適用於應用程式擁有者的日誌記錄和監控指南

AWS 規定指引

AWS 規定指引: 適用於應用程式擁有者的日誌記錄和監控指南

Table of Contents

適用於應用程式擁有者的日誌記錄和監控指南

John Buckley，Amazon Web Services (AWS)

2023 年 1 月 (文件歷史記錄)

工作負載是可提供商業價值的資源和程式碼集合，例如客戶面向的應用程式或後端程序。工作負載可能由單一 AWS 帳戶 中的資源子集組成，也可能跨越多個 AWS 帳戶。在雲端中，應用程式是一種工作負載。它可能專門部署在雲端環境中，也可能受到本機內部部署硬體的支援。許多出版物著重於日誌記錄和監控雲端基礎設施，並且面向安全團隊。本指南面向應用程式擁有者，重點介紹 AWS 雲端 中記錄和監控應用程式的有效且高效的方法。

本指南可協助您在適當的層級設定日誌記錄和監控，以便您可以快速識別異常並做出回應。它還可協助您確保您的應用程式日誌支援對任何問題的詳細分析和解決方法。

雖然本指南針對 AWS 雲端 部署編寫，但您可以將這些原則套用於在內部部署或其他雲端供應商基礎設施上執行的應用程式。

目標業務成果

閱讀本指南後，您應能夠了解：

- 應用程式通常記錄的事件類型
- 您應考慮記錄的事件屬性 (例如人物、事件和時間)
- 您應考慮從日誌中排除的資料類型，例如可能危及您的安全狀態或個人身分識別資訊的資料
- 如何在適當的層級為您的應用程式設定日誌記錄和監控
- 誰應能夠管理和存取您的應用程式日誌
- 您可以設定用於監控和記錄 AWS 雲端 中的應用程式的 AWS 服務 和功能
- 如何使用應用程式和 AWS 服務 及功能中的日誌資料來分類問題和診斷問題

關於應用程式的日誌記錄和監控

日誌記錄、監控、提醒和報告是不同的安全程序，這些程序協同工作以提供應用程式運作狀態和效能的可見性。建立並維護應用程式的動作和事件的詳細記錄至關重要，以便您可以根據記錄的活動進行監控、提醒和報告。

應用程式日誌記錄是收集應用程式產生的事件並將其記錄在一個或多個日誌檔案中的程序。此事件歷史記錄可以協助您執行安全和效能分析、追蹤資源變更以及對應用程式問題進行疑難排解。

應用程式監控是評估應用程式的整體效能和運作狀態的程序。您應能夠持續監控應用程式的前端和後端。由於雲端上託管的應用程式高度分散，因此日誌記錄和監控工具可以協助您快速對效能問題進行疑難排解或即時識別和修復安全威脅。日誌資料是監控的關鍵輸入。

可觀測性與監控類似，但它引入了使用不同參數測量應用程式行為的方法，並且允許複雜的關聯。例如，測量特定地理區域中的一組使用者在特定日期的 HTTP 成功率。如需詳細資訊，請參閱監控和可觀測性 (AWS 行銷)。

最終，應用程式擁有者的目標是維護安全、運作狀態良好的應用程式以及這些應用程式的積極使用者體驗。透過實作日誌記錄和監控，您的開發人員和營運團隊可以更快地規劃應用程式問題並進行疑難排解。

每個應用程式所需的日誌記錄和監控層級各不相同。可能會影響監控和日誌記錄層級的因素包括組織政策和程序、應用程式帶來的安全風險層級、應用程式對業務營運的重要性以及應用程式管理的資料的敏感度。一般來說，公共或面向客戶的應用程式比組織內部使用的應用程式需要更高層級的監控和日誌記錄。本指南包括一般資訊和建議，您應根據應用程式的要求自訂您的方法。

> **Note**
>
> 您組織中的標準或程序可能會強制要求特定的日誌記錄和監控屬性。例如，將使用者許可傳遞到企業權利審核系統。請確保您的日誌記錄和監控計畫符合您組織的要求。

AWS 雲端 中的應用程式的日誌記錄

對於 AWS 雲端 中的日誌記錄應用程式，檢閱常見事件類型、事件屬性和最佳實務。

本節包含下列主題：

事件類型

建立應用程式日誌記錄策略時最重要的考量事項之一是決定要記錄的事件和動作。雖然您的組織和應用程式的要求可能會影響此決策，但我們建議您永遠記錄下列內容 (如果其適用於您的應用程式)：

- 輸入驗證失敗 – 範例包括協定違規、不可接受的編碼以及無效的參數名稱和值。
- 輸出驗證失敗 – 範例包括資料庫記錄集不相符和無效的資料編碼。
- 身分驗證成功和失敗 – 記錄身分驗證活動，但不記錄使用者名稱和密碼。由於使用者可能會意外地將密碼鍵入到使用者名欄位中，因此我們建議您不要記錄使用者名稱。這可能會無意中暴露憑證並導致授權存取。對包含身分驗證資料的任何日誌實作安全控制。
- 授權 (存取控制) 失敗 – 對於相關授權系統，記錄失敗的存取嘗試。您可以監控此日誌資料，以了解可能指出應用程式中的授權系統存在攻擊或問題的模式。
- 工作階段管理失敗 – 範例包括修改工作階段 Cookie 或字符。應用程式通常使用 Cookie 或字符來管理使用者狀態。惡意使用者可以嘗試修改 Cookie 值以取得未經授權的存取。記錄被篡改的工作階段字符提供了一種偵測此行為的方法。
- 應用程式錯誤和系統事件 – 範例包括語法和執行期錯誤、連線問題、效能問題、來自第三方服務的錯誤訊息、檔案系統錯誤、檔案上傳的病毒偵測和組態變更。
- 應用程式狀態 – 啟動或停止應用程式及其相關資源。
- 日誌記錄狀態 – 啟動、停止或暫停日誌記錄。
- 使用風險較高的功能 – 範例包括網路連線變更、新增或刪除使用者、變更權限、為使用者指派字符、新增或刪除字符、使用系統管理權限、由應用程式管理員存取、具有管理權限的使用者執行的所有動作、存取支付持卡人資料、使用資料加密金鑰、變更加密金鑰、建立和刪除系統層級物件、提交使用者產生的內容 (尤其是檔案上傳)，以及匯入和匯出資料 (包括報告)。
- 法律和其他選擇加入 – 範例包括行動電話功能的許可、使用條款、條款和條件、個人資料使用同意以及接收行銷通訊的許可。

除了建議的屬性之外，對於您的應用程式，請考慮哪些其他屬性可以為監控、提醒和報告提供有用的資料。範例包括：

- 定序失敗
- 協助您評估違反組織可接受使用政策的使用者行為的屬性
- 資料變更
- 遵守標準或法規所需的屬性，例如防止金融犯罪、限制股權交易或收集健康或其他個人資訊。
- 協助您識別可疑或意外行為的屬性，例如嘗試執行未經授權的動作
- 組態變更
- 應用程式程式碼檔案或記憶體變更

事件屬性

每個日誌項目都需要包含足夠詳細的資訊以進行監控和分析。您可以記錄完整的內容資料，但記錄摘錄或摘要屬性會更有效。應用程式日誌必須記錄每個事件的時間、位置、使用者、內容及影響。其中的屬性會有所不同，具體取決於架構、應用程式類別以及主機系統或裝置。

記錄日期和時間戳記時，使用國際標準時間 (UTC) 以及 ISO 8601 (ISO 網站) 中國際認可的日期和時間格式。

> **Note**
>
> 請考慮使用網路時間同步服務來協助確保準確的時間戳記。Amazon 提供 Amazon Time Sync Service，許多 AWS 服務 都在使用此服務，包括 Amazon Elastic Compute Cloud (Amazon EC2)。Amazon Time Sync Service 在每個 AWS 區域 中使用一組與衛星連線的原子參考時鐘，透過網路時間協定 (NTP) 提供對 UTC 全球標準的最新精準時間讀數。如需詳細資訊，請參閱使用 Amazon Time Sync Service 確保時間 (AWS 部落格文章)。

下列事件屬性通常包含在日誌中。

屬性類別	事件屬性	描述
當	記錄日期和時間	記錄事件新增至日誌的日期和時間。

	事件日期和時間	記錄事件發生的日期和時間。這可能與日誌記錄不同，例如，由於用戶端應用程式託管在定期或間歇性處於線上狀態的遠端裝置上而導致日誌記錄延遲。
	事件識別符	記錄使用者名稱、帳號或其他唯一屬性，以確保永遠可以識別事件。
位置	應用程式識別符	記錄應用程式名稱和版本。
	應用程式地址	記錄叢集或主機名稱、伺服器 IPv4 或 IPv6 位址、連接埠號碼、工作站身分和本機裝置識別符。
	服務	記錄服務名稱和協定。
	GeoLocation	記錄使用者的地理位置。
	視窗、表單或頁面	記錄進入點 URL、Web 應用程式的 HTTP 方法或執行動作的對話方塊名稱。
	程式碼位置	記錄指令碼或模組名稱。
使用者 (人類或機器使用者)	來源地址	記錄使用者的裝置識別符、IP 地址、行動或無線射頻 (RF) 塔樓 ID 或行動電話號碼。
	使用者身分	如果使用者已通過身分驗證或以其他方式已知，則記錄使用者資料庫表主索引鍵值、使用者名稱或授權編號。

	使用者類型分類	記錄使用者類型，例如公有、經過身分驗證、CMS、搜尋引擎、授權滲透測試人員或正常執行時間監控。如需有關執行時間監控的詳細資訊，請參閱本指南中的 注意事項和排除。
	請求 HTTP 標頭或 HTTP 使用者代理程式	(僅限 Web 應用程式) 記錄 HTTP 請求標頭資訊，包括 HTTP 使用者代理程式字串，因為這些值會影響用戶端傳送至伺服器的資訊。
內容	事件類型	記錄事件是提供資訊、警告還是錯誤。
	事件嚴重性	將事件嚴重性分類，例如高、中和低。
	安全事件旗標	如果日誌包含與安全事件無關的資料，請為與安全相關的事件建立旗標以協助您進行識別。
	事件描述	(選用) 包括事件的簡短描述。
	動作或意圖	記錄請求的原始預期用途，例如登入、重新整理工作階段 ID、登出或更新設定檔。
	使用者或應用程式回應	記錄使用者或應用程式對事件的回應，例如狀態碼、自訂文字訊息、停止工作階段或管理員提醒。
	結果狀態	記錄動作是否成功，例如成功、失敗或延遲。

	結果原因	記錄狀態發生的原因。例如，登入請求可能會失敗，因為使用者未在資料庫中進行身分驗證。
	延伸詳細資訊	記錄與事件關聯的任何其他資訊，例如堆疊追蹤、系統錯誤訊息、偵錯資訊和 HTTP 請求內文。
	HTTP 回應狀態碼	(僅限 Web 應用程式) 記錄傳回給使用者的 HTTP 回應狀態碼，例如 200 或 301。如需詳細資訊，請參閱本指南中的 日誌記錄層級。
影響	影響的資源	記錄針對哪些資源採取行動。
	物件	記錄受影響的元件或其他物件，例如使用者帳戶、資料資源、檔案、URL 或工作階段 ID。
	資源名稱	記錄受影響資源的名稱。
	資源標籤	記錄指派給受影響資源的標籤。如需有關標籤的詳細資訊，請參閱標記 AWS 資源 (AWS 一般參考)。
其他	分析可信度	記錄日誌服務對事件偵測的可信度，例如指派低、中或高評分或數值。
	內部分類	記錄標準或合規遵守的任何內部分類。

外部分類	記錄標準或合規遵守的任何外部分類，例如 NIST 安全內容自動化協定 (SCAP)。

記錄最佳實務

日誌記錄層級

請注意不要記錄過多的資料量。日誌應擷取有用且可操作的資料。過多的日誌記錄會對效能產生負面影響，且還會增加日誌記錄儲存和處理成本。過多的日誌記錄也可能會導致問題和安全事件未偵測到。

記錄 HTTP 回應狀態碼可能會產生大量日誌記錄資料，尤其是 200 層級 (成功) 和 300 層級 (重新導向) 狀態碼。我們建議您考慮僅記錄 400 層級 (用戶端錯誤) 和 500 層級 (伺服器端錯誤) 狀態碼。

應用程式日誌記錄架構提供不同層級的日誌記錄，例如資訊、偵錯或錯誤。對於開發環境，您可能要使用詳細日誌記錄 (例如包括資訊和偵錯)，以協助您的開發人員。但是，我們建議您對生產環境停用資訊和偵錯層級，因為這些層級可能會產生過多的日誌記錄資料。

注意事項和排除

- 確保您記錄的資料符合法律規定，特別是在您的組織營運所在的司法管轄區內。
- 請勿排除來自已知使用者 (例如其他內部系統)、受信任的第三方、搜尋引擎機器人、正常執行時間或程序監控以及其他遠端監控系統的任何事件。但是，您可以在記錄的資料中包含每個旗標的分類旗標。請考慮應用程式產生的日誌檔案可能會被未授權檢視應用程式處理的任何敏感資料的各方 (例如第三方日誌監控解決方案或外部服務供應商) 使用。
- 下列屬性不應直接記錄在日誌中。移除、遮罩、清理、雜湊或加密下列項目：
  - 應用程式原始程式碼
  - 工作階段識別值 (如果需要追蹤工作階段特定的事件，請考慮將其取代為雜湊值)
  - 存取權杖
  - 敏感個人資料和某些形式的個人身分識別資訊 (PII)，例如健康資訊或政府頒發的身分證明
  - 身分驗證密碼
  - 資料庫連線字串
  - 加密金鑰和其他主要密碼
  - 銀行帳戶或支付卡持有人資料
  - 允許存儲比日誌記錄系統更高的安全分類資料

- 商業敏感資訊
- 在相關司法管轄區內收集的非法資訊
- 使用者已選擇退出或未明確同意收集的資訊
- 同意收集的資訊已過期

特殊資料類型

有時，下列資料也可以記錄在日誌中。雖然它可以用於調查和疑難排解用途，但它可能會洩露有關系統的敏感資訊。在記錄事件之前，您可能需要匿名化、雜湊或加密這些資料類型：

- 檔案路徑
- 內部網路名稱和地址
- 非敏感個人資料，例如個人姓名、電話號碼和電子郵件地址

如果日誌中不需要個人的真實身分或認為風險太大，請使用資料匿名化。

存取和變更管理

- 非管理使用者不應具有停用事件日誌記錄的許可，尤其是滿足合規要求所需的事件日誌記錄。
- 只有管理使用者才應具有暫停或停止日誌記錄服務或修改組態的許可。
- 如果您的日誌記錄服務具有日誌檔案完整性驗證功能，請將其啟用。這有助於您偵測日誌檔案的修改，刪除或偽造。如需有關 AWS 服務 中此功能的詳細資訊，請參閱本指南中的 使用 CloudTrail。
- 日誌記錄變更必須是應用程式固有的 (例如應用程式根據已核准的演算法自動進行的變更)，或遵循已核准的變更管理程序 (例如當您變更組態資料或修改原始程式碼時)。

AWS 服務 用於記錄日誌和監控

本指南重點介紹 AWS 雲端 中部署的日誌記錄和監控應用程式。您可以使用 AWS 服務 來實作您的日誌記錄和監控計畫，也可以用其來增強您目前的解決方案。例如，如果您正在對應用程式的問題進行疑難排解，您可以：

- 使用 Amazon Virtual Private Cloud (Amazon VPC) 中的 VPC 流程日誌功能對應用程式日誌進行分類，並檢視與問題對應的網路流量。
- 使用 AWS CloudTrail 檢視與問題事件時間對應的 API 呼叫。
- 檢閱 Amazon CloudWatch Logs 中的日誌，以檢查與問題事件時間對應的 CPU 峰值。

您可以部署下列 AWS 服務 和功能來記錄和監控您的應用程式：

- AWS CloudTrail 透過記錄使用者、角色或 AWS 服務 所採取的動作來協助您稽核 AWS 帳戶 的控管、合規和營運風險。如需有關使用此服務記錄或監控應用程式事件的詳細資訊，請參閱本指南中的 CloudTrail。
- Amazon CloudWatch 可協助您分析日誌，並即時監控 AWS 資源和託管應用程式的指標。您也可以使用 ServiceLens 功能來監控應用程式的運作狀態，或使用 Synthetics 功能來建立監控端點和 API 的 Canary。如需有關使用此服務監控應用程式的詳細資訊，請參閱本指南中的 CloudWatch。
- Amazon CloudWatch Logs 可協助您集中所有系統、應用程式和 AWS 服務 的日誌，以便您可以對其進行監控並安全地進行封存。如需有關使用此服務記錄應用程式事件的詳細資訊，請參閱本指南中的 CloudWatch Logs。
- Amazon Virtual Private Cloud (Amazon VPC) 的 VPC 流程日誌功能可協助您擷取有關傳入及傳出您 VPC 中網路介面的 IP 流量的資訊。如需有關使用此服務記錄應用程式事件的詳細資訊，請參閱本指南中的 VPC 流量日誌。
- AWS X-Ray 可收集有關您的應用程式處理的請求的資料，並可協助您檢視和篩選該資料以獲取深入見解，從而識別問題與優化的機會。如需有關使用此服務監控應用程式的詳細資訊，請參閱本指南中的 X-Ray。

使用 AWS CloudTrail 進行應用程式日誌記錄和監控

AWS CloudTrail 是一種 AWS 服務，可協助您啟用 AWS 帳戶 的營運和風險稽核、控管和合規。使用者、角色或 AWS 服務 所執行的動作會在 CloudTrail 中記錄為事件。事件可以包含在 AWS Management Console、AWS Command Line Interface (AWS CLI) 以及 AWS SDK 和 API 中採取的動作。

使用 CloudTrail

當您建立帳戶時，系統即會在 AWS 帳戶 中啟用 CloudTrail。AWS 帳戶 中發生活動時，該活動會記錄在 CloudTrail 事件中。您可以在 CloudTrail 主控台中前往事件歷史記錄輕鬆地檢視最近事件。

若要持續記錄 AWS 帳戶 中的活動和事件，請建立追蹤。您可以為單一 AWS 區域 或所有區域建立追蹤。追蹤可記錄每個區域中的日誌檔案，CloudTrail 可以將日誌檔案交付至單一合併的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

您可以分別設定多筆追蹤，以便追蹤只處理和記錄您指定的事件。當您想要將 AWS 帳戶 中發生的事件與應用程式中發生的事件進行分類時，這可能很有用。

> **Note**
>
> CloudTrail 具有驗證功能，您可以使用此功能確定日誌檔案在 CloudTrail 交付後是否已修改、已刪除或保持不變。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這可透過運算方式防止修改、刪除或偽造 CloudTrail 日誌檔案，而無需偵測。您可以使用 AWS CLI 驗證 CloudTrail 交付檔案之位置中的檔案。如需有關此功能以及如何啟用它的詳細資訊，請參閱驗證 CloudTrail 日誌檔案完整性 (CloudTrail 文件)。

CloudTrail 的使用案例

- 合規協助 – 使用 CloudTrail 可以透過提供您 AWS 帳戶 中的事件歷史記錄來協助您遵守內部政策和法規標準。
- 安全分析 – 您可以透過將 CloudTrail 日誌檔案擷取到日誌管理和分析解決方案 (例如 CloudWatch Logs、Amazon EventBridge、Amazon Athena、Amazon OpenSearch Service 或其他第三方解決方案) 來執行安全分析並偵測使用者行為模式。
- 資料外洩 – 您可以透過 CloudTrail 中記錄的物件層級 API 事件收集 Amazon S3 物件上的活動資料來偵測資料外洩。收集活動資料後，您可以使用其他 AWS 服務 (例如 EventBridge 和 AWS Lambda) 來觸發自動回應。
- 操作問題疑難排解 – 您可以使用 CloudTrail 日誌檔案對操作問題進行疑難排解。例如，您可以快速識別對環境中的資源所做的最新變更，包括建立、修改和刪除 AWS 資源。

CloudTrail 的最佳實務

- 在所有 AWS 區域 中啟用 CloudTrail。
- 啟用日誌檔案完整性驗證。
- 加密日誌。
- 將 CloudTrail 日誌檔案擷取到 CloudWatch Logs。
- 集中所有 AWS 帳戶 和區域的日誌。
- 將生命週期政策套用至包含日誌檔案的 S3 儲存貯體。
- 防止使用者關閉 CloudTrail 中的日誌記錄。在 AWS Organizations 中套用下列服務控制政策 (SCP)。此 SCP 為整個組織內的 `StopLogging` 和 `DeleteTrail` 動作設定了明確的拒絕規則。

```
{
"Version": "2012-10-17",
"Statement":
       [
                 { "Action":
                     [
                     "cloudtrail:StopLogging",
                     "cloudtrail:DeleteTrail"
                      ],
                      "Resource": "*",
                      "Effect": "Deny"
                  }
        ]
}
```

使用 Amazon CloudWatch 進行應用程式日誌記錄和監控

Amazon CloudWatch 會即時監控您的 AWS 資源，以及您在 AWS 上執行的應用程式。您可以使用 CloudWatch 收集和追蹤指標，這些是您可以為您的資源和應用程式測量的變數。

使用 CloudWatch

CloudWatch 本質上是指標儲存庫。AWS 服務 (例如 Amazon EC2) 可讓您將指標放到儲存庫，並根據這些指標擷取統計資料。如果您將自己的自訂指標放到儲存庫，也可以對這些指標擷取統計資料。如需詳細資訊，請參閱使用 CloudWatch 指標 (CloudWatch 文件)。

您也可以設定警示，它會自動代表您啟動動作。警示會監看指定時段內的單一指標，並根據隨著時間與閾值相對的指標值來執行一或多個指定動作。例如，警示可以將通知傳送至 Amazon Simple Notification Service (Amazon SNS) 主題。您也可以將警示新增至儀表板。如需詳細資訊，請參閱使用 CloudWatch 警示 (CloudWatch 文件)。

CloudWatch 主控台會自動顯示您使用的每個 AWS 服務 的相關指標。您可以建立其他自訂儀表板來顯示應用程式的指標和警示。如需詳細資訊，請參閱使用 CloudWatch 儀表板 (CloudWatch 文件)。

CloudWatch 自動支援跨區域功能。您不需要執行任何額外的步驟，就能在同一個圖形或儀表板上顯示單一帳戶中來自不同 AWS 區域 的指標。您可以透過實作跨帳戶可觀測性來實現跨帳戶功能 (CloudWatch 文件)。

如需有關使用 CloudWatch 記錄和監控 AWS 雲端 中工作負載的詳細資訊和詳細指引，請參閱使用 Amazon CloudWatch 設計和實作日誌記錄和監控 (AWS 規格指南)。

CloudWatch 的使用案例

- 應用程式運作狀態監控 – CloudWatch ServiceLens 可讓您將追蹤、指標、日誌、警示和其他資源運作狀態資訊整合到同一個位置，來增強您服務和應用程式的可觀測性。ServiceLens 可將 CloudWatch 與 AWS X-Ray 整合以提供應用程式的端對端檢視，有助您更有效率地找出效能瓶頸，並識別受影響的使用者。如需詳細資訊，請參閱使用 ServiceLens 監控應用程式的運作狀態 (CloudWatch 文件)。
- 綜合監控 – 您可以使用 CloudWatch Synthetics 建立 Canary (依排程執行的可設定指令碼)，來監控端點和 API。Canary 遵循相同的路由並執行與客戶相同的動作，即使您的應用程式沒有任何客戶流量，也能持續驗證您的客戶體驗。Canary 會檢查端點的可用性和延遲，並可儲存 UI 的載入時間資料和螢幕擷取畫面。它們會監控您的 REST API、URL 和網站內容，並且可以檢查來自網路釣魚、程式碼注入和跨網站指令碼的未經授權變更。如需詳細資訊，請參閱使用綜合監控 (CloudWatch 文件)。
- 使用者監控 – 使用 CloudWatch RUM，您可以執行實際使用者監控，以收集和檢視有關 Web 應用程式效能的用戶端資料。資料包括頁面載入時間、用戶端錯誤和使用者行為。您可以使用收集到的資料對用戶端效能問題進行快速識別和偵錯。如需詳細資訊，請參閱使用 CloudWatch RUM (CloudWatch 文件)。
- 異常行為偵測 – 當您為指標啟用異常偵測時，CloudWatch 會套用統計和機器學習演算法。這些演算法會持續分析系統和應用程式的指標、判斷正常基準以及表面異常情況。如需詳細資訊，請參閱使用 CloudWatch 異常偵測 (CloudWatch 文件)。
- 功能驗證和 A/B 實驗 – 您可以使用 Amazon CloudWatch Evidently 在推出功能時，將新功能提供給指定百分比的使用者，以安全地驗證新功能。您也可以執行 A/B 實驗，根據證據和資料作出功能設

計決策。如需詳細資訊，請參閱使用 CloudWatch Evidently 執行啟動和 A/B 實驗 (CloudWatch 文件)。

使用 Amazon CloudWatch Logs 進行應用程式日誌記錄和監控

Amazon CloudWatch Logs 可將您使用的所有系統、應用程式和 AWS 服務 中的日誌，集中在可高度擴展的單一服務中。然後，您可以輕鬆檢視日誌、在日誌中搜尋特定的錯誤碼或模式、根據特定欄位篩選日誌，或安全封存日誌以供日後分析。您可以將您的所有日誌事件 (無論其來源為何) 視為依時間排序的單一且一致的事件流程。您可以對其進行查詢並對其進行排序、依特定欄位進行分組、建立自訂計算以及在儀表板中視覺化日誌資料。

使用 CloudWatch Logs

在 CloudWatch Logs 中，日誌事件會組織到日誌串流和日誌群組。日誌串流是一系列共用相同來源的日誌事件。更具體地說，日誌串流通常旨在表示來自正在監視的應用程式執行個體或被監控的資源。日誌群組定義了共用相同保留、監控和存取控制設定的一或多個日誌串流。每個日誌串流都必須屬於至少一個日誌群組。如需詳細資訊，請參閱使用日誌群組和日誌串流 (CloudWatch Logs 文件)。

您可以使用 CloudWatch Logs Insights 搜尋和分析 Amazon CloudWatch Logs 中的日誌資料。您可以執行查詢，協助您有效率地回應操作問題。如果發生問題，您可以使用 CloudWatch Logs 來識別可能的原因並驗證已部署的修正。如需詳細資訊，請參閱使用 CloudWatch Logs Insights 分析日誌資料 (CloudWatch Logs 文件)。

您可以建立一個或多個指標篩選條件，以搜尋並篩選進入 CloudWatch Logs 的日誌資料。指標篩選條件可定義要在傳送至 CloudWatch Logs 的日誌資料中尋找的詞彙和模式。CloudWatch Logs 使用這些指標篩選條件將日誌資料轉換為數值 CloudWatch 指標，供您繪製圖形或設定警示。如需詳細資訊，請參閱使用篩選條件從日誌事件建立指標 (CloudWatch Logs 文件)。

CloudWatch Logs 的使用案例

- 監控 CloudTrail 日誌 - 您可以在 CloudWatch 中建立警示，並接收 CloudTrail 所擷取特定 API 活動的通知，然後使用此通知執行疑難排解。如需詳細資訊，請參閱將 CloudTrail 事件傳送至 CloudWatch Logs (CloudTrail 文件)。
- 記錄 AWS API 呼叫 – 如果您具有第三方監控解決方案，可以使用 CloudWatch Logs 記錄 AWS API 呼叫。您可設定第三方監控服務來評估此日誌和應用程式層級 API。
- 設定日誌保留 – 依預設，CloudWatch Logs 中的日誌將無限期保留且永遠不會過期。您可以調整每個日誌群組的保留政策，維持無限期保留，或選擇保留期間為 1 天至 10 年。

- 封存和儲存日誌 - 您可以使用 CloudWatch Logs 將日誌資料儲存在高耐用性儲存中。CloudWatch Logs 代理程式可將輪換和非輪換的日誌資料傳送到日誌服務。然後，您可以在需要時存取原始日誌資料。

使用 VPC 流程日誌進行應用程式日誌記錄和監控

VPC 流程日誌是 Amazon Virtual Private Cloud (Amazon VPC) 的一項功能，可協助您擷取有關傳入及傳出您 VPC 中網路介面的 IP 流量的資訊。

使用 VPC 流程日誌

您可以為虛擬私有雲端 (VPC)、子網路或網路介面建立流量日誌。如果建立子網或 VPC 的流量日誌，則會監控該子網或 VPC 中的每個網路介面。如需詳細資訊，請參閱使用流程日誌 (Amazon VPC 文件)。

受監控網路介面的流程日誌資料記錄為流程日誌記錄。流程日誌記錄代表您 VPC 中的網路流程。依預設，每筆記錄都會擷取出現在彙總間隔內的網路 IP 流量。每筆記錄都是包含欄位的字串，其中欄位會由空格分隔。記錄包含 IP 流程不同元件的值，例如來源、目標和通訊協定。建立流量日誌時，您可以使用流量日誌記錄的預設格式，或指定自訂格式。如需詳細資訊，請參閱流程日誌記錄範例 (Amazon VPC 文件)。

流程日誌不會擷取下列資訊：

- 由執行個體在與 Amazon 網域名稱系統 (DNS) 伺服器聯絡時產生的流量。若您使用您自己的 DNS 伺服器，則會記錄所有流向該 DNS 伺服器的流量。
- 由 Windows 執行個體針對 Amazon Windows 授權啟用所產生的流量。
- 針對執行個體中繼資料，流入及流出 `254.169.254` 的流量。
- 針對 Amazon Time Sync Service，流入及流出 `254.169.123` 的流量。
- 動態主機組態協定 (DHCP) 流量。
- 流入預設 VPC 路由器預留 IP 地址的流量。
- 端點網路介面和 Network Load Balancer 網路介面之間的流量。

流程日誌資料可以發佈至數個 AWS 服務，包括 Amazon CloudWatch Logs。建立流程日誌之後，您可以在您設定的日誌群組中擷取和檢視 CloudWatch Logs 中的流程日誌記錄。如需詳細資訊，請參閱將流程日誌發佈至 CloudWatch Logs (Amazon VPC 文件)。

流量日誌資料是在網路流量路徑之外收集，因此不會影響網路輸送量或延遲。您可以建立或刪除流量日誌，而不會影響網路效能。

VPC 流程日誌的使用案例

- 診斷過於嚴苛的安全群組規則
- 監控進入應用程式執行個體的流量
- 確定流量的方向

使用 AWS X-Ray 進行應用程式日誌記錄和監控

AWS X-Ray 可收集有關您的應用程式處理的請求的資料，並可協助您檢視和篩選該資料以獲取深入見解，從而識別問題與優化的機會。

使用 X-Ray

AWS X-Ray 從您的應用程式接收追蹤，如果其與 X-Ray 整合，則從您的應用程式使用的 AWS 服務接收追蹤。在請求流過應用程式元件時，X-Ray 會對請求進行取樣並在服務圖表上視覺化。X-Ray 會產生追蹤識別符，以便您可以在請求流過多個元件時將其關聯，從而協助您從頭到尾檢視請求。您可以透過包含註釋和中繼資料來進一步增強此功能，以協助唯一地搜尋和識別請求的特性。

建議您使用 X-Ray 設定應用程式中的每個伺服器或端點。透過呼叫 X-Ray 服務在您的應用程式程式碼中實作 X-Ray。X-Ray 還提供適用於多種語言的 AWS SDK，包括自動將資料傳送至 X-Ray 的經檢測的用戶端。X-Ray SDK 為用於呼叫其他服務 (例如 HTTP、MySQL、PostgreSQL 或 MongoDB) 的常見程式庫提供修補程式。

如需詳細資訊，請參閱使用 AWS X-Ray 追蹤應用程式 (AWS 方案指引)。

X-Ray 的使用案例

- 應用程式分析和偵錯 – 追蹤資料可以透過提供請求的端對端檢視來協助您對應用程式進行偵錯，以便您可以識別瓶頸並對問題進行疑難排解。X-Ray 服務地圖是一種視覺化工具，可協助您識別發生錯誤的位置、高延遲的連線或不成功請求的追蹤。
- 效能分析 – Analytics 主控台是互動式工具，用於解譯追蹤資料以快速了解您的應用程式及其基礎服務的執行方式。主控台可協助您探索、分析和視覺化追蹤。您也可以比較不同條件下的追蹤集，以進行根本原因分析。

常見問答集

我是否可以使用目前監控服務？

Amazon CloudWatch 是一項為 DevOps 工程師、開發人員、網站可靠性工程 (SRE)、IT 經理和應用程式擁有者建置的監控和可觀測性服務。可為您提供資料和可行的洞察以協助您監控應用程式、回應整個系統的效能變更，以及優化資源使用率。但是，如果您已建立監控服務，則無需進行取代。

如何防止日誌檔案被篡改？

您可以啟用日誌檔案完整性驗證。您最好在專用 AWS 帳戶 中管理和儲存日誌並限制對該帳戶的存取。如需詳細資訊，請參閱本指南中的 使用 CloudTrail。

我是否必須為每個應用程式維護個別日誌檔案？

否，您可以將日誌資料從多個應用程式合併到相同日誌檔案。但是，請確保每個應用程式的唯一識別符都記錄在日誌串流中。

資源

AWS 文件

- AWS CloudTrail 文件
- AWS 雲端 查看文件
- AWS 雲端 查看日誌文件
- Amazon VPC 流程日誌文件
- AWS X-Ray 文件
- 使用 Amazon CloudWatch 設計和實作日誌記錄和監控 (AWS 方案指引)

AWS 行銷

- AWS CloudTrail
- Amazon CloudWatch
- AWS 上的集中式日誌記錄 (AWS 解決方案)
- 監控和可觀測性 (AWS 雲端 操作)
- 如何有效地監控您的應用程式 (AWS 新創公司)

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
初次出版	—	2023 年 1 月 6 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 資料庫遷移到與 Amazon Aurora PostgreSQL 相容的版本。
- 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 資料庫遷移到 Amazon Relational Database Service 服務 (Amazon RDS)，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：將您的現場部署 Oracle 資料庫遷移至中 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。

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、耐久性 (ACID)

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

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱 AWS Identity and Access Management (IAM) 文件 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 (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 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。常見的雲存儲庫包括 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)

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

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected 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。資料漂移可降低機器學習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。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，一 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

可自動化並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，可限制故障的影響，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，用於定義其在 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 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。這些也稱為抽象服務。

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，可提供驗證要移轉至的商業案例的 AWS 雲端資訊。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. 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

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

查看產品生命週期管理。

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。化名化有助於保護個人隱私。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（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。

拉西矩陣

請參閱負責任，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。

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。每個都 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) 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「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，然後再遷移伺服器和應用程式。

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。