 資源的通知。

Trusted Advisor

[AWS Trusted Advisor](#) 可以用作偵測性控制的服務。透過一組檢查，Trusted Advisor 找出您可以最佳化基礎架構、改善效能和安全性或降低成本的區域。Trusted Advisor 根據您可以遵循的 AWS 最佳做法提供建議，以改善您的服務和資源。商業和企業 Support 計劃可讓您存取 AWS Well-Architected 架構支柱的所有可用檢查。

以下是在 Trusted Advisor 中設定偵測性控制的最佳實務：

- 檢閱檢查層級摘要
- 針對警告和錯誤狀態實作資源特定的建議。
- Trusted Advisor 經常檢查以積極檢討和實施其建議。

Amazon Inspector

[Amazon Inspector](#) 是一項自動化漏洞管理服務，在啟用之後，可持續掃描您的工作負載，以尋找任何意外的網路暴露或軟體漏洞。它將調查結果融入風險分數中，可以協助您確定後續步驟，例如修復或確認合規狀態。

以下是在 Amazon Inspector 中設定偵測性控制的最佳實務：

- 在所有帳戶上啟用 Amazon Inspector，並將其整合到 EventBridge 和 Security Hub，以設定安全漏洞的報告和通知。
- 根據 Amazon Inspector 風險分數，排定修復和其他動作的優先順序。

業務成果

減少人工和錯誤

您可以使用基礎設施即程式碼 (IaC) 來實現自動化。自動化部署、監控組態及修復服務和工具可降低手動錯誤的風險，並減少擴展這些偵測性控制所需的時間和精力。自動化有助於制定安全執行手冊，並減少安全分析師的手動操作。定期審核有助於調整自動化工具並持續反覆運算並改進偵測性控制。

針對潛在威脅採取適當動作

從日誌和指標中擷取和分析事件對於取得可見性至關重要。這有助於分析師針對安全事件和潛在威脅採取行動，以協助保護您的工作負載。可以快速識別存在的漏洞，有助於分析師採取適當的動作來解決和修復這些漏洞。

更好的事件回應和調查處理

自動化偵測性控制工具可以提高偵測、調查和復原的速度。基於定義條件的自動提醒和通知可讓安全分析師適當地調查和回應。這些回應因素可以協助您識別和了解異常活動的範圍。

回應性控制

回應性控制是安全控制，旨在驅動不良事件或偏離安全基準的補救措施。技術回應性控制的範例包括修補系統、隔離病毒、關閉程序或重新啟動系統。

檢閱下列有關此類型控制的資訊：

- [目標](#)
- [處理](#)
- [使用案例](#)
- [技術](#)
- [業務成果](#)

目標

- 回應性控制可以協助您為常見類型的攻擊 (例如網路釣魚或暴力破解) 建立執行手冊。
- 回應性控制可以實作對潛在安全問題的自動回應。
- 回應式控制項可自動修復 AWS 資源上未預期或未核准的動作，例如刪除未加密的 S3 儲存貯體。
- 回應性控制可以與預防性和偵測性控制進行協調，以建立一種全面、主動的方法來解決潛在的安全事件。

處理

偵測性控制是建立回應性控制的先決條件。您必須能夠偵測安全問題，然後才能進行修復。然後，您可以建立針對安全問題的政策或回應。例如，如果發生暴力攻擊，將實作修復程序。修復程序存在後，可以使用程式設計語言 (例如 Shell 指令碼) 將其自動化並作為腳本執行。

考慮回應性控制是否可能破壞現有的生產工作負載。例如，如果偵測性安全控制是 S3 儲存貯體不得公開存取和修復是關閉 Amazon S3 的公開存取，這可能會對您的公司及其客戶產生重大影響。如果 S3 儲存貯體為公有網站提供服務，則關閉公有存取可能會導致中斷。資料庫是一個類似的範例。如果資料庫不得透過網際網路公開存取，則關閉公開存取可能會影響應用程式的連線。

使用案例

- 自動回應偵測到的安全事件
- 自動修復偵測到的安全漏洞
- 自動復原控制可減少營運停機時間

技術

安全中樞

[AWS Security Hub](#) 自動將所有新發現項目和現有發現的所有更新 EventBridge 作為事件發送到。您也可以建立自訂動作，將選取的發現項目和深入分析結果傳送至 EventBridge。您可以設定 EventBridge 回應每種類型的事件。此事件可啟動執行修正動作的 AWS Lambda 函數。

AWS Config

[AWS Config](#) 使用規則來評估您的 AWS 資源，並協助您修復不符合標準的資源。AWS Config 使用 [AWS Systems Manager 自動化](#) 套用補救。在「自動化」文件中，您可以定義要對 AWS Config 決定不相容的資源執行的動作。建立自動化文件之後，您可以透過 AWS Management Console 或使用 API 在 Systems Manager 中使用這些文件。您可以選擇手動或自動修復不符合標準的資源。

業務成果

最大限度地減少資料損失

在網路安全事件發生後，使用回應性安全控制可以協助最大限度地減少資料損失以及對系統或網路的損壞。回應性控制還可以協助盡快還原關鍵業務系統和程序，從而增強工作負載的恢復能力。

降低成本

自動化可降低與人力資源相關的成本，因為團隊成員不必手動回應事件或以其他方式對事件進行管 case-by-case 理。

後續步驟

閱讀本指南後，您應熟悉四種類型的**安全控制**，了解其如何成為**安全控管架構**的一部分，並準備好開始在**AWS 雲端**中實作和**自動化安全控制**。如需詳細資訊，我們建議您檢閱包含在 [資源](#) 部分中的參考。

我們也建議您採取下列後續步驟來評估雲端基礎設施的安全性並開始實作安全控制：

1. 啟用和設定 AWS Security Hub。作為最佳實務，我們建議啟用可用的標準控制。如需詳細資訊，請參閱 [安全標準和控制](#) (Security Hub 文件)。
2. 啟用和設定 AWS Config。如需詳細資訊，請參閱 [入門](#) (AWS Config 文件)。
3. 使用 AWS 服務 (例如 Security Hub、Amazon Macie、AWS Config、AWS Trusted Advisor 和 Amazon Inspector) 評估您的組織和帳戶基礎設施，識別需要改進的區域，並對這些服務進行審核和提出建議。使用 Security Hub 中的安全檢查功能來產生安全標準的安全分數。如需詳細資訊，請參閱 [確定安全分數](#) (Security Hub 文件)。
4. 根據已確定的改進實作預防性、主動性、偵測性和回應性安全控制。
5. 進行後續安全評定，以評估所實作安全控制的有效性。在 Security Hub 中，確定安全分數是否已提升。反覆運算以改進或新增安全控制。
6. 建立執行安全評定的定期頻率，例如每年。

常見問答集

如果我的時間和資源有限且無法實作所有這些控制類型，我應關注什麼？

我們建議實作 AWS Security Hub。Security Hub 具有一組自動化安全控制，稱為 [AWS 基礎安全最佳實務標準](#) (Security Hub 文件)。這是由 AWS 安全專家管理的一組精心策劃的安全最佳實務。您可以在關聯資源發生變更時連續執行這些標準控制，也可以定期執行。每個控制都有特定的嚴重性評分，可協助您排定修正作業的優先順序。如需詳細資訊，請參閱[執行安全檢查](#) (Security Hub 文件)。如果您正在使用 AWS Control Tower，也可以檢閱並選擇啟用其預防性、偵測和主動性[控制](#)。

資源

AWS 文件

- [AWS 安全參考架構 \(AWS SRA\)](#)
- [AWS CAF 安全層面](#)
- [安全、身分和合規的最佳實務](#)
- AWS 上的自動化安全回應 (AWS 解決方案)
 - [解決方案登陸頁面](#)
 - [實作指南](#)

AWS 部落格文章

- [身分指南 – 透過 AWS 身分進行預防性控制 – SCP](#)
- [如何為 AWS Organizations 中的帳戶實作唯讀服務控制政策 \(SCP\)](#)
- [多帳戶環境中 AWS Organizations 服務控制政策的最佳實務](#)
- [使用服務控制政策維護合規並確保永遠將其套用](#)
- [何時何地使用 IAM 許可界限](#)
- [主動確保資源安全並符合 AWS CloudFormation 勾點要求](#)

其他資源

- [雲端控制矩陣 \(CCM\) \(雲端安全聯盟\)](#)
- [許可界限範例 \(GitHub\)](#)

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
主動性控制	我們在本指南中新增了有關主動性控制的資訊，包括 主動性控制 部分。	2023 年 12 月 4 日
初次出版	—	2022 年 12 月 12 日

AWS 規定指引詞彙

以下是 AWS 規範性指引所提供的策略、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 Postgre SQL 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：將您的現場部署 Oracle 資料庫遷移至 Amazon Relational Database Service 服務 (AmazonRDS)，適用於 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：將您的內部部署 Oracle 資料庫移轉至中 EC2 執行個體上的 Oracle 資料庫 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 應用程式移轉至 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

請參閱以 [屬性為基礎的存取控制](#)。

抽象的服務

請參閱[受管理服務](#)。

ACID

請參閱[原子性、一致性、隔離性、耐用性](#)。

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。它比[主動-被動遷移](#)更具彈性，但需要更多的工作。

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。

聚合函數

此SQL函數會在一組資料列上運作，並計算群組的單一傳回值。彙總函式的範例包括SUM和MAX。

AI

請參閱[人工智慧](#)。

AIOps

請參閱[人工智慧作業](#)。

匿名化

永久刪除資料集中個人資訊的程序。匿名化可以幫助保護個人隱私。匿名資料不再被視為個人資料。

反模式

一種常用的解決方案，用於重複發生的問題，其中解決方案是適得其反，無效，或者比替代方案效果低。

應用控制

一種安全性方法，只允許使用核准的應用程式，以協助保護系統免受惡意軟體的攻擊。

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？](#)

人工智能操作 (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 AIOps 在 AWS 移轉策略中使用的詳細資訊，請參閱[作業整合指南](#)。

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，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。

以屬性為基礎的存取控制 () 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](#) AWS 中的「」。

授權資料來源

儲存資料主要版本的位置，被認為是最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以便處理或修改資料，例如匿名化、編輯或將其虛擬化。

可用區域

一個獨立的位置，與其他 AWS 區域 可用區域中的故障隔離，並為相同區域中的其他可用區域提供廉價、低延遲的網路連線能力。

AWS 雲端採用架構 (AWS CAF)

指導方針和最佳做法的架構，可協 AWS 助組織制定有效率且有效的計畫，以順利移轉至雲端。AWS CAF 將指引組織到六個重點領域中，稱為「觀點」：商業、人員、治理、平台、安全性和營運。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。針對此觀點，AWS CAF 提供人員開發、訓練和通訊的指引，協助組織為成功採用雲端做好準備。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)

可評估資料庫移轉工作負載、建議移轉策略並提供工作預估的工具。AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。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

壞機器人

旨在破壞或對個人或組織造成傷害的**機器人**。

BCP

請參閱[業務連續性規劃](#)。

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。您可以使用 Amazon Detective 的行為圖表來檢查失敗的登入嘗試、可疑 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「[位元順序](#)」。

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

建立兩個獨立但相同環境的部署策略。您可以在一個環境中執行目前的應用程式版本 (藍色)，而在另一個環境 (綠色) 中執行新的應用程式版本。此策略可協助您以最小的影響快速回復。

機器人

透過網際網路執行自動化工作並模擬人類活動或互動的軟體應用程式。某些漫遊器是有用的或有益的，例如用於索引 Internet 上信息的網絡爬蟲。其他一些機器人 (稱為不良機器人) 旨在破壞或對個人或組織造成傷害。

殭屍網絡

受**惡意軟件**感染並受到單一方 (稱為**機器人牧民**或**機器人操作員**) 控制的**機器人網絡**。殭屍網絡是擴展**機器人**及其影響的最著名機制。

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)。

防碎玻璃訪問

在特殊情況下，並透過核准的程序，使用者可以快速取得他 AWS 帳戶 們通常沒有存取權限的存取權。如需詳細資訊，請參閱 AWS Well-Architected 指南中的[實作防破玻璃程序](#)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](#)。

金絲雀部署

向最終用戶發行版本的緩慢和增量版本。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[雲端卓越中心](#)。

CDC

請參閱[變更資料擷取](#)。

更改數據捕獲 (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改的中繼資料的程序。您可以將其用CDC於各種目的，例如稽核或複寫目標系統中的變更，以維護同步化。

混沌工程

故意引入故障或破壞性事件來測試系統的彈性。您可以使用 [AWS Fault Injection Service \(AWS FIS\)](#) 執行實驗來 stress 您的 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。

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。雲計算通常連接到[邊緣計算](#)技術。

雲端運作模式

在 IT 組織中，這是用來建置、成熟和最佳化一或多個雲端環境的作業模型。如需詳細資訊，請參閱[建立您的雲端作業模型](#)。

採用雲端階段

組織移轉至下列四個階段時通常會經歷 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率 (例如，建立 landing zone、定義 CCoE、建立營運模式)
- 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

這些階段是 Stephen Orban 在 AWS 雲端 企業策略部落格部落格文章 [「邁向雲端優先的旅程與採用階段」](#) 中所定義的。如需其與 AWS 移轉策略之間關聯的詳細資訊，請參閱 [移轉準備指南](#)。

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。常見的雲儲存庫包括 GitHub 或 AWS CodeCommit。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。查詢此類資料時，通常可以接受慢速查詢。將此資料移至效能較低且成本較低的儲存層或類別可降低成本。

計算機視覺 (CV)

一個 [AI](#) 領域，它使用機器學習來分析和從數字圖像和視頻等視覺格式中提取信息。例如，提 AWS Panorama 供將 CV 添加到現場部署攝像機網絡的設備，Amazon 為 CV SageMaker 提供圖像處理算法。

配置漂移

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

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 CMDB 在移轉的產品組合探索和分析階段使用資料。

一致性套件

AWS Config 規則和補救動作的集合，您可以組合這些動作來自訂合規性和安全性檢查。您可以使用範本，將一致性套件部署為 AWS 帳戶 和區域中的單一YAML實體，或跨組織部署。如需詳細資訊，請參閱文件中的[AWS Config 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 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 架構中安全性支柱的一個組成部分。如需詳細資訊，請參閱[資料分類](#)。

資料漂移

生產資料與用來訓練 ML 模型的資料之間有意義的變化，或輸入資料隨著時間的推移有意義的變化。資料漂移可降低 ML 模型預測中的整體品質、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

透過集中式管理和控管，提供分散式、分散式資料擁有權的架構架構。

資料最小化

僅收集和處理絕對必要的數據的原則。在中執行資料最小化 AWS 雲端 可降低隱私權風險、成本和分析碳足跡。

資料周長

您 AWS 環境中的一組預防性護欄，可協助確保只有受信任的身分正在存取來自預期網路的受信任資源。若要取得更多資訊，請參閱 [〈在上建立資料周長〉](#) 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。

數據來源

在整個生命週期中追蹤資料來源和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧 (例如分析) 的資料管理系統。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。在上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層加入多個控制項，以協助保護資源。例如，— defense-in-depth 種方法可能會結合多因素驗證、網路分段和加密。

委派的管理員

在中 AWS Organizations，相容的服務可以註冊成 AWS 員帳戶，以管理組織的帳戶並管理該服務的權限。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](#)。

發展價值流映射 (DVSM)

用於識別限制並排定優先順序，對軟體開發生命週期中的速度和品質產生不利影響的程序。DVSM 擴展了最初為精益生產實踐而設計的價值流映射過程。它著重於創造和通過軟件開發過程中移動價值所需的步驟和團隊。

數字雙胞胎

真實世界系統的虛擬表現法，例如建築物、工廠、工業設備或生產線。數位雙胞胎支援預測性維護、遠端監控和生產最佳化。

維度表

在 [star 結構描述](#) 中，較小的資料表包含事實資料表中定量資料的相關資料屬性。維度表格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、篩選和結果集標籤。

災難

防止工作負載或系統在其主要部署位置達成其業務目標的事件。這些事件可能是自然災害、技術故障或人為行為造成的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您使用的策略和程序，將因[災難](#)造成的停機時間和資料遺失降到最低。如需詳細資訊，請參閱 AWS Well-Architected [的架構中的雲端中的工作負載的災難復原](#) [AWS：雲端復原](#)。

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。如需如何使用網域導向設計搭配絞死程式圖案的詳細資訊，請參閱[現代化舊版 Microsoft .ASP NET \(ASMX \) 通過使用容器和 Amazon 網API關逐步增量的 Web 服務](#)。

博士

請參閱[災難復原](#)。

漂移檢測

追蹤基線組態的偏差。例如，您可以用 AWS CloudFormation 來[偵測系統資源中的漂移](#)，也可以用 AWS Control Tower 來[偵測 landing zone 中可能會影響法規遵循治理要求的變更](#)。

DVSM

請參閱[開發價值流映射](#)。

E

EDA

請參閱[探索性資料分析](#)。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與[雲計算](#)相比，邊緣計算可以減少通信延遲並縮短響應時間。

加密

一種計算過程，將純文本數據（這是人類可讀的）轉換為密文。

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 (VPC) 中託管以與其他使用者共用的服務。您可以建立端點服務，AWS PrivateLink 並將權限授與其他 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端點私下連線到您的 VPC 端點服務。如需詳細資訊，請參閱 Amazon 虛擬私有雲端 ([Amazon VPC](#)) 文件中的[建立端點服務](#)。

企業資源規劃 (ERP)

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

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 安全史詩包括身分識別和存取管理、偵探控制、基礎架構安全性、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通過計算摘要統計和創建數據可視化來執行。

F

事實表

[星型架構](#)中的中央表格。它存儲有關業務運營的定量數據。事實資料表通常包含兩種類型的資料欄：包含計量的資料欄，以及包含維度表格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減少開發生命週期的理念。這是敏捷方法的關鍵組成部分。

故障隔離邊界

在中 AWS 雲端，可用區域、AWS 區域控制平面或資料平面等界限，可限制故障影響並協助改善工作負載的彈性。如需詳細資訊，請參閱[AWS 錯誤隔離邊界](#)。

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。這通常表示為可以通過各種技術計算的數值得分，例如 Shapley 加法解釋 (SHAP) 和集成漸變。如需詳細資訊，請參閱[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。

FGAC

請參閱[精細的存取控制](#)。

精細的存取控制 () FGAC

使用多個條件來允許或拒絕訪問請求。

閃切遷移

一種資料庫移轉方法，透過[變更資料擷取使用連續資料](#)複寫，在最短的時間內移轉資料，而不是使用階段化方法。目標是將停機時間降至最低。

G

地理阻塞

請參閱[地理限制](#)。

地理限制 (地理封鎖)

在 Amazon 中 CloudFront，防止特定國家/地區的使用者存取內容分發的選項。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 工作流程被認為是遺留的，[基於主幹的工作流程是現代的首選方法](#)。

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

有助於跨組織單位控管資源、原則和合規性的高階規則 (OUs)。預防性防護機制會強制執行政策，以確保符合合規標準。它們是透過使用服務控制原則和IAM權限界限來實作。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。它們是通過使用 AWS Config，Amazon AWS Security Hub GuardDuty，AWS Trusted Advisor亞馬遜檢查 Amazon Inspector 和自定義 AWS Lambda 檢查來實現的。

H

公頃

查看[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, 無需干預。HA 系統的設計可自動容錯移轉、持續提供高品質的效能, 以及處理不同的負載和故障, 並將效能影響降到最低。

歷史學家現代化

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。歷史學家是一種類型的數據庫, 用於收集和存儲工廠中的各種來源的數據。

異質資料庫遷移

將您的來源資料庫遷移到共用相同資料庫引擎的目標資料庫 (例如, Microsoft SQL 伺服器至 Amazon RDS 伺服器版SQL伺服器)。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。

熱數據

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的儲存層或類別, 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, 修補程式通常是在典型的 DevOps 發行工作流程之外進行。

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。

IaC

查看[基礎結構即程式碼](#)。

身分型政策

附加至一或多個IAM主參與者的原則, 可定義其在 AWS 雲端環境中的權限。

閒置應用程式

在 90 天內，平均記憶 CPU 體使用量介於 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](#)。

不可變基礎設施

為生產工作負載部署新基礎結構的模型，而不是更新、修補或修改現有基礎結構。[不可變的基礎架構本質上比可變基礎架構更加一致、可靠且可預測](#)。如需詳細資訊，請參閱 Well-Architected 的架構中的[使用不可變基礎結構 AWS 構進行部署最佳作法](#)。

入境 (入口) VPC

在 AWS 多帳戶架構中，可接 VPC 受、檢查和路由來自應用程式外部的網路連線。[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您 VPCs 的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

[Klaus Schwab](#) 於 2016 年推出的一個術語，指的是透過連線能力、即時資料、自動化、分析和 AI/ML 的進步來實現製造流程的現代化。

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 VPC 管理 VPCs (相同或不同 AWS 區域)、Internet 和內部部署網絡之間的網絡流量檢查。[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您的 VPCs 的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[機器學習模型可解釋性 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。

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。如需將雲端作業與 ITSM 工具整合的相關資訊，請參閱[作業整合指南](#)。

ITIL

請參閱[IT 資訊庫](#)。

ITSM

請參閱[IT 服務管理](#)。

L

基於標籤的訪問控制 () LBAC

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派了一個安全性標籤值。使用者安全性標籤與資料安全性標籤之間的交集決定了使用者可以看到哪些列與欄。

登陸區域

landing zone 是一個架構良好的多帳戶 AWS 環境，具有可擴展性和安全性。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](#)。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱以[標示為基礎的存取控制](#)。

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，請參閱文件IAM中的[套用最低權限權限](#)。

隨即轉移

見 [7 盧比](#)

小端序系統

首先儲存最低有效位元組的系統。另請參閱 [「位元順序」](#)。

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

旨在危及計算機安全性或隱私的軟件。惡意軟件可能會破壞計算機系統，洩漏敏感信息或獲得未經授權的訪問。惡意軟體的例子包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、間諜軟體和鍵盤記錄程式。

受管理服務

AWS 服務用於 AWS 操作基礎架構層、作業系統和平台，並且您可以存取端點以儲存和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也被稱為抽象的服務。

製造執行系統 (MES)

用於跟踪，監控，記錄和控制生產過程的軟件系統，可在現場將原材料轉換為成品。

MAP

請參閱 [Migration Acceleration Program](#)。

機制

一個完整的過程，您可以在其中創建工具，推動工具的採用，然後檢查結果以進行調整。機制是一個循環，它加強和改善自己，因為它運行。如需詳細資訊，請參閱 AWS Well-Architected 的架構中 [建置機制](#)。

成員帳戶

屬於 AWS 帳戶中組織的管理帳戶以外的所有帳戶 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](#)。

郵件佇列遙測傳輸 (MQTT)

[以發佈/訂閱模式為基礎的輕量型 machine-to-machine \(M2M\) 通訊協定，適用於資源受限 IoT 裝置。](#)

微服務

一個小型的獨立服務，通過明確定義的溝通 APIs，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 AWS 無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。這些微服務通過使用輕量級通過明確定義的接口進行通信。APIs 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 [上 AWS 的實作微服務](#)。

Migration Acceleration Program (MAP)

提供諮詢支援、訓練和服務的 AWS 計畫，協助組織為移轉至雲端建立穩固的營運基礎，並協助抵消移轉的初始成本。MAP 包含用於以有條理的方式執行舊版移轉的移轉方法，以及一組可自動化和加速常見移轉案例的工具。

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。移轉工廠團隊通常包括營運、業務分析師和擁有者、移轉工程師、開發人員和 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。移轉中繼資料的範例包括目標子網路、安全性群組和 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：EC2 使用 AWS 用應用程式遷移服務將遷移重新託管至 Amazon。

移轉組合評估 (MPA)

這是一種線上工具，可提供驗證要移轉至的商業案例的 AWS 雲端資訊。MPA 提供詳細的產品組合評估 (伺服器適當大小、定價、TCO 比較、移轉成本分析) 以及移轉規劃 (應用程式資料分析與資料收集、應用程式分組、移轉優先順序，以及波浪規劃)。所有 AWS 顧問和 APN 合作夥伴顧問均可免費使用該 [MPA 工具](#) (需要登錄)。

移轉準備程度評估 (MRA)

取得有關組織雲端準備狀態的深入解析、識別優勢和弱點，以及建立行動計劃以縮小已識別差距的程序，使用 AWS CAF。如需詳細資訊，請參閱 [遷移準備程度指南](#)。MRA 是 [AWS 移轉策略](#) 的第一階段。

遷移策略

將工作負載移轉至 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 [7 Rs](#) 項目，並參閱 [動員您的組織以加速大規模移轉](#)。

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[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[評估應用程式的現代化準備程度 AWS 雲端](#)。

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[移轉組合評估](#)。

MQTT

請參閱[佇列遙測傳輸](#)的郵件。

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？」

可變的基礎

更新和修改生產工作負載現有基礎結構的模型。為了提高一致性，可靠性和可預測性，AWS Well-Architected 框架建議使用[不可變的基礎結構](#)作為最佳實踐。

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[作業整合](#)。

OLA

請參閱[作業層級協定](#)。

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 提供了具有數據加密，身份驗證和授權方案的互操作性標準。

作業層級協定 () OLA

一份協議，闡明哪些功能 IT 群組承諾互相交付，以支援服務等級協議 () SLA。

操作準備審查 (ORR)

問題和相關最佳做法的檢查清單，可協助您瞭解、評估、預防或減少事件和可能的故障範圍。如需詳細資訊，請參閱 AWS Well-Architected 的架構中的[作業準備檢閱 \(ORR\)](#)。

操作技術

可與實體環境搭配使用的硬體和軟體系統，以控制工業作業、設備和基礎設施。在製造業中，整合 OT 和資訊技術 (IT) 系統是[工業 4.0](#) 轉型的關鍵焦點。

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

由建立的追蹤 AWS CloudTrail 記錄中組織 AWS 帳戶 中所有人的所有事件 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文件中的為組織建立追蹤](#)。

組織變革管理 (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革，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 移轉策略中，這個架構稱為人員加速，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](#)。

原點存取控制 (OAC)

在中 CloudFront，限制存取權限以保護 Amazon Simple Storage Service (Amazon S3) 內容的增強選項。OAC支援所有 S3 儲存貯體 AWS 區域、伺服器端加密 AWS KMS (SSE-KMS)，以及 S3 儲存貯體的動態PUT和DELETE請求。

原點存取識別 (OAI)

在中 CloudFront，用於限制存取以保護 Amazon S3 內容的選項。使用時OAI，CloudFront 會建立 Amazon S3 可用來進行驗證的主體。經驗證的主體只能透過特定散發存取 S3 儲存 CloudFront 貯體中的內容。另請參閱 [OAC](#)，其中提供更精細且增強的存取控制。

ORR

請參閱[作業整備檢閱](#)。

OT

請參閱[操作技術](#)。

出站 (出口) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動的網路連線。VPC[AWS 安全參考架構](#)建議您設定您的網路帳戶與輸入、輸出和檢查，以保護您VPCs的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

附加至IAM主參與者的IAM管理原則，可設定使用者或角色可擁有的最大權限。如需詳細資訊，請參閱IAM文件中的[權限界限](#)。

個人身份信息 (PII)

直接查看或與其他相關數據配對時，可用於合理推斷個人身份的信息。PII包括姓名、地址和聯絡資訊的範例。

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[可編程邏輯控制器](#)

PLM

請參閱[產品生命週期管理](#)

政策

可以定義權限 (請參閱以[身分識別為基礎的策略](#))、指定存取條件 (請參閱以[資源為基礎的策略](#)) 或定義組織中所有帳戶的最大權限的物件 AWS Organizations (請參閱[服務控制策略](#))。

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，通常位於子WHERE句中。

謂詞下推

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。這樣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 AWS 可執行動作和存取資源的實體。此實體通常是IAM角色或使用 AWS 帳戶者的根使用者。如需詳細資訊，請參閱IAM文件中[角色術語與概念](#)中的主參與者。

隱私設計

一種系統工程方法，在整個工程過程中將隱私權納入考量。

私有託管區域

一種容器，其中包含有關您希望 Amazon Route 53 如何回應一或多VPCs個網域內網域及其子網域的DNS查詢的相關資訊。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

一種[安全控制項](#)，旨在防止部署不符合規範的資源。這些控制項會在資源佈建之前進行掃描。如果資源不符合控制項，則不會佈建該資源。如需詳細資訊，請參閱 AWS Control Tower 文件中的[控制項參考指南](#)，並參閱實作安全性[控制中的主動](#)控制 AWS。

產品生命週期管理 (PLM)

在產品的整個生命週期中管理資料和流程，從設計、開發、上市到成長與成熟度，再到下降和移除。

生產環境

請參閱[環境](#)。

可編程邏輯控制器 (PLC)

在製造業中，一台高度可靠且適應性強的計算機，可監控機器並自動化製造過程。

化名化

以預留位置值取代資料集中的個人識別碼的程序。假名化可以幫助保護個人隱私。假名化數據仍被認為是個人數據。

發布/訂閱 (發布/訂閱)

一種模式，可在微服務之間實現非同步通訊，以提高延展性和回應能力 例如，在以微服務為基礎的微服務中 [MES](#)，微服務可以將事件訊息發佈到其他微服務可訂閱的通道。系統可以在不變更發佈服務的情況下新增微服務。

Q

查詢計劃

一系列步驟，如指令，用來存取關聯式資料SQL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

見[負責任，負責，諮詢，通知 \(\) RACI](#)。

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

見[負責任，負責，諮詢，通知 \(\) RACI](#)。

RCAC

請參閱[列與欄存取控制](#)。

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。

重新建築師

見 [7 盧比](#)

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這決定了最後一個恢復點和服務中斷之間可接受的數據丟失。

恢復時間目標 (RTO)

服務中斷與恢復服務之間的最大可接受延遲。

重構

見 [7 盧比](#)

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 是隔離和獨立於其他的，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 您的帳戶可以使用的項目](#)。

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。

重新主持

見 [7 盧比](#)

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

見 [7 盧比](#)

再平台

見 [7 盧比](#)

買回

見 [7 盧比](#)

彈性

應用程式抵抗或從中斷中復原的能力。在規劃備援時，[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 復原力](#)。

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，通知 () 矩陣 RACI

定義移轉活動和雲端作業所涉及之所有各方的角色與責任的矩陣。矩陣名稱衍生自矩陣中定義的責任型別：負責 (R)、負責 (A)、諮詢 (C) 及通知 (I)。支撐 (S) 類型是可選的。如果包括支持，則該矩陣稱為RASCI矩陣，如果將其排除，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

見 [7 盧比](#)

退休

見 [7 盧比](#)

旋轉

定期更新[密碼](#)以使攻擊者更難以存取認證的程序。

列與欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性SQL運算式。RCAC由列權限和欄遮罩組成。

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

SAML2.0

許多身份提供者 (IdPs) 使用的開放標準。此功能可啟用同盟單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 作業，而不必 IAM 為組織中的每個人建立使用者。如需有關 SAML 2.0 型聯合的詳細資訊，請參閱說明文件中的[關於 SAML 以 2.0 為基礎的 IAM 聯合](#)。

SCADA

請參閱[監督控制和資料擷取](#)。

SCP

請參閱[服務控制策略](#)。

秘密

您以加密形式儲存的機密或受限制資訊，例如密碼或使用者認證。AWS Secrets Manager 它由秘密值及其中繼資料組成。密碼值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱「[Secrets Manager 碼中有什麼內容？](#)」在 Secrets Manager 文檔中。

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。安全性控制有四種主要類型：[預防性](#)、[偵測](#)、[回應式](#)和[主動式](#)。

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。

安全信息和事件管理 (SIEM) 系統

結合安全性資訊管理 (SIM) 與安全性事件管理 (SEM) 系統的工具與服務。SIEM 系統收集、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

預先定義且程式化的動作，其設計用來自動回應或修復安全性事件。這些自動化作業可做為[偵探](#)或[回應式](#)安全控制項，協助您實作 AWS 安全性最佳實務。自動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

在其目的地的數據加密，通 AWS 服務 過接收它。

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 定義護欄或設定管理員可委派給使用者或角色的動作限制。您可以用 SCPs 作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 [服務控制原則](#)。

服務端點

URL 的進入點的 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](#)。

服務等級協議 () 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。

服務等級指示器 () SLI

對服務效能層面的測量，例如錯誤率、可用性或輸送量。

服務層級目標 () SLO

代表服務狀況的目標測量結果，由 [服務層次指示器](#) 測量。

共同責任模式

描述您在雲端安全性和合規方面共享的責任的模型。AWS 負責雲端的安全性，而您則負責雲端的安全性。如需詳細資訊，請參閱 [共同責任模式](#)。

SIEM

請參閱 [安全性資訊和事件管理系統](#)。

單點故障 (SPOF)

應用程式的單一重要元件發生故障，可能會中斷系統。

SLA

請參閱 [服務等級協議](#)。

SLI

請參閱 [服務層級指示器](#)。

SLO

請參閱 [服務等級目標](#)。

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[中的應用程式現代化的階段化方法](#)。AWS 雲端

SPOF

請參閱[單一故障點](#)。

星型綱要

使用一個大型事實資料表來儲存交易或測量資料，並使用一或多個較小的維度表格來儲存資料屬性的資料庫組織結構。這種結構是專為在[數據倉庫](#)中使用或用於商業智能目的。

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[現代化舊版 Microsoft ASP.NET \(ASMX \) 通過使用容器和 Amazon 網API關逐步增量的 Web 服務](#)。

子網

您的VPC. 子網必須位於單一可用區域。

監督控制與資料擷取 () SCADA

在製造業中，使用硬體與軟體來監控實體資產與生產作業的系統。

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

以模擬使用者互動以偵測潛在問題或監控效能的方式測試系統。您可以使用 [Amazon CloudWatch Synthetics](#) 來創建這些測試。

T

標籤

作為組織 AWS 資源的中繼資料的索引鍵值配對。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

可用來互連VPCs與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[傳輸閘道是什麼](#)。

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

授與權限給您指定的服務，以代表您在組織內 AWS Organizations 及其帳戶中執行工作。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 AWS Organizations 文件中的[AWS Organizations 與其他 AWS 服務搭配使用](#)。

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

一個小 DevOps 團隊，你可以餵兩個比薩餅。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。

無差別的任務

也稱為繁重工作，是創建和操作應用程序所必需的工作，但不能為最終用戶提供直接價值或提供競爭優勢。無差異化作業的範例包括採購、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凝視

兩者之間的連線VPCs，可讓您使用私有 IP 位址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的[什麼是對VPC等互連](#)。

漏洞

會危及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。

溫暖的數據

不常存取的資料。查詢此類資料時，通常可以接受中度緩慢的查詢。

視窗功能

一種SQL函數，可對以某種方式與目前記錄相關的一組資料列執行計算。視窗函數對於處理工作非常有用，例如計算移動平均值或根據目前列的相對位置存取列的值。

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

看到 [寫一次，多讀](#)。

WQF

請參閱 [AWS工作負載限定架構](#)

寫一次，多讀 (WORM)

一種儲存模型，可單次寫入資料並防止資料遭到刪除或修改。授權用戶可以根據需要多次讀取數據，但無法更改數據。這種數據存儲基礎設施被認為是 [不可變](#) 的。

Z

零日漏洞利用

一種利用 [零時差漏洞](#) 的攻擊，通常是惡意軟件。

零時差漏洞

生產系統中未緩解的瑕疵或弱點。威脅參與者可以利用這種類型的漏洞攻擊系統。由於攻擊，開發人員經常意識到該漏洞。

殭屍應用程式

具有平均CPU且記憶體使用率低於 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。