



AWS 啟動安全性基準 (AWS SSB)

AWS 規定指引



AWS 規定指引: AWS 啟動安全性基準 (AWS SSB)

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，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

Table of Contents

簡介	1
目標對象	1
基礎架構和安全責任	2
保護您的帳戶	3
ACCT.01 – 設定帳戶層級聯絡人	3
ACCT.02 – 限制根使用者的使用	4
ACCT.03 – 設定主控台存取權	4
ACCT.04 – 指派許可	6
ACCT.05 – 需要 MFA	6
ACCT.06 – 強制執行密碼政策	7
ACCT.07 – 日誌事件	8
ACCT.08 – 防止公開存取私有 S3 儲存貯體	9
ACCT.09 – 刪除未使用的資源	9
ACCT.10 – 監控成本	10
11 — 啟用 GuardDuty	10
ACCT.12 – 監控高風險問題	11
保護工作負載	12
WKLD.01 – 將 IAM 角色用於許可	12
WKLD.02 – 使用資源型政策	13
WKLD.03 – 使用暫時性機密或機密管理服務	14
WKLD.04 – 保護應用程式機密	15
WKLD.05 – 偵測並修復暴露的機密	15
WKLD.06 – 使用 Systems Manager 而不是 SSH 或 RDP	16
WKLD.07 – 記錄選定 S3 儲存貯體的資料事件	16
WKLD.08 – 加密 Amazon EBS 磁碟區	17
WKLD.09 – 加密 Amazon RDS 資料庫	17
WKLD.10 – 將私有資源部署在私有子網路中	18
WKLD.11 – 使用安全群組限制存取	18
WKLD.12 – 使用 VPC 端點存取服務	19
WWKLD.13 – 所有公有網路端點都需要 HTTPS	20
WKLD.14 – 對公有端點使用邊緣保護服務	21
WKLD.15 – 使用範本部署安全控制	22
貢獻者	23
文件歷史記錄	24

詞彙表	25
#	25
A	25
B	28
C	29
D	32
E	35
F	37
G	38
H	39
I	40
L	42
M	42
O	46
P	48
Q	50
R	50
S	53
T	56
U	57
V	57
W	58
Z	59
.....	ix

AWS Startup Security Baseline (AWS SSB)

Jay Michael , Amazon Web Services (AWS)

2023 年 5 月 ([文件歷史記錄](#))

AWS Startup Security Baseline (SSB) 是一組控制，為企業在 AWS 上安全建置奠定了最低基礎，而不會降低敏捷性。這些控制構成了安全狀態的基礎，重點是保護憑證、啟用日誌記錄和可見性、管理聯絡資訊以及實作基本資料界限。

本指南中的控制在設計時考慮了早期新創公司，無需付出大量精力即可減輕最常見的安全風險。許多新創公司在 AWS 雲端以單一 AWS 帳戶開始其旅程。隨著組織的發展，其會遷移至多帳戶架構。本指南中的指引是針對單一帳戶架構設計的，但它可以協助您設定安全控制，以便在您轉移至多帳戶架構時輕鬆遷移或修改。

AWS SSB 中的控制分為以下兩個類別：帳戶和工作負載。帳戶控制有助於保持您的 AWS 帳戶安全。其中包括有關設定使用者存取、政策和許可的建議，還包括有關如何監控您的帳戶是否存在未經授權或潛在惡意活動的建議。工作負載控制有助於保護雲端中的資源和程式碼，例如應用程式、後端程序和資料。其中包括加密和縮小存取範圍等建議。

Note

本指南中建議的一些控制會取代初始設定期間設定的預設值，而大多數控制會設定新的設定和政策。本文件不應視為涵蓋了所有可用的控制。

目標對象

本指南最適合處於發展初期、人員和營運最少的新創公司。

處於營運和成長後期的新創公司或其他企業仍然可以透過根據目前實務審核這些控制來獲得重要的價值。如果您識別任何差距，可以實作本指南中的各個控制，然後評估其是否適合作為長期解決方案。

Note

本指南中建議的控制本質上是基礎性的。新創公司或其他處於規模或成熟階段的公司應酌情新增額外的控制。

基礎架構和安全責任

[AWS Well-Architected](#) 可協助雲端架構師針對應用程式和工作負載建置安全、高效能、具彈性且有效率的基礎設施。AWS Startup Security Baseline 與 AWS Well-Architected Framework 的[安全支柱](#)保持一致。安全支柱描述如何利用雲端技術來保護資料、系統和資產，從而改善您的安全狀態。這可協助您遵循目前 AWS 建議來滿足您的業務和合規要求。

您可以使用 AWS 帳戶中的 [AWS Well-Architected Tool](#) 來評估您對良好架構的最佳實務的遵守情況。

安全和合規是 AWS 與客戶之間共同責任。[共同責任模型](#)通常這樣描述：AWS 負責雲端的安全 (即保護執行 AWS 雲端中提供的所有服務的基礎設施)，而您負責雲端中的安全 (如由您選取的 AWS 雲端服務決定)。在共同責任模型中，實作本文件中的安全控制是您作為客戶的責任的一部分。

保護您的帳戶

本節中的控制項和建議有助於確保 AWS 帳戶安全。它強調使用 AWS Identity and Access Management (IAM) 用戶，用戶組和角色 (也稱為主體) 進行人類和機器訪問，限制 root 用戶的使用，並需要多因素身份驗證。在本節中，您確認 AWS 擁有必要的聯絡資訊，以便與您聯絡，以瞭解您的帳戶活動和狀態。您還可以設置監控服務，例如 AWS Trusted Advisor Amazon 和 GuardDuty AWS Budgets，以便在帳戶中收到活動的通知，並且在活動未經授權或意外時可以快速響應。

本節包含下列主題：

- [ACCT.01 – 將帳戶層級聯絡人設定為有效的電子郵件通訊群組清單](#)
- [ACCT.02 – 限制根使用者的使用](#)
- [ACCT.03 – 為每個使用者設定主控台存取權](#)
- [ACCT.04 – 指派許可](#)
- [ACCT.05 – 需要多重重要素驗證 \(MFA\) 才能登入](#)
- [ACCT.06 – 強制執行密碼政策](#)
- [ACT.07 — 將 CloudTrail 日誌交付到受保護的 S3 存儲桶](#)
- [ACCT.08 – 防止公開存取私有 S3 儲存貯體](#)
- [ACCT.09 – 刪除未使用的 VPC、子網路及安全群組](#)
- [ACT.10 — 配置 AWS Budgets 以監控您的支出](#)
- [ACT.11 — 啟用和回應通知 GuardDuty](#)
- [ACCT.12 – 使用 Trusted Advisor 監控並解決高風險問題](#)

ACCT.01 – 將帳戶層級聯絡人設定為有效的電子郵件通訊群組清單

為您的 AWS 帳戶設定主要和備用聯絡人時，請使用電子郵件通訊群組清單，而非個人的電子郵件地址。使用電子郵件通訊群組清單可確保在組織中的個人進出時保留擁有權和連線能力。設置帳單，操作和安全通知的備用聯繫人，並相應地使用適當的電子郵件分發列表。AWS 使用這些電子郵件地址與您聯繫，因此您保留對它們的訪問權限非常重要。

編輯您的帳戶名稱、根使用者密碼或根使用者電子郵件地址

1. 登入帳單和成本管理主控台內的帳戶設定頁面 (<https://console.aws.amazon.com/billing/home?#/account>)。
2. 在帳戶設定頁面的帳戶設定旁，選擇編輯。

3. 在您要更新的欄位旁，選擇編輯。
4. 輸入完變更後，選擇儲存變更。
5. 完成所有變更後，選擇完成。

若要編輯您的聯絡資訊

1. 在[帳戶設定](#)頁面的聯絡資訊下，選擇編輯。
2. 對於要變更的欄位，輸入更新資訊，然後選擇更新。

若要新增、更新或移除替代聯絡人

1. 在[帳戶設定](#)頁面的替代聯絡人下，選擇編輯。
2. 對於要變更的欄位，輸入更新資訊，然後選擇更新。

ACCT.02 – 限制根使用者的使用

root 使用者是在您註冊 AWS 帳戶時建立的，而且此使用者對帳戶具有無法變更的完整擁有權和權限。僅將根使用者用於需要它的特定任務。如需詳細資訊，請參閱[需要根使用者憑證的任務](#) (AWS Account Management)。使用其他類型的 IAM 身分 (例如具有 IAM 角色的聯合身分使用者) 在您的帳戶中執行所有其他動作。如需詳細資訊，請參閱[AWS 安全憑證](#) (IAM 文件)。

限制根使用者的使用

1. 需要對根使用者進行多重要素驗證 (MFA)，如[ACCT.05 – 需要多重要素驗證 \(MFA\) 才能登入](#) 所述。
2. 建立管理使用者，讓您可以不使用根使用者處理日常任務。如需有關設定使用者存取的詳細資訊，請參閱[ACCT.03 – 為每個使用者設定主控台存取權](#)。

ACCT.03 – 為每個使用者設定主控台存取權

最佳作法是 AWS 建議使用臨時登入資料來授 AWS 帳戶與資源的存取權限。暫時憑證的生命週期有限，因此當不再需要時，您不需要將其進行輪換或明確予以撤銷。如需詳細資訊，請參閱[暫時安全憑證](#) (IAM 文件)。

對於人類使用者，AWS 建議使用集中式身分識別提供者 (IdP) 的同盟身分識別，例如 Okta AWS IAM Identity Center、作用中目錄或 Ping 身分識別。同盟使用者可讓您在單一集中位置定義身分識別，而

使用者可以安全地對多個應用程式和網站進行驗證 AWS，包括僅使用一組認證。如需詳細資訊，請參閱[中的聯合身分識別 AWS](#)和[IAM 身分中心](#) (AWS 網站)。

Note

聯合身分可能會使從單帳戶架構至多帳戶架構的轉換變得複雜。新創公司通常會延遲實作聯合身分，直到建立了在 AWS Organizations 中管理的多帳戶架構。

設定聯合身分

1. 如果您使用的是 IAM Identity Center，請參閱[入門](#) (IAM Identity Center 文件)。如果您使用的是外部或第三方 IdP，請參閱[建立 IAM 身分提供者](#) (IAM 文件)。
2. 確保您的 IdP 強制執行多重要素驗證 (MFA)。
3. 根據 [ACCT.04 – 指派許可](#) 套用許可。

對於尚未準備好設定聯合身分的新創公司，您可以直接在 IAM 中建立使用者。這不是建議的安全最佳實務，因此這是永不過期的長期憑證。但是，這是新創公司在早期營運中的常見實務，以防止在營運就緒後難以轉換至多帳戶架構。

作為基準，您可以為每個需要存取 AWS Management Console 的人員建立 IAM 使用者。如果您設定 IAM 使用者，請勿在使用者之間共用憑證，並定期輪換長期憑證。

Warning

IAM 使用者擁有長期登入資料，這會帶來安全風險。為了減輕此風險，我們建議您僅向這些使用者提供執行工作所需的權限，並在不再需要這些使用者時移除這些使用者。

建立 IAM 使用者

1. [建立 IAM 使用者](#) (IAM 文件)。
2. 根據 [ACCT.04 – 指派許可](#) 套用許可。

ACCT.04 – 指派許可

透過將政策指派給 IAM 身分 (使用者群組或角色) 來設定帳戶中的使用者許可。您可以自訂權限，也可以附加[AWS 受管理的原則](#)，這些原則是為許多常見使用案例 AWS 提供權限而設計的獨立原則。如果您自訂許可，請遵循[授予最低權限](#)的安全最佳實務。最低權限是授予每個使用者執行任務所需的最基本的一組許可的實務。

如果您使用的是聯合身分，使用者透過外部身分提供者擔任 IAM 角色來存取帳戶。IAM 角色定義了組織 IdP 驗證的使用者可由哪些使用者中 AWS 執行。您可以將自訂或 AWS 受管理的原則套用至此角色，以設定權限。

指派聯合身分的許可

- 如果您使用的是 IAM Identity Center，請參閱[使用許可集中的 IAM 政策](#) (IAM Identity Center 文件)。

如果您使用的是外部或第三方 IdP，請參閱[新增 IAM 身分許可](#) (IAM 文件)。

如果您使用的是 IAM 使用者，則可以使用使用者群組或角色來管理多個 IAM 使用者的許可。我們建議新創公司使用使用者群組，因為他們更易於管理，並且不太容易出現可能為您的帳戶帶來安全風險的錯誤組態。根據使用者的工作職能將使用者指派給使用者群組。使用者群組的範例包括應用程式、資料、網路和開發作業 (DevOps) 工程師。您也可以根據決策權將使用者類型劃分為更小的使用者群組，例如資深或非資深工程師。

指派 IAM 使用者的許可

- [建立 IAM 使用者群組](#) (IAM 文件)。
- [將受 AWS 管政策附加到 IAM 使用者群組](#) (IAM 文件)。

ACCT.05 – 需要多重要素驗證 (MFA) 才能登入

使用 MFA，使用者便可擁有一個裝置，針對身分驗證查問產生回應。擁有每位使用者的憑證及裝置產生的回應，才能完成登入程序。安全性最佳做法是啟用 MFA 以進行 AWS 帳戶存取，特別是針對長期登入資料，例如帳戶根使用者和 IAM 使用者。

為根使用者設定 MFA

- 登錄到 AWS Management Console 在<https://console.aws.amazon.com/>。

2. 在導覽列右側，選擇您的帳戶名稱，然後選擇我的安全憑證。
3. 如有需要，選擇繼續至安全憑證。
4. 展開多重要素驗證 (MFA) 區段。
5. 選擇啟用 MFA。
6. 遵循精靈指示相應地設定您的 MFA 裝置。如需詳細資訊，請參閱[在 AWS 中為使用者啟用 MFA 裝置](#) (IAM 文件)。

在 IAM Identity Center 中設定 MFA

- [啟用 MFA](#) (IAM Identity Center 文件)

為您自己的 IAM 使用者設定 MFA

1. 使用您的登入憑證，在 <https://console.aws.amazon.com/iam> 登入 IAM 主控台。
2. 在右上方的導覽列中，選擇您的使用者名稱，然後選擇我的安全憑證。
3. 在 AWS IAM 憑證標籤上，在多重要素驗證中，選擇管理 MFA 裝置。

為其他 IAM 使用者設定 MFA

1. 登入 AWS Management Console 並開啟 IAM 主控台，位於<https://console.aws.amazon.com/iam>。
2. 在導覽窗格中，選擇使用者。
3. 選擇要為其啟用 MFA 的使用者名稱，然後選擇 Security credentials (安全憑證) 索引標籤。
4. 在指派的 MFA 裝置旁，選擇管理。
5. 遵循精靈指示相應地設定您的 MFA 裝置。如需詳細資訊，請參閱[在 AWS 中為使用者啟用 MFA 裝置](#) (IAM 文件)。

ACCT.06 – 強制執行密碼政策

使用者 AWS Management Console 透過提供登入認證來登入，建議使用 MFA。要求密碼遵守強式密碼政策，以協助防止透過暴力破解或社會工程進行探索。

如需有關強式密碼的最新建議的詳細資訊，請參閱 Center for Internet Security (CIS) 網站上的[密碼政策指南](#)。

對於 IAM 使用者，您可以在自訂 IAM 密碼政策中設定密碼要求。如需詳細資訊，請參閱[設定帳戶密碼政策](#) (IAM 文件)。

建立自訂密碼政策

1. 登入 AWS Management Console 並開啟 IAM 主控台，位於<https://console.aws.amazon.com/iam>。
2. 在導覽窗格中，選擇帳戶設定。
3. 在密碼政策區段中，選擇變更密碼政策。
4. 選取要套用至密碼政策的選項，然後選擇儲存變更。

ACT.07 — 將 CloudTrail 日誌交付到受保護的 S3 存儲桶

您 AWS 帳戶中使用者、角色和服務所執行的動作會記錄為中的事件 AWS CloudTrail。CloudTrail 預設為啟用狀態，在 CloudTrail 主控台中，您可以存取 90 天的事件歷史記錄資訊。若要檢視、搜尋、下載、封存、分析和回應 AWS 基礎結構中的帳戶活動，請參閱[使用事件歷史記錄檢視 CloudTrail 事件](#) (文件)。

若要使用其他資料保留超過 90 天的 CloudTrail 歷史記錄，您可以建立新的追蹤，將日誌檔案交付到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，適用於所有事件類型。在 CloudTrail 主控台中建立追蹤時，您會建立多區域追蹤。

若要建立將所有記錄傳遞 AWS 區域 至 S3 儲存貯體的追蹤

1. [創建一個跟踪](#) (CloudTrail 文檔)。在選擇日誌事件頁面上，執行下列動作：
 - a. 對於 API 活動，同時選擇讀取和寫入。
 - b. 對於預生產環境，選擇排除 AWS KMS 事件。這會排除您追蹤中的所有 AWS Key Management Service (AWS KMS) 事件。AWS KMS 讀取動作 (例如EncryptDecrypt、和GenerateDataKey 可以產生大量的事件。

對於生產環境，選擇記錄寫入管理事件，並清除排除 AWS KMS 事件的核取方塊。這會排除大量 AWS KMS 讀取事件，但仍會記錄相關的寫入事件，例如DisableDelete、和ScheduleKey。這些是生產環境的最低建議 AWS KMS 記錄設定。

2. 新的追蹤會出現在追蹤頁面上。大約 15 分鐘後，會 CloudTrail 發佈記錄檔，其中顯示在您帳戶中進行的 AWS 應用程式設計介面 (API) 呼叫。您可以在所指定之 S3 儲存貯體中看到日誌檔案。

協助保護存放 CloudTrail 日誌檔案的 S3 儲存貯體

1. 檢閱 [Amazon S3 儲存貯體政策](#) (CloudTrail 文件)，瞭解存放日誌檔的所有儲存貯體，並視需要進行調整，以移除任何不必要的存取權。
2. 安全最佳實務是務必手動將 `aws:SourceArn` 條件金鑰新增至儲存貯體政策。如需詳細資訊，請參閱 [建立或更新 Amazon S3 儲存貯體以用來存放組織追蹤的日誌檔](#) (CloudTrail 文件)。
3. [啟用 MFA 刪除](#) (Amazon S3 文件)。

ACCT.08 – 防止公開存取私有 S3 儲存貯體

依預設，只有 AWS 帳戶 和 IAM 主體的根使用者 (如果使用) 具有讀取和寫入該主體建立的 Amazon S3 儲存貯體的許可。透過使用身分型政策向其他 IAM 主體授予存取權，並且可以使用儲存貯體政策強制執行存取條件。您可以建立儲存貯體政策，以將一般公開存取權授予儲存貯體 (公有儲存貯體)。

依預設，在 2023 年 4 月 28 日或之後建立的儲存貯體已啟用封鎖公開存取設定。對於在此日期之前建立的儲存貯體，使用者可能會錯誤設定儲存貯體政策並意外向公眾授予存取權。您可以透過為每個儲存貯體啟用封鎖公開存取設定來防止此錯誤組態。如果您目前或 future 沒有公用 S3 儲存貯體的使用案例，請在 AWS 帳戶 層級啟用此設定。此設定可阻止允許公開存取的策略。

防止公開存取 S3 儲存貯體

- [為 S3 儲存貯體設定封鎖公開存取設定](#) (Amazon S3 文件)。

AWS Trusted Advisor 為 S3 儲存貯體產生黃色發現項目，允許對公眾進行清單或讀取存取，並為允許公開上傳或刪除的值區產生紅色發現項目。作為基準，遵循控制 [ACCT.12 – 使用 Trusted Advisor 監控並解決高風險問題](#) 以識別並更正錯誤設定的儲存貯體。Amazon S3 主控台中也會指示可公開存取的 S3 儲存貯體。

ACCT.09 – 刪除未使用的 VPC、子網路及安全群組

為了減少出現安全問題的機會，請刪除或關閉任何未使用的資源。在新 AWS 帳戶中，默認情況下，每個都會自動創建虛擬私有雲 (VPC) AWS 區域，這使您可以在公共子網中分配公共 IP 地址。但是，如果不需要這些 VPC，這會導致資源意外暴露的風險。

如果未使用，請刪除所有區域中的預設 VPC，而不僅僅是您可能部署工作負載的區域中的預設 VPC。刪除 VPC 也會刪除其元件，例如子網路和安全群組。

Note

您可以在 Amazon EC2 全域檢視主控台 (<https://console.aws.amazon.com/ec2globalview/home>) 上檢視所有區域和 VPC。如需詳細資訊，請參閱 [使用 Amazon EC2 全域檢視列出和篩選跨區域的資源](#) (Amazon EC2 文件)。

刪除未使用的預設 VPC

1. [刪除您的 VPC](#) (Amazon VPC 文件)。
2. 視需要對其他區域中的 VPC 重複。

ACT.10 — 配置 AWS Budgets 以監控您的支出

AWS Budgets 可在預測成本超過目標臨界值時通知，監控每月成本和使用情況。預測的成本通知可以提供意外活動的指示，除了其他監控系統（例如 AWS Trusted Advisor 和 Amazon GuardDuty）之外，還提供額外的防禦。監控和了解您的 AWS 成本也是良好操作衛生的一部分。

若要在中設定預算 AWS Budgets

- [建立成本預算](#) (AWS Budgets 文件)。

ACT.11 — 啟用和回應通知 GuardDuty

Amazon GuardDuty 是一種威脅偵測服務，可持續監控惡意或未經授權的行為，以協助保護您的 AWS 帳戶、工作負載和資料。當它偵測到非預期和潛在的惡意活動時，會 GuardDuty 提供詳細的安全性發現資訊，以便能見度 GuardDuty 可偵測威脅，例如加密貨幣挖礦活動、來自 Tor 用戶端和中繼的存取權限、意外行為，以及受損的 IAM 登入資料。啟用 GuardDuty 並回應發現項目，以阻止 AWS 環境中潛在的惡意或未經授權的行為。如需有關中發現項目的詳細資訊 GuardDuty，請參閱 [尋找類型](#) (GuardDuty 說明文件)。

您可以使用 Amazon E CloudWatch vents 在 GuardDuty 建立發現項目或尋找變更時設定自動通知。首先，設定 Amazon Simple Notification Service (Amazon SNS) 主題，並為該主題新增端點或電子郵件地址。然後，為 GuardDuty 發現項目設定 CloudWatch 事件，事件規則會在 Amazon SNS 主題中通知端點。

啟用 GuardDuty 和 GuardDuty 通知

1. [啟用 Amazon GuardDuty](#) (GuardDuty 文檔)。
2. [建立 CloudWatch 事件規則以通知您發 GuardDuty 現項目](#) (GuardDuty文件)。

ACCT.12 – 使用 Trusted Advisor 監控並解決高風險問題

AWS Trusted Advisor 被動掃描您的 AWS 基礎架構是否存在與安全性、效能、成本和可靠性相關的高風險或高影響問題。它提供有關受影響資源和修復建議的詳細資訊。如需檢查和描述的完整清單，請參閱[AWS Trusted Advisor 檢查參考](#) (Trusted Advisor 文件)。

重複複查找 Trusted Advisor 結果，並視需要修正問題。如果您有 AWS 商業 Support 或企業 Support 方案，您可以訂閱每週發現的電子郵件。如需詳細資訊，請參閱[設定通知偏好設定](#) (AWS Support 文件)。

若要檢視中的問題 Trusted Advisor

- 根據檢視檢查類別 ([AWS Support 文件](#)) 中的指示檢閱每個檢查類別。至少，我們建議檢閱建議採取動作問題 (紅色)。

保護工作負載

本節中的控制和建議可協助您在建置工作負載時保護在 AWS 中執行的工作負載。它們會強調管理應用程式機密和存取範圍、最大限度地減少對私有資源的存取路由以及使用加密來保護傳輸中的資料和靜態資料的安全實務。

本節包含下列主題：

- [WKLD.01 – 將 IAM 角色用於運算環境許可](#)
- [WKLD.02 – 使用資源型政策許可限制憑證使用範圍](#)
- [WKLD.03 – 使用暫時性機密或機密管理服務](#)
- [WKLD.04 – 防止應用程式機密暴露](#)
- [WKLD.05 – 偵測並修復暴露的機密](#)
- [WKLD.06 – 使用 Systems Manager 而不是 SSH 或 RDP](#)
- [WKLD.07 – 記錄包含敏感資料的 S3 儲存貯體的資料事件](#)
- [WKLD.08 – 加密 Amazon EBS 磁碟區](#)
- [WKLD.09 – 加密 Amazon RDS 資料庫](#)
- [WKLD.10 – 將私有資源部署到私有子網路](#)
- [WKLD.11 – 使用安全群組限制網路存取](#)
- [WKLD.12 – 使用 VPC 端點存取支援的服務](#)
- [WWKLD.13 – 所有公有網路端點都需要 HTTPS](#)
- [WKLD.14 – 對公有端點使用邊緣保護服務](#)
- [WKLD.15 – 在範本中定義安全控制並使用 CI/CD 實務進行部署](#)

WKLD.01 – 將 IAM 角色用於運算環境許可

在 AWS Identity and Access Management (IAM) 中，角色代表個人或服務在可設定的時段可以擔任的一組許可。使用角色無需儲存或管理長期憑證，從而顯著降低非預期使用的可能性。將 IAM 角色直接指派給 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體、AWS Fargate 任務和服務、AWS Lambda 函數以及其他支援的 AWS 運算服務。使用 AWS SDK 並在這些運算環境中執行的應用程式會自動使用 IAM 角色憑證進行身分驗證。

您可以在服務的 [AWS 文件](#) 中找到針對每個服務使用 IAM 角色的方法和指示。例如，請參閱下列內容：

- [Amazon EC2 的 IAM 角色](#) (Amazon EC2 文件)
- [任務的 IAM 角色](#) (Amazon Elastic Container Service 文件)
- [Lambda 執行角色](#) (Lambda 文件)

WKLD.02 – 使用資源型政策許可限制憑證使用範圍

政策是可以定義許可或指定存取條件的物件。政策主要有以下兩種類型：

- 身分型政策附接至主體並定義主體在 AWS 環境中的許可。
- 資源型政策附接至資源，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體，或虛擬私有雲端 (VPC) 端點。這些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。

為了允許主體存取以對資源執行操作，它必須在身分型政策中授予許可並滿足資源型政策的條件。如需詳細資訊，請參閱[身分型政策和資源型政策](#) (IAM 文件)。

資源型政策的建議條件包括：

- 使用 `aws:PrincipalOrgID` 條件將存取限制為僅限指定組織 (在 AWS Organizations 中定義) 中的主體。
- 分別使用 `aws:SourceVpc` 或 `aws:SourceVpce` 條件限制對源自特定 VPC 或 VPC 端點的流量的存取。
- 使用 `aws:SourceIp` 條件根據來源 IP 地址允許或拒絕流量。

以下是資源型政策範例，此政策使用 `aws:PrincipalOrgID` 條件僅允許 `<o-xxxxxxxxxxx>` 組織中的主體存取 `<bucket-name>` S3 儲存貯體：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFromOrganization",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::<bucket-name>/*",
      "Condition": {
```

```
    "StringEquals": {"aws:PrincipalOrgID": "<o-xxxxxxxxxxxx>"}
  }
}
]
```

WKLD.03 – 使用暫時性機密或機密管理服務

應用程式機密主要由憑證組成，例如金鑰對、存取字符、數位憑證和登入憑證。應用程式使用這些機密來存取它所依賴的其他服務，例如資料庫。為了協助保護這些機密，我們建議其或者是暫時性的 (在請求時產生並且是短期的，例如 IAM 角色)，或者是從機密管理服務中擷取的。這可防止透過不太安全的機制 (例如保留在靜態組態檔案中) 意外暴露。這也可更輕鬆地將應用程式程式碼從開發環境提升至生產環境。

對於機密管理服務，我們建議使用 Parameter Store、AWS Systems Manager 的功能和 AWS Secrets Manager 的組合：

- 使用 Parameter Store 來管理機密和其他參數，這些參數是個別鍵值對、字串型、總長度短且存取頻繁的參數。您可以使用 AWS Key Management Service (AWS KMS) 密鑰來加密機密。將參數儲存在 Parameter Store 的標準層中無需付費。如需有關參數層的詳細資訊，請參閱「管理參數層」(Systems Manager 文件)。
- 使用 Secrets Manager 儲存文件形式的機密 (例如多個相關的金鑰值對)、大於 4 KB 的機密 (例如數位憑證) 或受益於自動輪換的機密。

您可以使用 Parameter Store API 擷取儲存在 Secrets Manager 中的機密。這可讓您在同時使用這兩種服務的組合時，將應用程式中的程式碼標準化。

在 Parameter Store 中管理機密

1. [建立對稱 AWS KMS 金鑰](#) (AWS KMS 文件)。
2. [建立 SecureString 參數](#) (Systems Manager 文件)。Parameter Store 中的機密使用 SecureString 資料類型。
3. 在您的應用程式中，使用適合您的程式設計語言的 AWS SDK 從 Parameter Store 擷取參數。如需 Java 中的範例，請參閱 [GetParameter.java](#) (AWS 程式碼範例目錄)。

在 Secrets Manager 中管理機密

1. [建立機密](#) (Secrets Manager 文件)。

2. [從程式碼中的 AWS Secrets Manager 擷取機密](#) (Secrets Manager 文件)。

請務必閱讀[使用 AWS Secrets Manager 用戶端快取庫提高使用機密的可用性和延遲](#) (AWS 部落格文章)。使用已實作最佳實務的客戶端 SDK 應可以加速並簡化 Secrets Manager 的使用和整合。

WKLD.04 – 防止應用程式機密暴露

在本機開發期間，應用程式機密可能儲存在本機組態或程式碼檔案中，並意外簽入原始程式碼儲存庫。公共服務供應商託管的不安全儲存庫可能會受到未經授權的存取，並隨後發現這些機密。使用可用的工具來防止機密被簽入。將檢查暴露的機密納入為手動程式碼審核程序的一部分。

可以阻止應用程式機密簽入原始程式碼儲存庫的一些常見工具包括：

- [Gitleaks](#) (GitHub 儲存庫)
- [Whispers](#) (GitHub 儲存庫)
- [detect-secrets](#) (GitHub 儲存庫)
- [git-secrets](#) (GitHub 儲存庫)
- [TruffleHog](#) (GitHub 儲存庫)

WKLD.05 – 偵測並修復暴露的機密

在 [WKLD.03 – 使用暫時性機密或機密管理服務](#) 和 [WKLD.04 – 防止應用程式機密暴露](#) 中，您可採取措施來保護機密。在此控制中，部署一個解決方案，可以偵測機密是否繞過了這些預防措施，並且可以相應地進行修復。

Amazon CodeGuru Reviewer 可偵測原始程式碼中的應用程式機密，並提供一個機制在 Secrets Manager 中修復和發佈偵測到的機密。還提供了用於從 Secrets Manager 擷取機密的應用程式程式碼。進行成本效益分析，以確定此解決方案是否適合您的業務。作為替代方案，[WKLD.04 – 防止應用程式機密暴露](#) 中的一些開放原始碼解決方案提供了現有機密的偵測功能。

若要設定 CodeGuru Reviewer 與 Secrets Manager 的整合

- [使用 CodeGuru Reviewer 識別硬式編碼機密並使用 AWS Secrets Manager 進行保護](#) (AWS 部落格文章和引導式逐步解說)。

WKLD.06 – 使用 Systems Manager 而不是 SSH 或 RDP

具有指向網際網路閘道的預設路由的公有子網路本質上比沒有通往網際網路的路由的私有子網路具有更大的安全風險。您可以在私有子網路中執行 EC2 執行個體，並使用 AWS Systems Manager 的 Session Manager 功能透過 AWS Command Line Interface (AWS CLI) 或 AWS Management Console 遠端存取執行個體。然後，您可以使用 AWS CLI 或主控台啟動透過安全通道連接到執行個體的工作階段，從而無需管理用於 Secure Shell (SSH) 或 Windows 遠端桌面協定 (RDP) 的其他憑證。

使用 Session Manager 而不是在公有子網路中執行 EC2 執行個體、執行跳接方塊或執行堡壘主機。

設定 Session Manager

1. 確保 EC2 執行個體使用最新的作業系統 Amazon Machine Image (AMI)，例如 Amazon Linux 2 或 Ubuntu。AWS Systems Manager Agent (SSM Agent) 已預先安裝在 AMI 上。
2. 確保執行個體透過網際網路閘道或 VPC 端點連接至這些地址 (將 **<region>** 取代為適當的 AWS 區域)：
 - a. `Ec2messages.<region>.amazonaws.com`
 - b. `ssm.<region>.amazonaws.com`
 - c. `ssmmessages.<region>.amazonaws.com`
3. 將 AWS 受管政策 `AmazonSSMManagedInstanceCore` 附接至與執行個體關聯的 IAM 角色。

如需詳細資訊，請參閱[設定 Session Manager](#) (Systems Manager 文件)。

啟動工作階段

- [啟動工作階段](#) (Systems Manager 文件)。

WKLD.07 – 記錄包含敏感資料的 S3 儲存貯體的資料事件

依預設，AWS CloudTrail 會擷取管理事件，即在您的帳戶中建立、修改或刪除資源的事件。這些管理事件不會擷取對 Amazon Simple Storage Service 儲存貯體中個別物件的讀取或寫入操作。在安全事件期間，擷取個別記錄或物件層級的未經授權的資料存取或使用非常重要。使用 CloudTrail 記錄儲存敏感或業務關鍵資料的任何 S3 儲存貯體的資料事件，以用於偵測和稽核目的。

Note

記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 [AWS CloudTrail 定價](#)。

記錄追蹤的資料事件

1. 登入 AWS Management Console 並開啟 CloudFront 主控台 (<https://console.aws.amazon.com/cloudtrail/>)
2. 在導覽窗格中，選擇追蹤，然後選擇追蹤名稱。
3. 在一般詳細資訊中，選擇「編輯」以變更下列設定。您無法變更追蹤的名稱。
 - a. 在資料事件中，選擇編輯。
 - b. 對於資料來源，請選擇 S3。
 - c. 對於所有目前和未來的 S3 儲存貯體，清除讀取和寫入。
 - d. 在個別儲存貯體選擇中，瀏覽要記錄資料事件的儲存貯體。您可以在此視窗中選取多個儲存貯體。選擇新增儲存貯體以記錄更多儲存貯體的資料事件。選擇記錄讀取事件 (例如 GetObject)、寫入事件 (例如 PutObject) 還是兩者。
 - e. 選擇更新追蹤。

WKLD.08 – 加密 Amazon EBS 磁碟區

強制加密 Amazon Elastic Block Store (Amazon EBS) 磁碟區作為您 AWS 帳戶中的預設行為。加密磁碟區具有與未加密磁碟區相同的每秒讀寫次數 (IOPS) 效能，並且對延遲的影響最小。這可以防止以後出於合規或其他原因重建磁碟區。如需詳細資訊，請參閱 [必須了解的 Amazon EBS 加密最佳實務](#) (AWS 部落格文章)。

加密 Amazon EBS 磁碟區

- [依預設啟用加密](#) (Amazon EC2 文件)。

WKLD.09 – 加密 Amazon RDS 資料庫

與 [WKLD.08 – 加密 Amazon EBS 磁碟區](#) 類似，啟用加密 Amazon Relational Database Service (Amazon RDS) 資料庫。此加密在基礎磁碟區層級執行，具有與未加密磁碟區相同的 IOPS 效能，且對延遲的影響最小。如需詳細資訊，請參閱 [加密 Amazon RDS 資源的概觀](#) (Amazon RDS 文件)。

加密 RDS 資料庫執行個體

- [加密資料庫執行個體](#) (Amazon RDS 文件)。

WKLD.10 – 將私有資源部署到私有子網路

將不需要直接網際網路存取的資源 (例如 EC2 執行個體、資料庫、佇列、快取或其他基礎設施) 部署到 VPC 私有子網路。私有子網路的路由表中沒有宣告至已附接網際網路閘道的路由，因此無法接收網際網路流量。源自私有子網路、目的地為網際網路的流量必須透過受管 AWS NAT 閘道或在公有子網路中執行 NAT 程序的 EC2 執行個體進行網路位址轉譯 (NAT)。如需有關網路隔離的詳細資訊，請參閱 [Amazon VPC 中的基礎設施安全](#) (Amazon VPC 文件)。

建立私有資源和子網路時，請遵循下列實務：

- 建立私有子網路時，停用自動指派公有 IPv4 地址。
- 建立私有 EC2 執行個體時，停用自動指派公有 IP。如果執行個體透過錯誤組態意外部署到公有子網路，這可以防止指派公有 IP。

需要時，您可以在資源組態過程中指定資源的子網路。您可以使用 [模組化和可擴展 VPC 架構快速入門](#) (AWS 快速入門) 來部署遵循最佳實務的 VPC。

WKLD.11 – 使用安全群組限制網路存取

使用安全群組控制 EC2 執行個體、RDS 資料庫和其他支援資源的流量。安全群組可作為虛擬防火牆，可套用於任何相關資源群組，以一致地定義允許傳入和傳出流量的規則。除了基於 IP 地址和連接埠的規則之外，安全群組還支援允許來自與其他安全群組關聯的資源的流量的規則。例如，資料庫安全群組可以具有僅允許來自應用程式伺服器安全群組的流量的規則。

依預設，安全群組允許所有傳出流量，但不允許傳入流量。您可以移除傳出流量規則，也可以設定新增的其他規則以限制傳出流量並允許傳入流量。如果安全群組沒有傳出規則，將不會允許來自您執行個體的傳出流量。如需詳細資訊，請參閱 [使用安全組控制到資源的流量](#) (Amazon VPC 文件)。

在下列範例中，有三個安全群組控制從 Application Load Balancer 到連接至 Amazon RDS for MySQL 資料庫的 EC2 執行個體的流量。

安全群組	傳入規則	傳出規則
Application Load Balancer 安全群組	<p>描述：允許來自任何地方的 HTTPS 流量</p> <p>類型：HTTPS</p> <p>來源：Anywhere-IPv4 (0.0.0.0/0)</p>	<p>描述：允許來自任何地方的所有流量</p> <p>類型：所有流量</p> <p>目的地：Anywhere-IPv4 (0.0.0.0/0)</p>
EC2 執行個體安全群組	<p>描述：允許來自 Application Load Balancer 的 HTTP 流量</p> <p>類型：HTTP</p> <p>來源：Application Load Balancer 安全群組</p>	<p>描述：允許來自任何地方的所有流量</p> <p>類型：所有流量</p> <p>目的地：Anywhere-IPv4 (0.0.0.0/0)</p>
RDS 資料庫安全群組	<p>描述：允許來自 EC2 執行個體的 MySQL 流量</p> <p>類型：MySQL</p> <p>來源：EC2 執行個體安全群組</p>	無傳出規則

WKLD.12 – 使用 VPC 端點存取支援的服務

在 VPC 中，需要存取 AWS 或其他外部服務的資源需要路由至網際網路 (0.0.0.0/0) 或路由至目標服務的公有 IP 地址。使用 VPC 端點啟用從 VPC 至支援的 AWS 或其他服務的私有 IP 路由，因此無需使用網際網路閘道、NAT 裝置、虛擬私有網路 (VPN) 連線或 AWS Direct Connect 連線。

VPC 端點支援附接政策和安全群組以進一步控制對服務的存取。例如，您可以為 Amazon DynamoDB 撰寫 VPC 端點政策，以僅允許項目層級動作並阻止 VPC 中所有資源的資料表層級動作，無論其本身的許可政策為何。您也可以撰寫 S3 儲存貯體政策以僅允許源自特定 VPC 端點的請求，拒絕所有其他外部存取。VPC 端點還可以具有安全群組規則，例如，限制僅存取與應用程式特定的安全群組關聯的 EC2 執行個體，例如 Web 應用程式的商業邏輯層。

有不同類型的 VPC 端點。您可以使用 VPC 介面端點存取大多數服務。使用閘道端點存取 DynamoDB。Amazon S3 同時支援介面和閘道端點。建議對單一 AWS 帳戶和區域內包含的工作負載

使用閘道端點，無需額外付費。如果需要更多可擴展的存取 (例如從其他 VPC、內部部署網路或不同 AWS 區域存取 S3 儲存貯體)，建議使用介面端點。介面端點需要支付每小時正常執行時間費用和每 GB 資料處理費用，這兩項費用均低於透過 AWS NAT 閘道向 0.0.0.0/0 傳送資料的相應費用。

如需有關使用 VPC 端點的其他資訊，請參閱下列資源：

- 如需有關在 Amazon S3 的閘道與介面端點之間選取的詳細資訊，請參閱 [為 Amazon S3 選擇您的 VPC 端點策略](#) (AWS 部落格文章)。
- [建立介面端點](#) (Amazon VPC 文件)。
- [建立閘道端點](#) (Amazon VPC 文件)。
- 例如，限制對特定 VPC 或 VPC 端點的存取的 S3 儲存貯體政策，請參閱 [限制對特定 VPC 的存取](#) (Amazon S3 文件)。
- 如需限制動作的 DynamoDB 端點政策範例，請參閱 [DynamoDB 的端點政策](#) (Amazon VPC 文件)。

WWKLD.13 – 所有公有網路端點都需要 HTTPS

需要 HTTPS 為您的 Web 端點提供額外的可信度，可讓您的端點使用憑證來證明身分，並確認您的端點與已連線用戶端之間的所有流量均已加密。對於公有網站，這提供了更高的搜尋引擎排名的額外好處。

許多 AWS 服務為您的資源提供了公有 Web 端點，例如 AWS Elastic Beanstalk、Amazon CloudFront、Amazon API Gateway、Elastic Load Balancing 和 AWS Amplify。如需有關如何要求其中每個服務都使用 HTTPS 的指示，請參閱下列內容：

- [Elastic Beanstalk](#) (Elastic Beanstalk 文件)
- [CloudFront](#) (CloudFront 文件)
- [Application Load Balancer](#) (AWS 知識中心)
- [Classic Load Balancer](#) (AWS 知識中心)
- [Amplify](#) (Amplify 文件)

Amazon S3 上託管的靜態網站不支援 HTTPS。若要要求這些網站使用 HTTPS，您可以使用 CloudFront。不需要對透過 CloudFront 提供內容的 S3 儲存貯體進行公開存取。

使用 CloudFront 為 Amazon S3 上託管的靜態網站提供服務

1. [使用 CloudFront 為 Amazon S3 上託管的靜態網站提供服務](#) (AWS 知識中心)。

2. 如果您要設定對公有 S3 儲存貯體的存取，[需要在檢視器與 CloudFront 之間使用 HTTPS](#) (CloudFront 文件)。

如果您要設定對私有 S3 儲存貯體的存取，[使用原始存取身分來限制對 Amazon S3 內容的存取](#) (CloudFront 文件)。

此外，將 HTTPS 端點設定為需要現代 Transport Layer Security (TLS) 協定和加密，除非需要與舊協定相容。例如，使用 ELBSecurityPolicy-FS-1-2-Res-2020-10 或可用於 Application Load Balancer HTTPS 接聽程式的最新政策，而不是預設 ELBSecurityPolicy-2016-08。最新政策至少需要 TLS 1.2、轉送密碼以及與現代 Web 瀏覽器相容的強加密。

如需有關 HTTPS 公有端點的可用安全政策的詳細資訊，請參閱：

- [Classic Load Balancer 適用的預先定義 SSL 安全政策](#) (Elastic Load Balancing 文件)
- [Application Load Balancer 的安全政策](#) (Elastic Load Balancing 文件)
- [檢視器與 CloudFront 之間支援的協定和加密](#) (CloudFront 文件)

WKLD.14 – 對公有端點使用邊緣保護服務

使用邊緣保護服務，而不是直接從 EC2 執行個體或容器等運算服務為流量提供服務。這在來自網際網路的傳入流量與為該流量提供服務的資源之間提供額外的安全層。這些服務可以在流量到達您的內部資源之前篩選不需要的流量、強制加密並套用路由或其他規則 (例如負載平衡)。

可以提供公有端點保護的 AWS 服務包括 AWS WAF、CloudFront、Elastic Load Balancing、API Gateway 和 Amplify Hosting。在公有子網路中執行 VPC 型服務 (例如 Elastic Load Balancing)，作為私有子網路中執行的 Web 服務資源的代理。

CloudFront、API Gateway 和 Amazon Route 53 免費提供對第 3 層和第 4 層分散式拒絕服務 (DDoS) 攻擊的保護，且 AWS WAF 可以防禦第 7 層攻擊。

您可以在此處找到其中每個服務的入門指示：

- [AWS WAF 入門](#) (AWS 網站)
- [Amazon CloudFront 入門](#) (CloudFront 文件)
- [Elastic Load Balancing 入門](#) (Elastic Load Balancing 文件)
- [API Gateway 入門](#) (API Gateway 文件)
- [Amplify Hosting 入門](#) (Amplify 文件)

WKLD.15 – 在範本中定義安全控制並使用 CI/CD 實務進行部署

基礎設施即程式碼 (IaC) 是在使用持續整合與持續交付 (CI/CD) 管道 (與用於部署軟體應用程式的管道相同的管道) 部署的範本和程式碼中定義所有 AWS 服務資源和組態的實務。IaC 服務 (例如 AWS CloudFormation) 同時支援 IAM 身分型和資源型政策，並支援 AWS 安全服務，例如 Amazon GuardDuty、AWS WAF 和 Amazon VPC。擷取這些成品作為 IaC 範本，將範本遞交至原始程式碼儲存庫，然後使用 CI/CD 管道進行部署。

除非另有要求，否則應將應用程式許可政策與應用程式程式碼遞交在相同儲存庫中，並在單獨的程式碼儲存庫和部署管道中管理一般資源政策和安全服務組態。

如需有關 IaC on AWS 入門的詳細資訊，請參閱 [AWS Cloud Development Kit \(AWS CDK\) 入門](#)。

貢獻者

本文件的貢獻者包括：

- Jay Michael，首席解決方案架構師
- Cole Calistra，首席解決方案架構師
- Justin Plock，首席解決方案架構師
- Faisal Farooq，解決方案架構師
- Michael Nguyen，資深解決方案架構師
- Ritik Khatwani，資深解決方案架構師
- Paul Hawkins，資訊安全長 (CISO) 辦公室負責人

特別感謝下列同樣提供指導和審核的人員：

- Robert Put
- Mike Sullivan
- Bob Lee III

文件歷史記錄

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
Amazon S3 儲存貯體設定	我們更新了 ACCT.08 – 防止公開存取私有 S3 儲存貯體 部分，以反映 2023 年 4 月 28 日之後建立的 Amazon S3 儲存貯體預設啟用封鎖公開存取設定。	2023 年 5 月 18 日
IAM 安全最佳實務	我們更新了本指南，以便與最新 AWS Identity and Access Management (IAM) 最佳實務保持一致。如需詳細資訊，請參閱 IAM 文件中的 安全最佳實務 。	2023 年 2 月 1 日
IAM 角色	我們在 WKLD.01 – 將 IAM 角色用於運算環境許可 部分中提供了 AWS 服務 文件的其他連結。	2022 年 9 月 22 日
密碼政策	我們更新了強式密碼的建議，以使用 Center for Internet Security (CIS) 的最新指引。	2022 年 5 月 10 日
初次出版	—	2022 年 4 月 13 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：將您的現場部署 Oracle 資料庫遷移至 Amazon Relational Database Service 服務 (Amazon RDS)，適用於 AWS 雲端中的 Oracle。
- **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：將現場部署 Oracle 資料庫遷移至 AWS 雲端 EC2 執行個體上的 Oracle。
- **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。此移轉案例適用於 VMware Cloud on AWS，支援內部部署環境與之間的虛擬機器 (VM) 相容性和工作負載可攜性 AWS。在將基礎設施遷移至 VMware Cloud on AWS 時，您可以使用內部部署資料中心的 VMware Cloud Foundation 技術。範例：將裝載 Oracle 資料庫的虛擬機器管理程序重新定位至 VMware 雲端。 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](#)。

酸

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

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

AI

請參閱[人工智慧](#)。

艾奧運

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

一種經常使用的解決方案，用於解決方案的生產力適得其反，效果不佳或效果低於替代方案。

應用控制

一種安全性方法，只允許使用已核准的應用程式，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、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 (IAM) 文件 AWS 中的 [ABAC](#)。

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 將指導組織到六個重點領域，稱為觀點：業務，人員，治理，平台，安全性和運營。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 為人員開發、訓練和通訊提供指導，以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 [「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

咖啡

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](#)。

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

組織遷移到 AWS 雲端時通常會經歷的四個階段：

- 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

這些階段是 Stephen Orban 在雲端企業策略部落格文章 [「邁向 AWS 雲端優先的旅程與採用階段」](#) 部落格文章中定義的。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，通常可以接受緩慢的查詢。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

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 YAML 範本，將一致性套件部署為 AWS 帳戶和區域中的單一實體，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。

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

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流程。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](#)。

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端 (VPC) 中託管以與其他使用者共用的服務。您可以使用其他或 (IAM) 主體建立端點服務，AWS PrivateLink 並將權限授予其他 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

自動化並管理企業的關鍵業務流程 (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 安全史詩包括身份和訪問管理，偵探控制，基礎結構安全性，數據保護和事件響應。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[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 (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 許可界限來將其實施。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。

I

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。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，VPC 可接受、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

[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，集中式 VPC 可管理 VPC (相同或不同 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[AWS 的機器學習模型可解釋性](#)。

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

標籤式存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派一個安全性標籤值。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 IAM 文件中的[套用最低權限許可](#)。

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

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 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[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。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：使 AWS 用應用程式遷移服務將遷移重新託管到 Amazon EC2。

遷移組合評定 (MPA)

這是一種線上工具，可提供驗證商業案例以移轉至 AWS 雲端的資訊。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)。所有 AWS 顧問和 APN 合作夥伴顧問均可免費使用[MPA 工具](#) (需要登入)。

遷移準備程度評定 (MRA)

使用 AWS CAF 獲得有關組織雲端準備狀態的見解、識別優勢和弱點，以及建立行動計劃以縮小已識別差距的過程。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

將工作負載移轉至 AWS 雲端時所使用的方法。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 AWS 雲端中應用程式的現代化準備情況](#)。

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

一種模型，用於更新和修改生產工作負載的現有基礎結構。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。

OPCA

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 提供數據加密，身份驗證和授權方案的互操作性標準。

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)。

操作準備程度檢討 (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 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](#)。

原始存取控制 (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。

原始存取身分 (OAI)

在中 CloudFront，用於限制存取以保護 Amazon S3 內容的選項。當您使用 OAI 時，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](#)，它可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](#)。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動的網路連線的 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](#)。

個人識別資訊 (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 的範例包括姓名、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。

公司

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 角色或使用者的根使用者。AWS 帳戶如需詳細資訊，請參閱 IAM 文件中[角色術語和概念](#)中的主體。

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，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

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，如指示，用來存取 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

拉齐矩阵

請參閱[負責任，負責，諮詢，通知 \(RAC I\)](#)。

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。

拉西矩陣

請參閱[負責任，負責，諮詢，通知 \(RAC I\)](#)。

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。

復原時間目標 (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。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

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)，以及通知 (I)。支撐 (S) 類型是可選的。如果您包含支援，則該矩陣稱為 RASCI 矩陣，如果您將其排除，則稱為 R ACI 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。

資料列與資料行存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 運算式。RCAC 由資料列權限和資料行遮罩所組成。

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

許多身份提供者 (IdPs) 使用的開放標準。此功能可啟用聯合單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 作業，而不必為組織中的每個人在 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](#)。

斯卡達

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[秘密管理員說明文件](#)中的秘密。

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。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[服務控制原則](#)。

服務端點

的進入點的 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。

服務等級目標 (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 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](#)。

暹

請參閱[安全性資訊和事件管理系統](#)。

單點故障 (SPF)

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

痙攣

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 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

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，可對以某種方式與當前記錄相關的一組行執行計算。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。

蠕蟲

看到[寫一次，多讀](#)。

WQF

請參閱[AWS 工作負載鑑定架構](#)。

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

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

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。