監控和提醒 Amazon RDS for MySQL 和 MariaDB 的工具和最佳實務

AWS 方案指引

AWS 方案指引: 監控和提醒 Amazon RDS for MySQL 和 MariaDB 的工具和最佳實務

Table of Contents

監控和提醒 Amazon RDS for MySQL 和 MariaDB 的工具和最佳實務

Igor Obradovic，Amazon Web Services (AWS)

2025 年 3 月 (文件歷史記錄)

資料庫監控是衡量、追蹤和評估資料庫可用性、效能和功能的程序。監控和提醒解決方案可協助組織確保其資料庫服務及其相關聯的應用程式和工作負載安全、高效能、有彈性且高效。在 上 AWS，您可以收集和分析工作負載日誌、指標、事件和追蹤，以了解工作負載的運作狀態，並取得一段時間內操作的洞見。

您可以監控您的 資源，以確保它們如預期般執行，並在影響您的客戶之前偵測和修復任何問題。您應該使用監控的指標、日誌、事件和追蹤，在超過閾值時發出警示。

本指南說明 Amazon Relational Database Service (Amazon RDS) 資料庫的資料庫可觀測性和監控工具和最佳實務。本指南著重於 MySQL 和 MariaDB 資料庫，但大多數資訊也適用於其他 Amazon RDS 資料庫引擎。

本指南適用於解決方案架構師、資料庫架構師、DBAs、資深 DevOps 工程師和其他團隊成員，他們參與設計、實作和管理在 中執行之資料庫工作負載的監控和可觀測性解決方案 AWS 雲端。

內容

概觀

監控和提醒包含在 AWS Well-Architected Framework 的四個支柱中。

- 卓越營運支柱規定，您的工作負載應設計為包含遙測和監控。Amazon Relational Database Service (Amazon RDS) 等 AWS 服務提供了解工作負載內部狀態所需的資訊（例如指標、日誌、事件和追蹤）。當您操作 Amazon RDS 資料庫時，您會想要了解資料庫執行個體的運作狀態、偵測操作事件，並能夠同時回應計劃和非計劃事件。 AWS 提供監控工具，協助您判斷組織和業務成果何時面臨風險，或可能面臨風險，因此您可以在正確的時間採取適當的動作。
- 效能效率支柱規定，您應該即時收集、彙總和處理效能相關指標，以監控 資源的效能，例如 Amazon RDS 資料庫執行個體。您可以識別效能降低並修復因素，例如未最佳化的 SQL 查詢或導致它的組態參數不足。您可以在測量超出預期界限時自動發出警示。建議您不僅將警示用於通知，也要啟動自動動作以回應偵測到的事件。您可以根據預先定義的閾值評估收集的指標，或使用機器學習演算法來識別異常行為。例如，若要偵測 CPU 使用率增加的趨勢，您可以收集和分析一段時間內的`cpuUtilization.total`指標。在 CPU 使用率達到硬性限制之前主動提醒異常情況，可協助您在問題影響客戶之前修復問題。
- 可靠性支柱將監控和提醒定義為關鍵，以確保您符合可用性需求。您的監控解決方案必須能夠有效地偵測失敗。當它偵測到問題或失敗時，其主要目標是提醒這些問題。實作持續可觀測性和監控實務對於雲端中的彈性架構至關重要。若要改善工作負載，您必須能夠測量它們並了解其狀態和運作狀態。從故障、水平可擴展性和容量佈建自動復原的設計原則取決於準確的監控和提醒服務。
- 安全支柱討論偵測和預防非預期或不想要的組態變更，以及非預期的行為。您可以使用 MariaDB 稽核外掛程式來設定 Amazon RDS for MySQL 和 MariaDB 資料庫執行個體，以記錄資料庫活動，例如使用者登入和針對資料庫執行的特定操作。 MariaDB 外掛程式會將資料庫活動的記錄儲存在日誌檔案中，該檔案可以整合並匯入監控和提醒工具。日誌檔案會即時分析資料庫中是否有非預期或可疑的行為。這種非預期或可疑的行為可能表示您的 Amazon RDS 資料庫執行個體已遭到入侵，這會向業務發出潛在風險訊號。如果監控工具偵測到這類事件，它會啟用警示來啟動對安全事件的回應，這有助於解決可疑和惡意活動。

目標業務成果

在監控和警示機制中實作最佳實務，可協助您確保應用程式和工作負載的高效能、彈性、高效率、安全且成本最佳化的基礎設施。您可以使用可觀測性工具即時收集、存放和視覺化指標、事件、追蹤和日誌，以觀察和分析資料庫的運作狀態和效能，從而防止相關 IT 服務降級或中斷。如果意外降級或服務中斷仍然發生，監控和提醒工具可協助您及時偵測問題、呈報、反應，以及快速調查和解決。雲端資料庫工作負載的全方位監控和提醒解決方案可協助您實現下列業務成果：

- 改善客戶體驗。可靠的服務可改善客戶的體驗。資料庫通常是數位服務的關鍵元件，例如 Web 和行動應用程式、媒體串流、付款、business-to-business(B2B) APIs 和整合服務。如果您可以在資料庫上監控和設定提醒，以快速偵測問題、有效率地調查問題，並儘快修復這些問題，以盡可能減少停機時間和其他中斷，您可以為客戶增強數位服務的可用性、安全性和效能。
- 建立客戶信任。 更好的效能和更順暢的使用者體驗可協助您贏得客戶的信任，進而在您的平台上產生更多業務。例如，提供可靠線上服務的付款處理服務供應商可預期客戶高度信任和忠誠度，進而產生更多客戶和更好的保留、增加可計費交易，以及產生更多收入的新創新服務。
- 避免財務損失。 資料庫基礎設施中的任何意外停機時間都可能會影響客戶使用您的應用程式執行的業務交易。在某些情況下，這可能會導致巨大的經濟損失。違反服務水準協議 (SLAs) 可能會導致失去客戶信任，進而導致收入損失。它也可以成為昂貴試驗的法律依據，客戶可能會根據您的責任和保固合約要求補償。根據軟體公司 Atlassian Corporation 的一項研究，服務中斷的平均成本在每小時 140，000 – 540，000 USD 的範圍內，取決於業務的類型和大小。穩定的資料庫環境是防止長時間中斷和業務損失的關鍵。
- 展開值。監控和提醒機制可協助您設計、開發和操作高可用性、彈性、可靠、高效能、經濟實惠且安全的數位服務，但這只是一個開始。您會希望您的組織隨著時間擴展和茁壯成長、增強現有的雲端工作負載，以及引進新的服務。新服務為您的客戶提供額外價值，並為您的業務帶來更多收入，從而為您的業務成長帶來飛輪效果。
- 改善開發人員生產力。 具有生產力和效率，且在開發任務中未遇到問題和瓶頸的開發人員，可以在較短的時間內提供高品質的產品。不過，軟體工程和 IT 操作通常會面臨複雜的挑戰，而且這種複雜性會隨著工作負載及其架構的規模而增加。為了分析分散式應用程式的效能和一致性，開發人員需要可提供相關指標和追蹤的工具。這些有助於盡快識別瑕疵程式碼成品和基礎設施元件，並協助判斷對最終使用者的影響。正確的監控和提醒工具套件可協助開發人員更妥善且更快速地編寫程式碼和進行測試。
- 改善營運效率和效率。 當您大規模操作雲端工作負載時，即使只有一小部分的效能改善，也可以節省數百萬美元。透過監控資料庫和分析指標、事件、日誌和追蹤，您可以了解和預測未來容量需求，並利用 中提供的成本節省 AWS 雲端。了解 Amazon RDS 工作負載和運作狀態可協助您回應事件、修正問題和規劃改善。

一般最佳實務

下列最佳實務可協助您充分了解 Amazon RDS 工作負載的運作狀態，並採取適當的動作來回應操作事件和監控資料。

- 識別 KPIs。根據所需的業務成果識別關鍵績效指標 KPIs)。評估 KPIs以判斷工作負載是否成功。例如，如果您的核心業務是電子商務，您所需的業務成果之一可能是您的電子商店全年無休，可供您的客戶進行購物。為了實現該業務成果，您可以為 e-shop 應用程式使用的後端 Amazon RDS 資料庫定義可用性 KPI，並將基準 KPI 設定為每週 99.99%。根據基準值評估實際可用性 KPI，可協助您判斷是否達到所需的資料庫可用性 99.99%，從而實現擁有全年無休服務的業務成果。
- 定義工作負載指標。定義工作負載指標，以測量 Amazon RDS 工作負載的數量和品質。評估指標以判斷工作負載是否達到所需的結果，並了解工作負載的運作狀態。例如，若要評估 Amazon RDS 資料庫執行個體的可用性 KPI，您應該測量資料庫執行個體的運作時間和停機時間等指標。然後，您可以使用這些指標來計算可用性 KPI，如下所示：

  ```
  availability = uptime / (uptime + downtime)
  ```

  指標代表資料點的時間順序集。指標也可以包含維度，這些維度在分類和分析中很有用。
- 收集和分析工作負載指標。Amazon RDS 會根據您的組態產生不同的指標和日誌。其中一些代表資料庫執行個體事件、計數器或統計資料，例如 `db.Cache.innoDB_buffer_pool_hits`。其他指標來自作業系統，例如 `memory.Total`，可測量主機 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的記憶體總量。監控工具應定期主動分析收集的指標，以識別趨勢並判斷是否需要任何適當的回應。
- 建立工作負載指標基準。為指標建立基準，以定義預期值並識別好或壞的閾值。例如，您可以在正常資料庫操作下，將 的基準定義為`ReadIOPS`高達 1，000。然後，您可以使用此基準進行比較和識別過度使用。如果您的新指標持續顯示讀取 IOPS 的範圍介於 2，000–3，000 之間，表示您發現可能觸發回應以進行調查、介入和改善的偏差。
- 當工作負載結果有風險時發出提醒。當您判斷業務結果有風險時，請發出提醒。然後，您可以在問題影響您的客戶之前主動解決問題，或及時減輕事件的影響。
- 識別工作負載的預期活動模式。根據您的指標基準，建立工作負載活動模式以識別意外行為，並視需要回應適當的動作。 AWS 提供監控工具，可套用統計和機器學習演算法來分析指標並偵測異常。
- 偵測到工作負載異常時發出提醒。在 Amazon RDS 工作負載的操作中偵測到異常時，請發出提醒，以便您可以在必要時以適當的動作回應。
- 檢閱和修訂 KPIs和指標。確認您的 Amazon RDS 資料庫符合您定義的需求，並識別可能改善的領域，以達成您的業務目標。驗證測量指標和評估 KPIs的有效性，並視需要加以修訂。例如，假設您

為最佳數量的並行資料庫連線設定 KPI，並監控有關嘗試和失敗連線的指標，以及建立和執行中的使用者執行緒。您的資料庫連線可能比 KPI 基準所定義的更多。透過分析目前的指標，您可以偵測結果，但可能無法判斷根本原因。若是如此，您應該修改指標並包含其他監控措施，例如資料表鎖定的計數器。新的指標有助於判斷資料庫連線數量增加是否由未預期的資料表鎖定所造成。

監控工具

我們建議您使用可觀測性、監控和提醒工具來：

- 深入了解 Amazon RDS 環境的效能
- 偵測非預期和可疑的行為
- 規劃容量並做出有關配置 Amazon RDS 執行個體的教育決策
- 主動分析指標和日誌以預測潛在問題
- 在違反閾值時產生提醒，以便在使用者受到影響之前疑難排解和解決問題

您可以選擇不同的選項和解決方案，包括 AWS提供的雲端原生可觀測性和監控工具和服務；免費的開放原始碼軟體解決方案；以及用於監控 Amazon RDS 資料庫執行個體的商業第三方解決方案。以下各節會討論其中一些工具。

若要判斷哪個工具最適合您的需求，請將每個工具的功能和功能與您組織的需求進行比較。我們也建議您評估工具，以簡化部署、組態和整合、軟體更新和維護、部署方法（例如硬體或無伺服器）、授權、價格，以及組織特有的任何其他因素。

章節

Amazon RDS 中包含的工具

Amazon Relational Database Service (Amazon RDS) 是 中的受管資料庫服務 AWS 雲端。由於 Amazon RDS 是一項受管服務，可讓您免於執行大多數管理任務，例如資料庫備份、作業系統 (OS) 和資料庫軟體安裝、作業系統和軟體修補、高可用性設定、硬體生命週期和資料中心操作。 AWS 也提供一組完整的工具，可讓您為 Amazon RDS 資料庫執行個體建置完整的可觀測性解決方案。

Amazon RDS 服務中包含、預先設定並自動啟用一些監控工具。啟動新的 Amazon RDS 執行個體後，您可以立即使用兩種自動化工具：

- Amazon RDS 執行個體狀態提供資料庫執行個體目前運作狀態的詳細資訊。例如，狀態碼包括可用、已停止、建立、備份和失敗。您可以使用 Amazon RDS 主控台、 AWS Command Line Interface (AWS CLI) 或 Amazon RDS API 來查看執行個體狀態。如需詳細資訊，請參閱 Amazon RDS 文件中的檢視 Amazon RDS 資料庫執行個體狀態。
- Amazon RDS 建議提供資料庫執行個體、僅供讀取複本和資料庫參數群組的自動化建議。這些建議是透過分析資料庫執行個體用量、效能資料和組態提供，並做為指引提供。例如，引擎版本過時建議指出您的資料庫執行個體未執行最新版本的資料庫軟體，而且您應該升級資料庫執行個體，以受益於最新的安全性修正和其他改進。如需詳細資訊，請參閱《Amazon RDS 文件》中的檢視 Amazon RDS 建議。

CloudWatch 命名空間

Amazon RDS 與 Amazon CloudWatch 整合，Amazon CloudWatch 是一種監控和提醒服務，適用於在其中執行的雲端資源和應用程式 AWS。Amazon RDS 會自動收集有關資料庫執行個體操作、使用率、效能和運作狀態的指標、日誌檔案、追蹤和事件，並將其傳送至 CloudWatch 以進行長期儲存、分析和提醒。

Amazon RDS for MySQL 和 Amazon RDS for MariaDB 會以一分鐘的間隔自動將一組預設指標發佈至 CloudWatch，無需額外費用。這些指標會收集到兩個命名空間，這是指標的容器：

- AWS/RDS 命名空間包含資料庫執行個體層級指標。範例包括 `BinLogDiskUsage`（二進位日誌佔用的磁碟空間量）、 `CPUUtilization`(CPU 使用率百分比）、 `DatabaseConnections`（與資料庫執行個體的用戶端網路連線數量） 等等。
- AWS/Usage 命名空間包含帳戶層級用量指標，用於判斷您是否在 Amazon RDS 服務配額內操作。範例包括 `DBInstances`（您 AWS 帳戶或區域中的資料庫執行個體數目）、 `DBSubnetGroups`（您 AWS 帳戶或區域中的資料庫子網路群組數目） 和 `ManualSnapshots`（您 AWS 帳戶或區域中手動建立的資料庫快照數目）。

CloudWatch 保留如下指標資料：

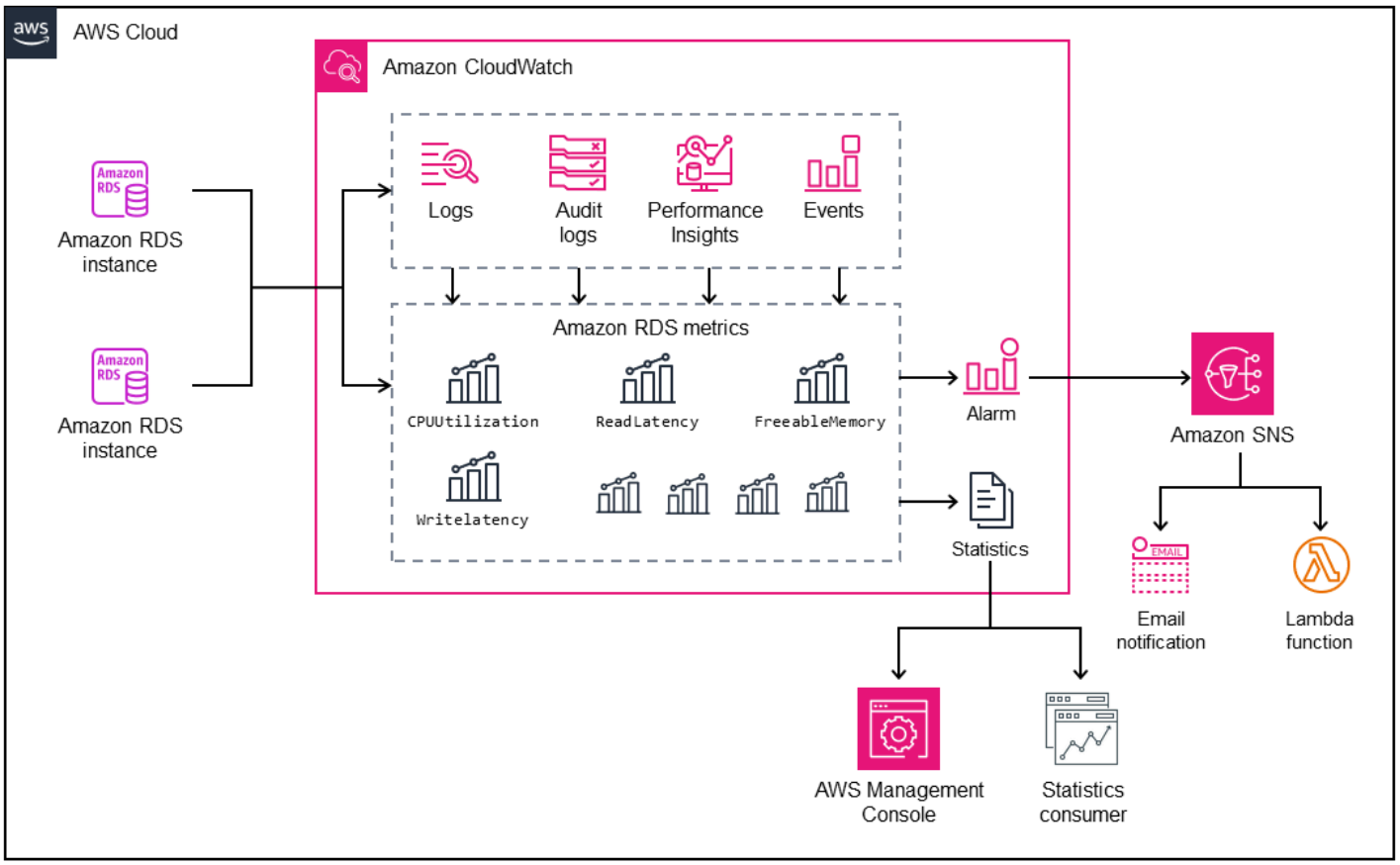
- 3 小時：期間少於 60 秒的高解析度自訂指標會保留 3 小時。3 小時後，資料點會彙總為 1 分鐘期間指標，並保留 15 天。
- 15 天：期間為 60 秒 (1 分鐘） 的資料點會保留 15 天。15 天後，資料點會彙總為 5 分鐘期間指標，並保留 63 天。

- 63 天：期間為 300 秒 (5 分鐘） 的資料點會保留 63 天。63 天後，資料點會彙總為 1 小時期間指標，並保留 15 個月。
- 15 個月：期間為 3，600 秒 (1 小時） 的資料點有效期為 15 個月 (455 天）。

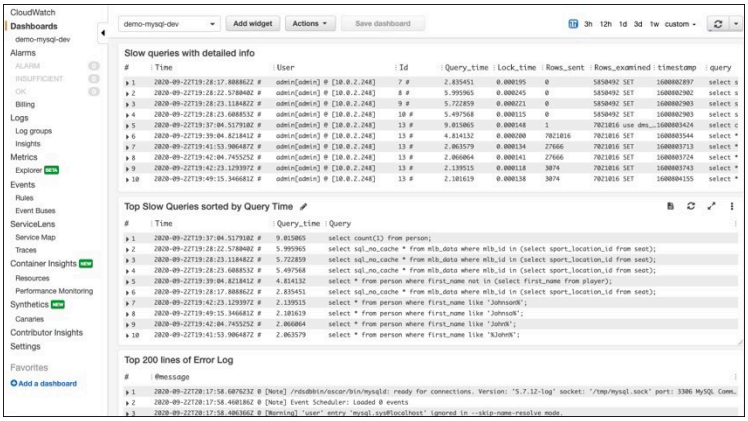
如需詳細資訊，請參閱 CloudWatch 文件中的指標。

CloudWatch 警示和儀表板

您可以使用 Amazon CloudWatch 警示來監看一段時間內的特定 Amazon RDS 指標。例如，您可以監控 `FreeStorageSpace`，然後在指標的值超過您設定的閾值時執行一或多個動作。如果您將閾值設定為 250 MB，且可用儲存空間為 200 MB （小於閾值），則會啟動警示，並觸發 動作來自動為 Amazon RDS 資料庫執行個體佈建額外的儲存空間。警示也可以使用 Amazon Simple Notification Service (Amazon SNS) 將通知簡訊傳送至 DBA。下圖說明此程序。

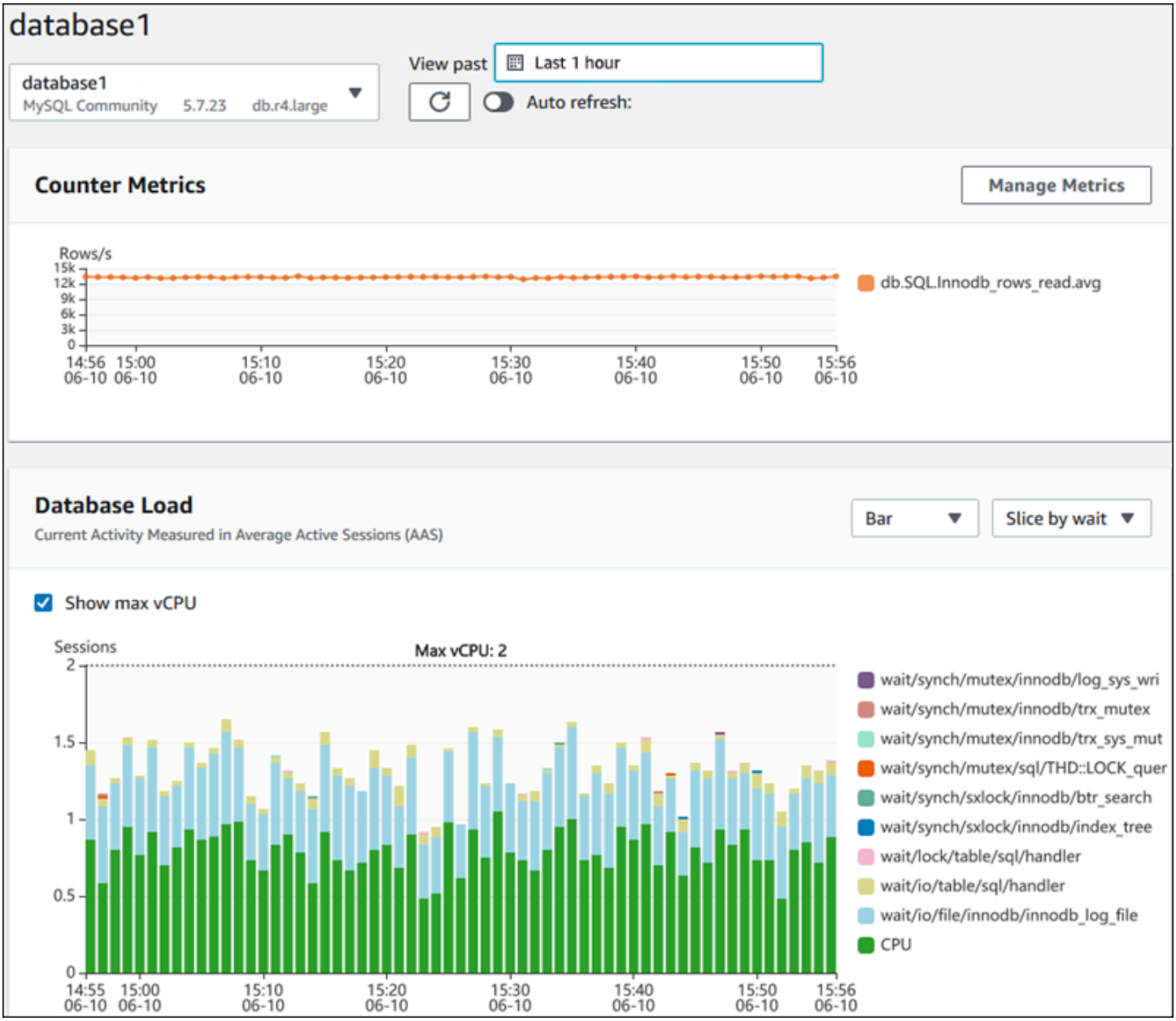


CloudWatch 也提供儀表板，可用來建立、自訂、互動和儲存指標的自訂檢視 （圖）。您也可以使用 CloudWatch Logs Insights 建立儀表板來監控慢查詢日誌和錯誤日誌，並在這些日誌中偵測到特定模式時接收提醒。下列畫面顯示 CloudWatch 儀表板範例。



Amazon RDS Performance Insights

Amazon RDS Performance Insights 是一種資料庫效能調校和監控工具，可擴展 Amazon RDS 監控功能。它透過視覺化資料庫執行個體負載並依等待、SQL 陳述式、主機或使用者篩選負載，協助您分析資料庫的效能。此工具將多個指標合併為單一互動式圖形，可協助您識別資料庫執行個體可能遇到的瓶頸類型，例如鎖定等待、高 CPU 耗用或 I/O 延遲，並判斷哪些 SQL 陳述式正在建立瓶頸。下列畫面顯示視覺化範例。



您必須在資料庫執行個體建立程序期間啟用績效詳情，才能收集您帳戶中 Amazon RDS 資料庫執行個體的指標。免費方案包括七天的效能資料歷史記錄和每月一百萬個 API 請求。或者，您可以購買較長的保留期。如需有關費用的資訊，請參閱 Performance Insights 定價。

如需有關如何使用績效詳情來監控資料庫執行個體的資訊，請參閱本指南稍後的資料庫執行個體監控一節。

Performance Insights 會自動將指標發佈至 CloudWatch。除了使用績效詳情工具之外，您還可以利用 CloudWatch 提供的其他功能。您可以使用 CloudWatch 主控台、 AWS CLI或 CloudWatch API 來檢查績效詳情指標。您也可以新增 CloudWatch 警示，就像任何其他指標一樣。例如，您可能想要觸發向

DBAs簡訊通知，或在DBLoad指標超過您設定的閾值時採取修正動作。您也可以將績效詳情指標新增至現有的 CloudWatch 儀表板。

Enhanced Monitoring (增強型監控)

增強型監控是一種工具，可即時擷取 Amazon RDS 資料庫執行個體執行所在的作業系統 (OS) 指標。這些指標可為 CPU、記憶體、Amazon RDS 和作業系統程序、檔案系統和磁碟 I/O 資料等提供高達一秒的精細程度。您可以在 Amazon RDS 主控台中存取和分析這些指標。如同績效詳情，增強型監控指標會從 Amazon RDS 交付至 CloudWatch，您可以在其中受益於其他功能，例如長期保留用於分析的指標、建立指標篩選條件、在 CloudWatch 儀表板上顯示圖形，以及設定警示。根據預設，當您建立新的 Amazon RDS 資料庫執行個體時，會停用增強型監控。您可以在建立或修改資料庫執行個體時啟用此功能。定價是根據從 Amazon RDS 傳輸到 CloudWatch Logs 的資料量，以及儲存費率。根據精細程度和啟用增強型監控的資料庫執行個體數量，CloudWatch Logs 免費方案中可以包含部分監控資料。如需完整的定價詳細資訊，請參閱 Amazon CloudWatch 定價。如需工具的詳細資訊，請參閱 Amazon RDS 文件和增強型監控常見問答集。

AWS 其他服務

AWS 提供數種支援服務，也與 Amazon RDS 和 CloudWatch 整合，進一步增強資料庫的可觀測性。其中包括 Amazon EventBridge、Amazon CloudWatch Logs 和 AWS CloudTrail。

- Amazon EventBridge 是無伺服器事件匯流排，可接收、篩選、轉換、路由和交付來自您應用程式 AWS 和資源的事件，包括您的 Amazon RDS 資料庫執行個體。Amazon RDS 事件表示 Amazon RDS 環境中的變更。例如，當資料庫執行個體將其狀態從可用變更為已停止時，Amazon RDS 會產生事件 `RDS-EVENT-0087 / The DB instance has been stopped`。Amazon RDS 會以近乎即時的方式將事件交付至 CloudWatch Events 和 EventBridge。使用 EventBridge 和 CloudWatch Events，您可以定義規則，以針對特定感興趣的 Amazon RDS 事件傳送提醒，並自動執行事件符合規則時要採取的動作。有各種目標可用於回應事件，例如可執行修正動作的 AWS Lambda 函數，或可傳送電子郵件或簡訊以通知 DBAs 或 DevOps 工程師有關事件的 Amazon SNS 主題。
- Amazon CloudWatch Logs 是一項服務，可集中儲存所有應用程式、系統和 AWS 服務的日誌檔案，包括 Amazon RDS for MySQL 和 MariaDB 資料庫執行個體 和 AWS CloudTrail。如果您為資料庫執行個體啟用 功能，Amazon RDS 會自動將下列日誌發佈至 CloudWatch Logs：
  - 錯誤日誌
  - 慢查詢日誌
  - 一般日誌
  - 稽核日誌

您可以使用 CloudWatch Logs Insights 來查詢和分析日誌資料。該功能包含專用查詢語言，可協助您搜尋符合您定義的模式的日誌事件。例如，您可以透過監控以下模式的錯誤日誌檔案來追蹤 MySQL 資料庫執行個體中的資料表損毀：`"ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"`。篩選的日誌資料可以轉換為 CloudWatch 指標。然後，您可以使用 指標建立具有圖形或表格資料的儀表板，或在違反定義的閾值時設定警示。這在使用稽核日誌時特別有用，因為您可以自動監控、傳送警示，並在偵測到任何非預期或可疑的行為時採取修正動作。您可以使用 AWS 管理主控台、 AWS CLI、Amazon RDS API 或適用於 CloudWatch Logs 的 AWS SDK 來存取和管理資料庫日誌。

- AWS CloudTrail 會記錄並持續監控 中的使用者和 API 活動 AWS 帳戶。它可協助您稽核、安全監控和操作故障診斷 Amazon RDS for MySQL 或 MariaDB 資料庫執行個體。CloudTrail 已與 Amazon RDS 整合。您可以記錄所有動作，CloudTrail 會提供 Amazon RDS 中使用者、角色 AWS 或服務所採取動作的記錄。例如，當使用者建立新的 Amazon RDS 資料庫執行個體時，會偵測到事件，而日誌包含有關請求的動作 (`"eventName": "CreateDBInstance"`)、動作的日期和時間 (`"eventTime": "2022-07-30T22:14:06Z"`)、請求參數 (`"requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}`) 等資訊。CloudTrail 記錄的事件包括來自 Amazon RDS 主控台的呼叫，以及來自使用 Amazon RDS API 之程式碼的呼叫。

第三方監控工具

在某些情況下，除了為 Amazon RDS AWS 提供的完整雲端原生可觀測性和監控工具套件之外，您可能還想要使用其他軟體供應商的監控工具。這類案例包括混合部署，您可以在內部部署資料中心中執行多個資料庫，以及在 中執行另一組資料庫 AWS 雲端。如果您已建立企業可觀測性解決方案，建議您繼續使用現有的工具，並將其擴展到您的 AWS 雲端 部署。設定第三方監控解決方案的挑戰通常在於 Amazon RDS 作為雲端受管服務實施的保護措施。例如，您無法在執行資料庫執行個體的主機作業系統上安裝代理程式軟體，因為對資料庫主機機器的存取遭拒。不過，您可以透過在 CloudWatch 和其他 AWS 雲端 服務上建置 ，將許多第三方監控解決方案與 Amazon RDS 整合。例如，Amazon RDS 指標、日誌、事件和追蹤可以匯出，然後匯入至第三方監控工具，以進行進一步分析、視覺化和提醒。其中一些第三方解決方案包括 Prometheus、Grafana 和 Percona。

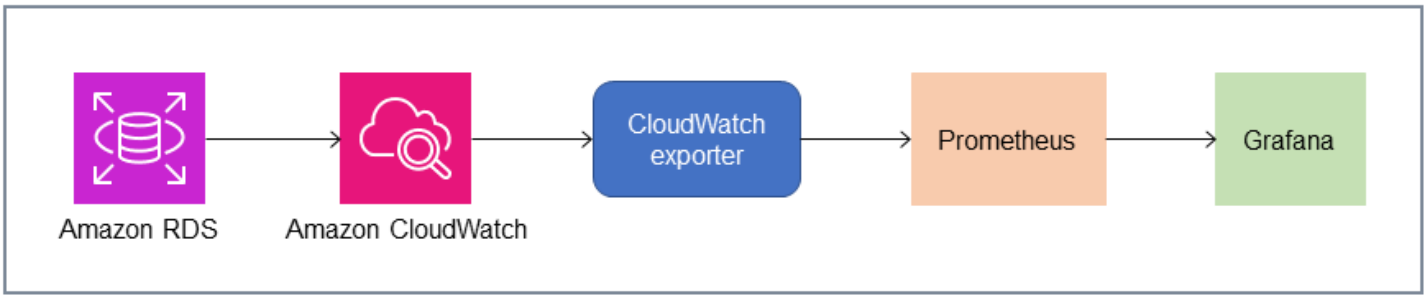
Prometheus 和 Grafana

Prometheus 是一種開放原始碼監控解決方案，可依指定間隔從設定的目標收集指標。這是一般用途的監控解決方案，可監控任何應用程式或服務。當您監控 Amazon RDS 資料庫執行個體時，CloudWatch 會從 Amazon RDS 收集指標。接著會使用 YACE 匯出工具或 CloudWatch Exporter 等開放原始碼匯出工具，將指標匯出至 Prometheus 伺服器。

- YACE 匯出工具透過在對 CloudWatch API 的單一請求中擷取多個指標來最佳化資料匯出任務。在 Prometheus 伺服器上存放指標之後，伺服器會評估規則表達式，並在觀察到指定條件時產生警示。
- CloudWatch Exporter 由 Prometheus 正式維護。它透過 CloudWatch API 擷取 CloudWatch 指標，並使用對 HTTP 端點的 REST API 請求，以與 Prometheus 相容的格式將其存放在 Prometheus 伺服器上。

當您選擇匯出工具、設計部署模型和設定匯出工具執行個體時，請考慮 CloudWatch 和 CloudWatch Logs 服務和 API 配額，因為 CloudWatch 指標匯出至 Prometheus 伺服器是在 CloudWatch API 上實作。例如，在單一 AWS 帳戶 和區域中部署多個 CloudWatch Exporter 執行個體來監控數百個 Amazon RDS 資料庫執行個體可能會導致限流錯誤 (ThrottlingException) 和程式碼 400 錯誤。若要克服此類限制，請考慮使用 YACE 匯出工具，該匯出工具已最佳化，可在單一請求中收集多達 500 個不同的指標。此外，若要部署大量 Amazon RDS 資料庫執行個體，您應該考慮使用多個 AWS 帳戶 ，而不是將工作負載集中到單一 AWS 帳戶，並限制每個 中的匯出者執行個體數量 AWS 帳戶。

提醒是由 Prometheus 伺服器產生，並由 Alertmanager 處理。此工具負責將警示刪除、分組和路由至正確的接收者，例如電子郵件、簡訊或 Slack，或啟動自動回應動作。另一個名為 Grafana 的開放原始碼工具會顯示這些指標的視覺化效果。Grafana 提供豐富的視覺化小工具，例如進階圖形、動態儀表板和分析功能，例如臨機操作查詢和動態向下切入。它也可以搜尋和分析日誌，並包含提醒功能以持續評估指標和日誌，並在資料符合提醒規則時傳送通知。



Percona

Percona Monitoring and Management (PMM) 是 MySQL 和 MariaDB 的免費開放原始碼資料庫監控、管理和可觀測性解決方案。PMM 會從資料庫執行個體及其主機收集數千個效能指標。它提供 Web UI，以視覺化儀表板中的資料和其他功能，例如資料庫運作狀態評估的自動建議。您可以使用 PMM 來監控 Amazon RDS。不過，PMM 用戶端 （代理程式） 不會安裝在 Amazon RDS 資料庫執行個體的基礎主機上，因為它無法存取主機。反之，工具會連線至 Amazon RDS 資料庫執行個體、查詢伺服器統計資料、INFORMATION_SCHEMA、sys 結構描述和效能結構描述，並使用 CloudWatch API 來取得指標、日誌、事件和追蹤。PMM 需要 AWS Identity and Access Management (IAM) 使用者存取金鑰 (IAM 角色），並自動探索可用於監控的 Amazon RDS 資料庫執行個體。PMM 工具的設定檔用於資料

庫監控，並收集比 Prometheus 更多的資料庫特定指標。若要使用 PMM Query Analytics 儀表板，您必須將效能結構描述設定為查詢來源，因為 Amazon RDS 未安裝 Query Analytics 代理程式，且無法讀取慢查詢日誌。相反`performance_schema`地，它會直接從 MySQL 和 MariaDB 資料庫執行個體查詢 以取得指標。PMM 的其中一個重要功能是能夠提醒和建議 DBAs 有關工具在其資料庫中識別的問題。PMM 提供一組檢查，可偵測常見的安全威脅、效能降低、資料遺失和資料損毀。

除了這些工具之外，市場上還提供多種商業可觀測性和監控解決方案，可與 Amazon RDS 整合。範例包括 Datadog 資料庫監控、Dynatrace Amazon RDS 監控和 AppDynamics 資料庫監控。

資料庫執行個體監控

資料庫執行個體是 Amazon RDS 的基本建置區塊。它是在雲端中執行的隔離資料庫環境。對於 MySQL 和 MariaDB 資料庫，資料庫執行個體是 mysqld 程式，也稱為 MySQL 伺服器，其中包含多個執行緒和元件，例如 SQL 剖析器、查詢最佳化器、執行緒/連線處理常式、系統和狀態變數，以及一或多個可插入儲存引擎。每個儲存引擎都旨在支援特殊的使用案例。預設和建議的儲存引擎是 InnoDB，這是一種交易、一般用途、關聯式資料庫引擎，符合原子性、一致性、隔離、耐久性 (ACID) 模型。InnoDB 具有記憶體內結構（緩衝集區、變更緩衝區、適應性雜湊索引、日誌緩衝區）以及磁碟上結構（資料表空間、資料表、索引、復原日誌、重做日誌、雙寫緩衝檔案）。為了確保您的資料庫緊密遵循 ACID 模型，InnoDB 儲存引擎實作許多功能來保護您的資料，包括交易、遞交、轉返、損毀復原、資料列層級鎖定和多版本並行控制 (MVCC)。

資料庫執行個體的所有這些內部元件會共同運作，以協助將資料的可用性、完整性和安全性維持在預期且令人滿意的效能層級。根據您的工作負載，每個元件和功能可能會對 CPU、記憶體、網路和儲存子系統施加資源需求。當特定資源的需求激增超過佈建容量或該資源的軟體限制時（由組態參數或軟體設計施加），資料庫執行個體可能會遇到效能降低或完全無法使用和損毀。因此，測量和監控這些內部元件、將它們與定義的基準值進行比較，以及在監控的值偏離預期值時產生提醒至關重要。

如前所述，您可以使用不同的工具來監控 MySQL 和 MariaDB 執行個體。我們建議您使用 Amazon RDS Performance Insights 和 CloudWatch 工具進行監控和警示，因為這些工具已與 Amazon RDS 整合、收集高解析度指標、近乎即時地呈現最新的效能資訊，以及產生警示。

無論您偏好的監控工具為何，建議您在 MySQL 和 MariaDB 資料庫執行個體中開啟效能結構描述。效能結構描述是監控 MySQL 伺服器（資料庫執行個體）在低層級操作的選用功能，旨在對整體資料庫效能產生最小的影響。您可以使用 `performance_schema` 參數來管理此功能。雖然此參數是選用的，但您必須使用它來收集 Amazon RDS Performance Insights 收集的高解析度（一秒）每個 SQL 指標、作用中工作階段指標、等待事件和其他詳細的低階監控資訊。

章節

- 資料庫執行個體的績效詳情指標
- 資料庫執行個體的 CloudWatch 指標
- 將績效詳情指標發佈至 CloudWatch

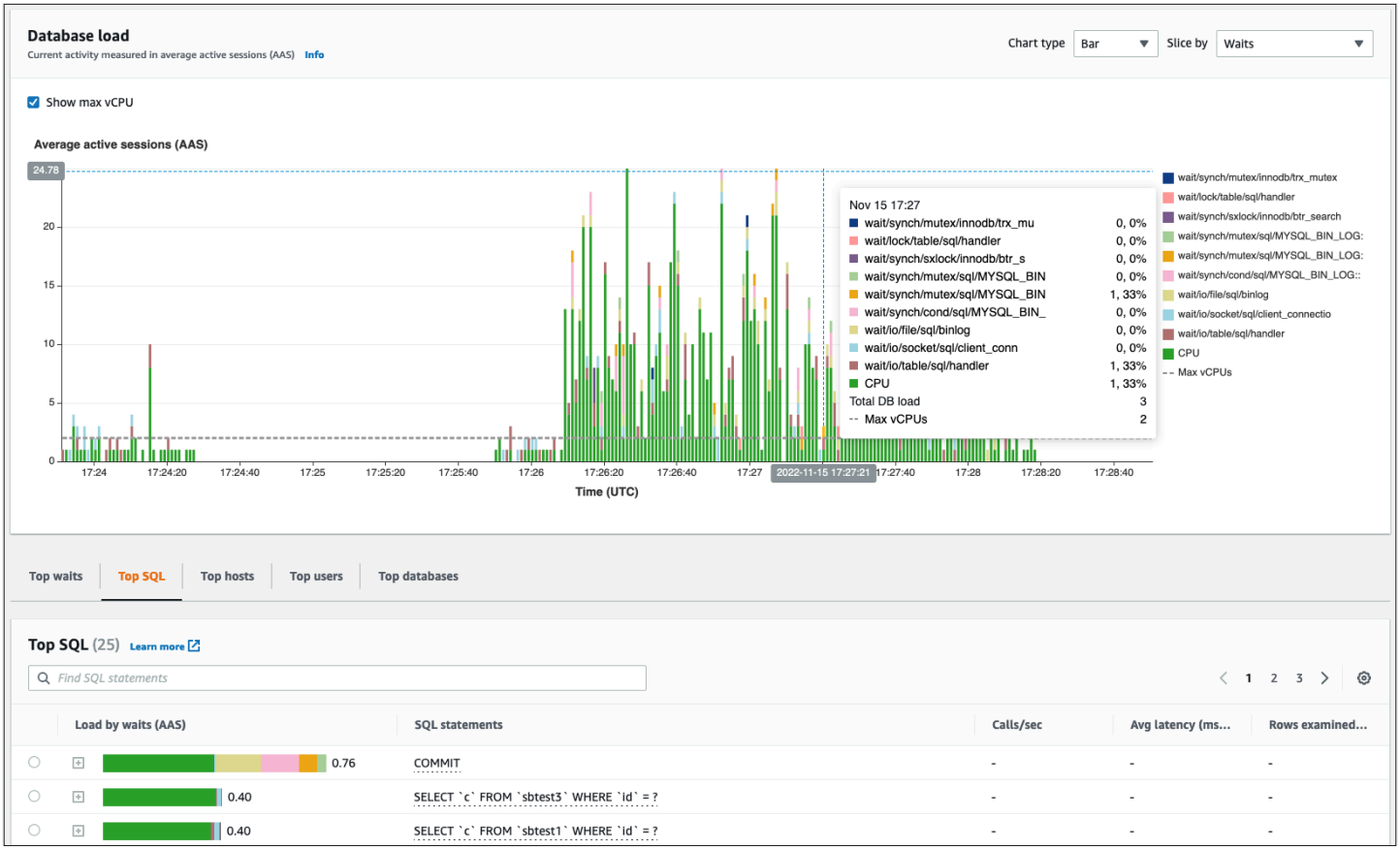
資料庫執行個體的績效詳情指標

Performance Insights 會監控不同類型的指標，如下列各節所述。

資料庫負載

資料庫負載 (DBLoad) 是績效詳情中測量資料庫中活動層級的關鍵指標。它會每秒收集一次，並自動發佈到 Amazon CloudWatch。它代表資料庫執行個體在平均作用中工作階段 (AAS) 中的活動，這是同時執行 SQL 查詢的工作階段數目。DBLoad 指標與其他時間序列指標不同，因為它可以使用以下五個維度中的任何一個來解譯：等待、SQL、主機、使用者和資料庫。這些維度是DBLoad指標的子類別。您可以使用它們做為依類別分割，以代表資料庫載入的不同特性。如需如何計算資料庫負載的詳細說明，請參閱 Amazon RDS 文件中的資料庫負載。

下列畫面圖顯示績效詳情工具。



維度

- 等待事件是資料庫工作階段等待資源或其他操作完成以繼續處理的條件。如果您執行 SQL 陳述式，例如 `SELECT * FROM big_table`，而且此資料表遠大於配置的 InnoDB 緩衝集區，則您的工作階段很可能會等待`wait/io/file/innodb/innodb_data_file`等待事件，這些事件是由資料檔案的實體 I/O 操作所造成。等待事件是資料庫監控的重要維度，因為它們表示可能的效能瓶頸。等待事件指出您在工作階段中執行的 SQL 陳述式花費最多時間等待的資源和操作。例如，當有大量交易的高資料庫活動時發生`wait/synch/mutex/innodb/trx_sys_mutex`事件，而執行緒

已在 InnoDB 緩衝集區上取得鎖定以存取記憶體中的頁面時發生`wait/synch/mutex/innodb/buf_pool_mutex`事件。如需有關所有 MySQL 和 MariaDB 等待事件的資訊，請參閱 MySQL 文件中的等待事件摘要資料表。若要了解如何解譯檢測器名稱，請參閱 MySQL 文件中的效能結構描述檢測器命名慣例。

- SQL 會顯示哪些 SQL 陳述式對總資料庫負載的貢獻最大。位於 Amazon RDS Performance Insights 中資料庫負載圖表下方的最高維度資料表是互動式的。您可以按一下「依等待載入 (AAS)」欄中的列，以取得與 SQL 陳述式相關聯的等待事件詳細清單。當您在清單中選取 SQL 陳述式時，績效詳情會在資料庫負載圖表中顯示相關聯的等待事件，並在 SQL 文字區段中顯示 SQL 陳述式文字。SQL 統計資料會顯示在最高維度資料表的右側。
- 主機會顯示連線用戶端的主機名稱。此維度可協助您識別哪些用戶端主機將大部分負載傳送至資料庫。
- 使用者依登入資料庫的使用者將資料庫負載分組。
- 資料庫會根據用戶端連線的資料庫名稱，將資料庫負載分組。

計數器指標

計數器指標是累積指標，其值只能在資料庫執行個體重新啟動時增加或重設為零。計數器指標的值無法降至其先前的值。這些指標代表單一、單調增加的計數器。

- 原生計數器是由資料庫引擎而非 Amazon RDS 定義的指標。例如：
  - `SQL.Innodb_rows_inserted` 代表插入 InnoDB 資料表的列數。
  - `SQL.Select_scan` 代表完成第一個資料表完整掃描的聯結數目。
  - `Cache.Innodb_buffer_pool_reads` 代表 InnoDB 引擎無法從緩衝集區擷取且必須直接從磁碟讀取的邏輯讀取數目。
  - `Cache.Innodb_buffer_pool_read_requests` 代表邏輯讀取請求的數量。

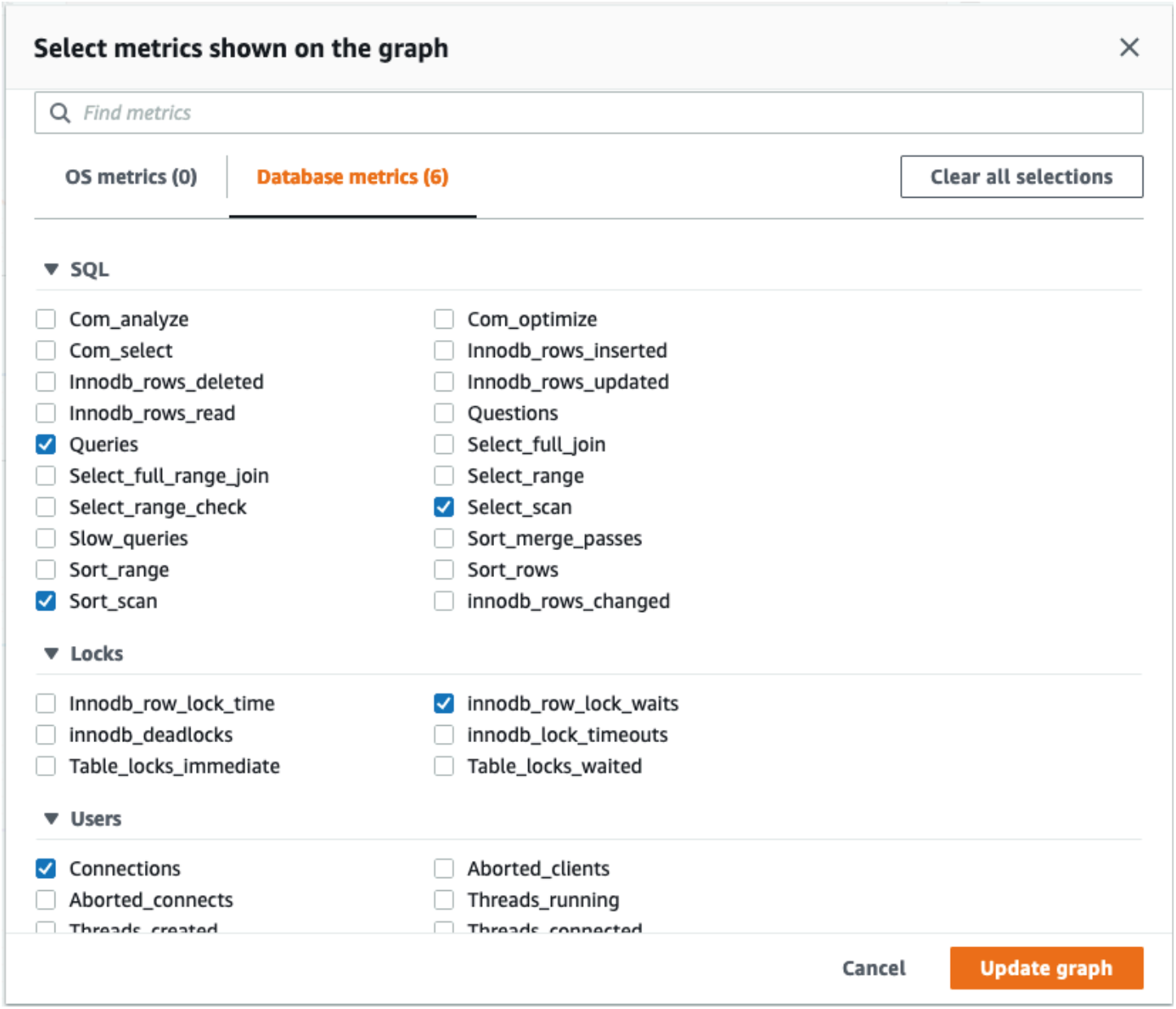
  如需所有原生指標的定義，請參閱 MySQL 文件中的伺服器狀態變數。
- 非原生計數器由 Amazon RDS 定義。您可以使用特定查詢來取得這些指標，或在計算中使用兩個或多個原生指標來衍生這些指標。非原生計數器指標可以代表延遲、比率或命中率。例如：
  - `Cache.innoDB_buffer_pool_hits` 代表 InnoDB 可以在不使用磁碟的情況下從緩衝集區擷取的讀取操作數目。它根據原生計數器指標計算，如下所示：

```
db.Cache.Innodb_buffer_pool_read_requests - db.Cache.Innodb_buffer_pool_reads
```

- `IO.innoDB_datafile_writes_to_disk` 代表磁碟的 InnoDB 資料檔案寫入操作數目。它只會擷取資料檔案的操作，而不是重寫或重做記錄寫入操作。其計算方式如下：

```
db.IO.Innodb_data_writes - db.IO.Innodb_log_writes - db.IO.Innodb_dblwr_writes
```

您可以直接在績效詳情儀表板中視覺化資料庫執行個體指標。選擇管理指標，選擇資料庫指標索引標籤，然後選取感興趣的指標，如下圖所示。



選擇更新圖形按鈕以顯示您選取的指標，如下圖所示。

SQL Statistics

Performance Insights 會針對查詢執行的每個秒和每個 SQL 呼叫，收集 SQL 查詢的效能相關指標。一般而言，績效詳情會在陳述式和摘要層級收集 SQL 統計資料。不過，對於 MariaDB 和 MySQL 資料庫執行個體，統計資料只會在摘要層級收集。

- 摘要統計資料是具有相同模式但最終具有不同常值之所有查詢的複合指標。摘要會以變數取代特定常值；例如：

```
SELECT department_id, department_name FROM departments WHERE location_id = ?
```

- 有些指標代表每個摘要 SQL 陳述式的每秒統計資料。例如，`sql_tokenized.stats.count_star_per_sec`代表每秒呼叫數（也就是 SQL 陳述式每秒執行多少次）。
- Performance Insights 也包含提供 SQL 陳述式每個呼叫統計資料的指標。例如，`sql_tokenized.stats.sum_timer_wait_per_call` 顯示每次呼叫 SQL 陳述式的平均延遲，以毫秒為單位。

SQL 統計資料可在績效詳情儀表板的頂部 SQL 索引標籤的頂部維度資料表中取得。

資料庫執行個體的 CloudWatch 指標

Amazon CloudWatch 也包含 Amazon RDS 自動發佈的指標。命名AWS/RDS空間中的指標是執行個體層級指標，是指 Amazon RDS （服務） 執行個體 （即在雲端中執行的隔離資料庫環境），而不是嚴格感知 mysqld 程序的資料庫執行個體。因此，這些預設指標大部分都屬於作業系統指標的類別，在 術語的嚴格定義中。範例包括：CPUUtilization、SwapUsage、 WriteIOPS和其他。不過，有些資料庫執行個體指標適用於 MariaDB 和 MySQL：

- `BinLogDiskUsage` – 二進位日誌佔用的磁碟空間量。
- `DatabaseConnections` – 資料庫執行個體的用戶端網路連線數目。
- `ReplicaLag` – 僅供讀取複本資料庫執行個體落後於來源資料庫執行個體的時間。

將績效詳情指標發佈至 CloudWatch

Amazon RDS Performance Insights 會監控大多數資料庫執行個體指標和維度，並透過 AWS 管理主控台上的績效詳情儀表板提供這些指標和維度。此儀表板非常適合資料庫故障診斷和根本原因分析。不過，無法在績效詳情中為效能相關指標建立警示。如果您想要根據績效詳情指標建立警示，這些指標必須在 CloudWatch 中。

Performance Insights 會自動將指標發佈至 CloudWatch。您可以從績效詳情中查詢相同的資料，但 CloudWatch 中的指標可讓您輕鬆地新增 CloudWatch 警示，並將指標新增至現有的 CloudWatch 儀表板。計數器是作業系統和資料庫效能指標，例如 `os.memory.free`或 `db.Locks.Innodb_row_lock_time`。作業系統指標集合取決於增強型監控設定。如果已關閉增強型監控，則會每分鐘收集一次作業系統指標。如果開啟增強型監控，則會在所選期間內收集作業系統指標。如需詳細資訊，請參閱 Amazon RDS 文件中的開啟和關閉增強型監控。

Performance Insights 可讓您將資料庫執行個體的預先設定或自訂指標儀表板匯出至 CloudWatch。您可以將此指標儀表板匯出為新的儀表板，或將其新增至現有的 CloudWatch 儀表板。將績效詳情指標儀表板匯出至 CloudWatch 儀表板可讓您全面檢視系統的運作狀態，提供與系統中各種資源相關聯的指標概觀，例如 EC2 執行個體、Amazon Elastic File System (Amazon EFS) 資源和 Elastic Load Balancing (ELB) 資源，以及資料庫執行個體指標。

您可以使用 CloudWatch DB_PERF_INSIGHTS 指標數學函數，根據 CloudWatch 的績效詳情指標來查詢和建立警示和圖形。若要在績效詳情指標上建立警示，請遵循 CloudWatch 文件中的指示。例如，如果您想要在資料庫執行個體中的作用中交易總數達到特定閾值時觸發警示，請遵循該頁面上的指示，使用下列DB_PERF_INSIGHTS數學表達式，然後選擇套用：

```
DB_PERF_INSIGHTS('RDS', 'db-BQ2TPYY7HG2GDFC7APMB3BVB3M',
 'db.Transactions.active_transactions.avg')
```

其中 db-BQ2TPYY7HG2GDFC7APMB3BVB3M是資料庫執行個體的資源 ID。指定期間（例如 1 分鐘）和條件（例如大於 1000)。若要完成警示的建立、設定警示動作、新增名稱和描述，以及預覽和建立警示。

作業系統監控

Amazon RDS for MySQL 或 MariaDB 中的資料庫執行個體會在 Linux 作業系統上執行，該作業系統使用基礎系統資源：CPU、記憶體、網路和儲存。

```
MySQL [(none)]> SHOW variables LIKE 'version%';
+-------------------------+----------------------+
| Variable_name           | Value                |
+-------------------------+----------------------+
| version                 | 8.0.28               |
| version_comment         | Source distribution |
| version_compile_machine | aarch64              |
| version_compile_os      | Linux                |
| version_compile_zlib    | 1.2.11               |
+-------------------------+----------------------+
5 rows in set (0.00 sec)
```

資料庫和基礎作業系統的整體效能，完全取決於系統資源的使用率。例如，CPU 是系統效能的關鍵元件，因為它會執行資料庫軟體指示並管理其他系統資源。如果 CPU 過度使用（也就是說，如果負載需要比為資料庫執行個體佈建更多的 CPU 功率），此問題會影響資料庫的效能和穩定性，進而影響您的應用程式。

資料庫引擎會動態配置和釋放記憶體。當 RAM 沒有足夠的記憶體來執行目前的工作時，系統會將記憶體頁面寫入位於磁碟上的交換記憶體。由於磁碟比記憶體慢得多，即使磁碟是以 SSD NVMe 技術為基礎，過度配置記憶體也會導致效能降低。高記憶體使用率會導致資料庫回應的延遲增加，因為頁面檔案的大小會成長以支援額外的記憶體。如果記憶體配置太高，以致於耗盡了 RAM 和交換記憶體空間，則資料庫服務可能會變得無法使用，使用者可能會發現錯誤，例如 `[ERROR] mysqld: Out of memory (Needed xyz bytes)`。

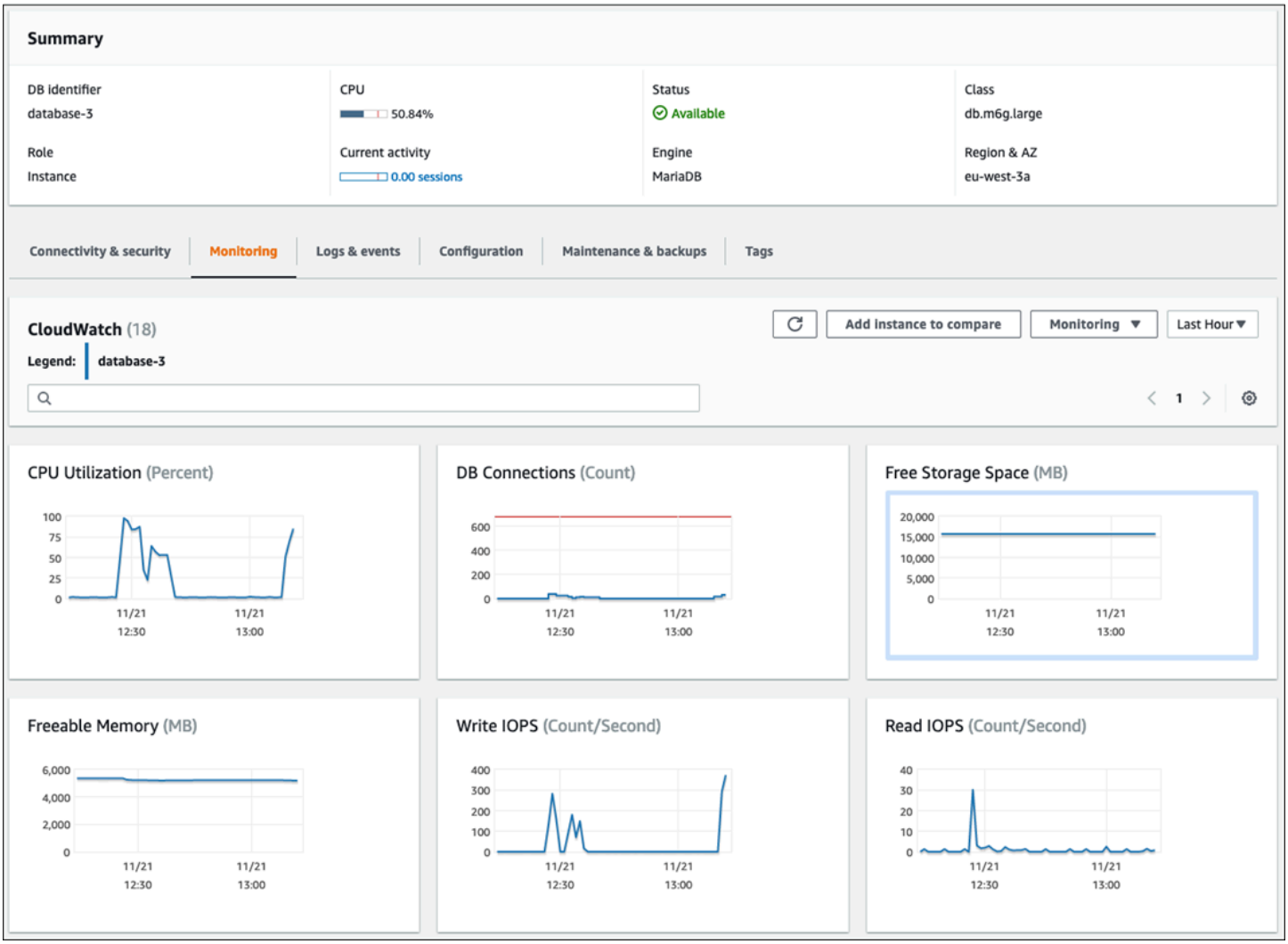
MySQL 和 MariaDB 資料庫管理系統使用儲存子系統，其中包含存放磁碟上結構的磁碟，例如資料表、索引、二進位日誌、重做日誌、復原日誌和雙寫緩衝區檔案。因此，相較於其他類型的軟體，資料庫必須執行許多磁碟活動。為了獲得最佳的資料庫操作，請務必監控和調整磁碟 I/O 使用率和磁碟空間配置。當資料庫達到磁碟支援的最大 IOPS 或輸送量限制時，資料庫效能可能會受到影響。例如，索引掃描導致的隨機存取暴增可能導致每秒大量的 I/O 操作，最終可能會影響基礎儲存體的限制。完整資料表掃描可能不會達到 IOPS 限制，但可能會導致高輸送量，以每秒 MB 為單位。監控和產生磁碟空間分配警示至關重要，因為 等錯誤`OS error code 28: No space left on device`可能會導致資料庫無法使用和損毀。

Amazon RDS 為您的資料庫執行個體執行所在的作業系統即時提供指標。Amazon RDS 會自動將一組作業系統指標發佈至 CloudWatch。您可以在 Amazon RDS 主控台和 CloudWatch 儀表板中顯示和分析這些指標，也可以在 CloudWatch 中設定所選指標的警示。範例包括：

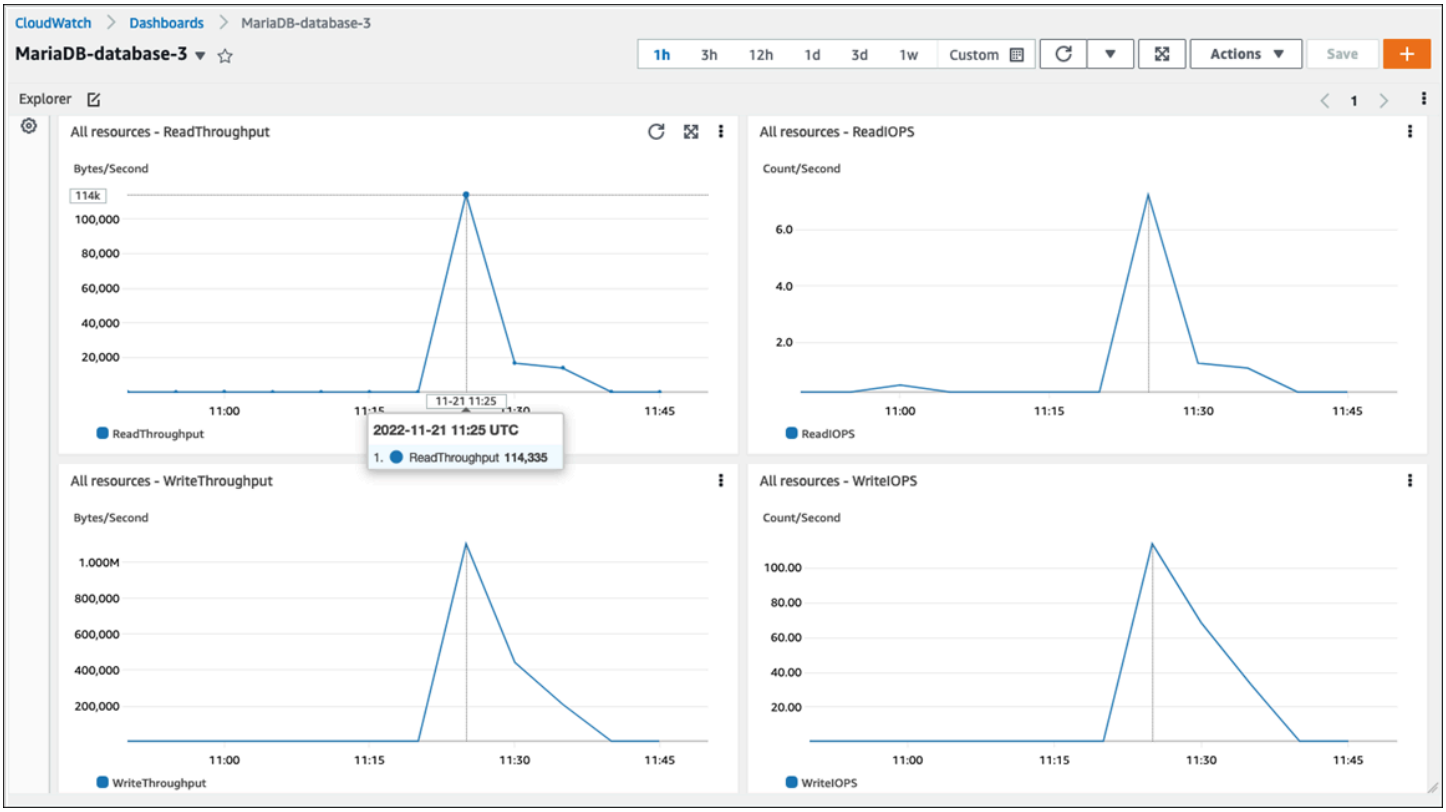
- `CPUUtilization` – CPU 使用率的百分比。
- `BinLogDiskUsage` – 二進位日誌佔用的磁碟空間量。
- `FreeableMemory` – 可用的隨機存取記憶體數量。這代表 的 `MemAvailable` 欄位值`/proc/meminfo`。
- `ReadIOPS` – 每秒磁碟讀取 I/O 操作的平均數量。
- `WriteThroughput` – 本機儲存體每秒寫入磁碟的平均位元組數。
- `NetworkTransmitThroughput` – 資料庫節點上的傳出網路流量，結合了用於監控和複寫的資料庫流量和 Amazon RDS 流量。

如需 Amazon RDS 發佈至 CloudWatch 的所有指標的完整參考，請參閱 Amazon RDS 文件中的 Amazon RDS 的 Amazon CloudWatch 指標。

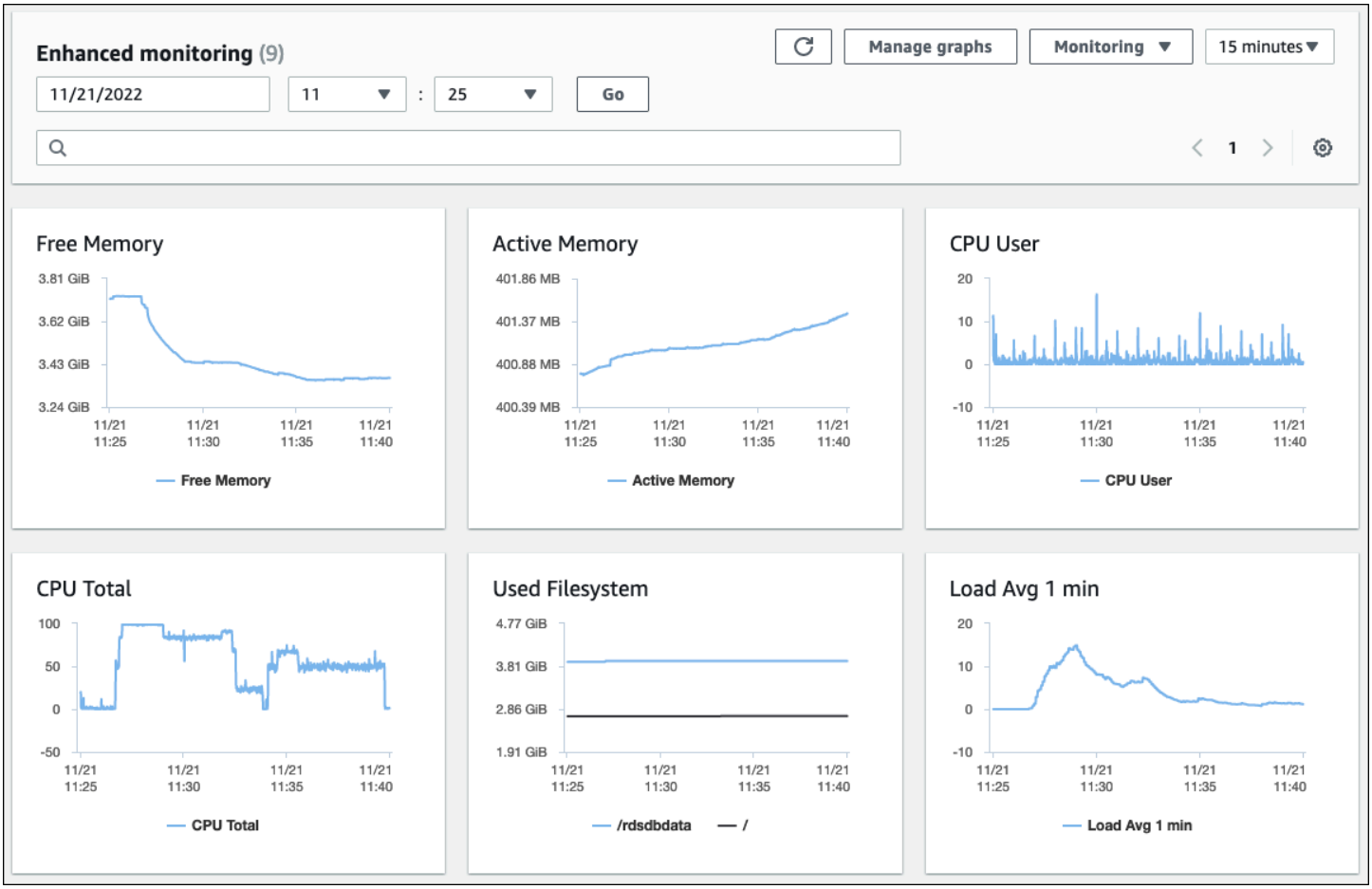
下表顯示 Amazon RDS 主控台上顯示的 Amazon RDS CloudWatch 指標範例。



下圖顯示 CloudWatch 儀表板中顯示的類似指標。



另一組作業系統指標是由 Amazon RDS 的增強型監控收集。此工具提供即時系統指標和作業系統程序資訊，讓您更深入了解 Amazon RDS for MariaDB 和 Amazon RDS for MySQL 資料庫執行個體的運作狀態。當您在資料庫執行個體上啟用增強型監控並設定所需的精細程度時，工具會收集作業系統指標和程序資訊，您可以在 Amazon RDS 主控台上顯示和分析這些資訊，如下畫面所示。



增強型監控提供的一些關鍵指標包括：

- `cpuUtilization.total` – 使用中 CPU 的總百分比。
- `cpuUtilization.user` – 使用者程式使用的 CPU 百分比。
- `memory.active` – 指派的記憶體數量，以 KB 為單位。
- `memory.cached` – 用於快取檔案系統型 I/O 的記憶體量。
- `loadAverageMinute.one` – 最後一分鐘內請求 CPU 時間的程序數目。

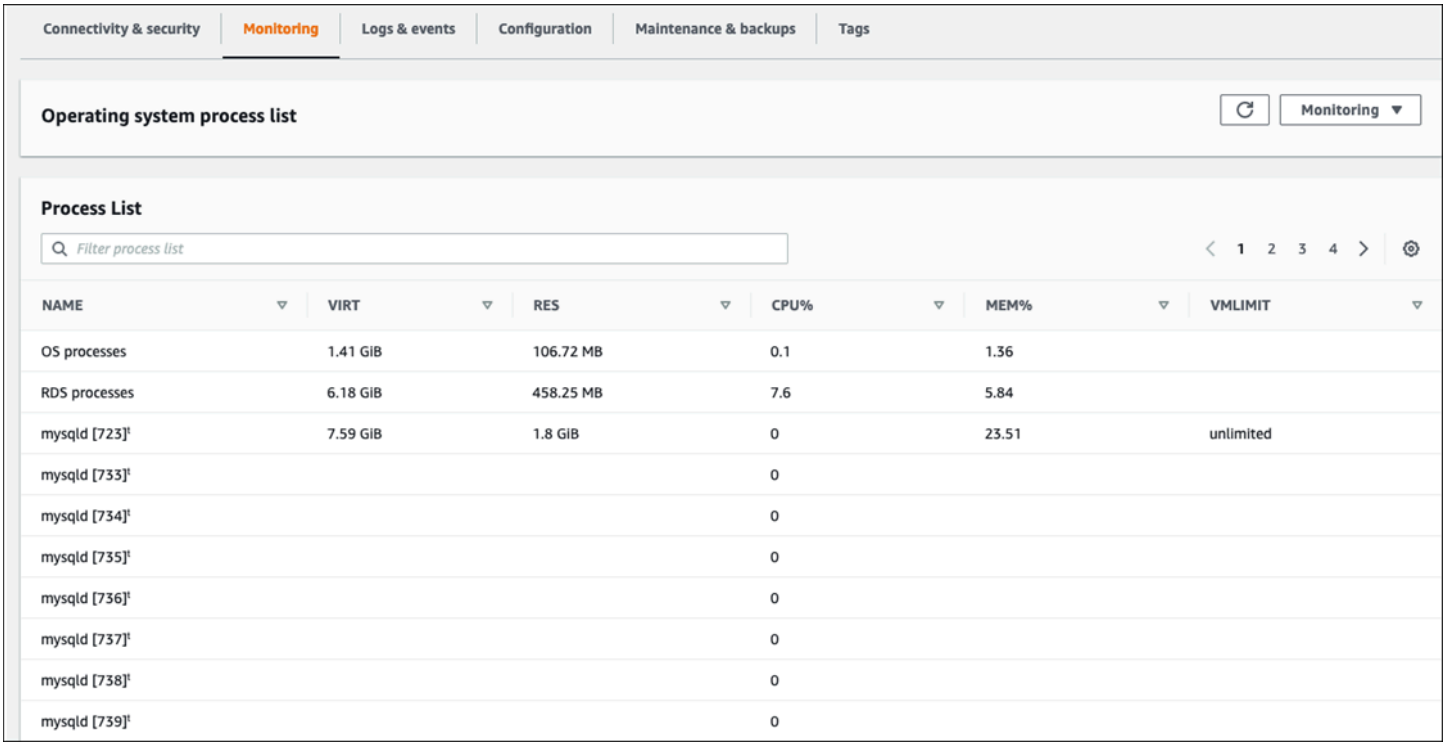
如需指標的完整清單，請參閱 Amazon RDS 文件中的增強型監控中的作業系統指標。

在 Amazon RDS 主控台上，作業系統程序清單會提供資料庫執行個體中執行之每個程序的詳細資訊。清單分為三個部分：

- 作業系統程序 – 本節代表所有核心和系統程序的彙總摘要。這些程序通常對資料庫效能的影響最小。

- RDS 程序 – 本節代表支援 Amazon RDS 資料庫執行個體所需的 AWS 程序摘要。例如，它包含 Amazon RDS 管理代理程式、監控和診斷程序，以及類似的程序。
- RDS 子程序 – 本節代表支援資料庫執行個體的 Amazon RDS 程序摘要，在此情況下為`mysqld`程序及其執行緒。`mysqld` 執行緒會在父`mysqld`程序下方巢狀顯示。

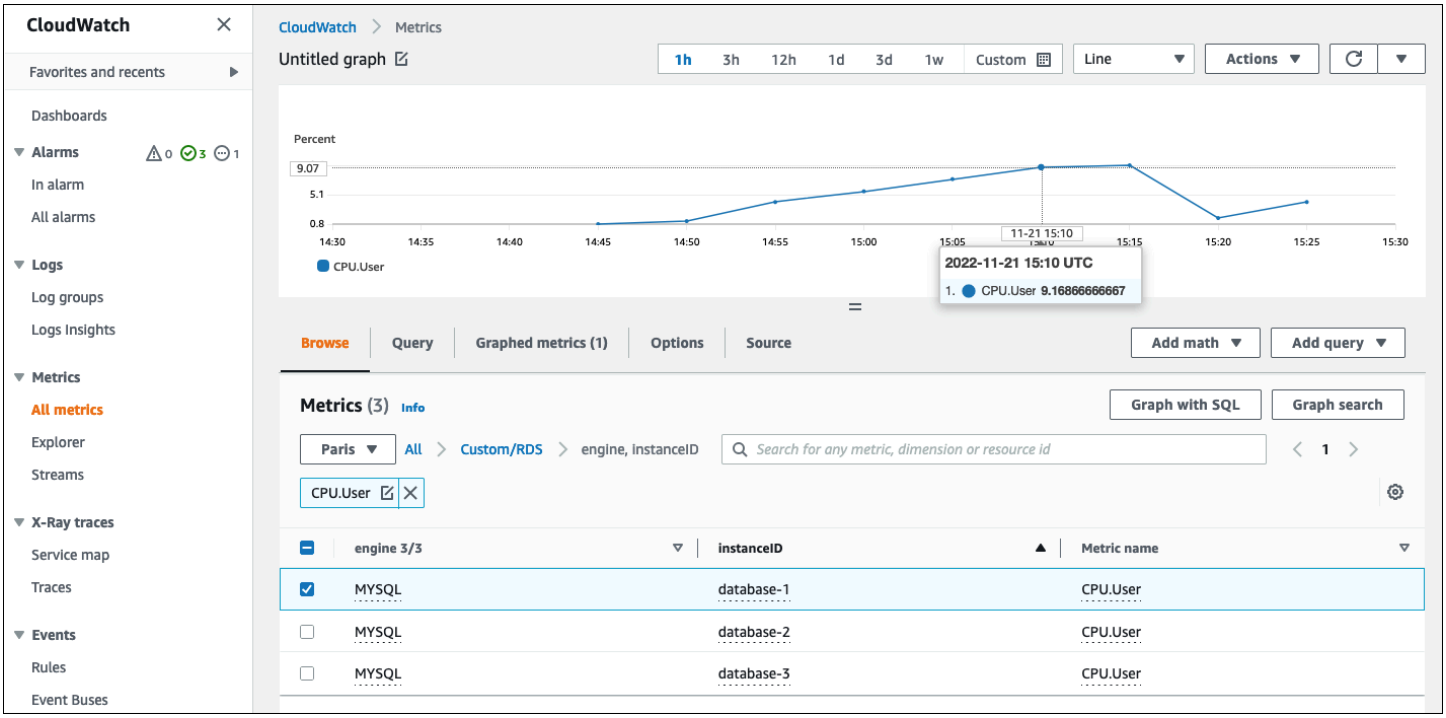
下圖顯示 Amazon RDS 主控台中的作業系統程序清單。



Amazon RDS 從增強型監控將指標交付到您的 CloudWatch Logs 帳戶。Amazon RDS 主控台上顯示的監控資料會從 CloudWatch Logs 擷取。您也可以從 CloudWatch Logs 擷取資料庫執行個體的指標做為日誌串流。這些指標會以 JSON 格式儲存。您可以在您所選的監控系統中，使用來自 CloudWatch Logs 的增強型監控 JSON 輸出。

為了在 CloudWatch 儀表板上顯示圖形並建立警示，以便在指標超過定義的閾值時啟動動作，您必須在 CloudWatch CloudWatch Logs 中建立指標篩選條件。如需詳細說明，請參閱 AWS re：Post 文章，了解如何篩選增強型監控 CloudWatch Logs，以產生 Amazon RDS 的自動自訂指標。

下列範例說明 `Custom/RDS` 命名空間`CPU.User`中的自訂指標。此自訂指標是透過從 CloudWatch Logs 篩選`cpuUtilization.user`增強型監控指標來建立。



當 CloudWatch 儲存庫中有指標可用時，您可以在 CloudWatch 儀表板中顯示和分析指標、套用進一步的數學和查詢操作，並設定警示來監控此特定指標，並在觀察到的值不符合定義的警示條件時產生警示。

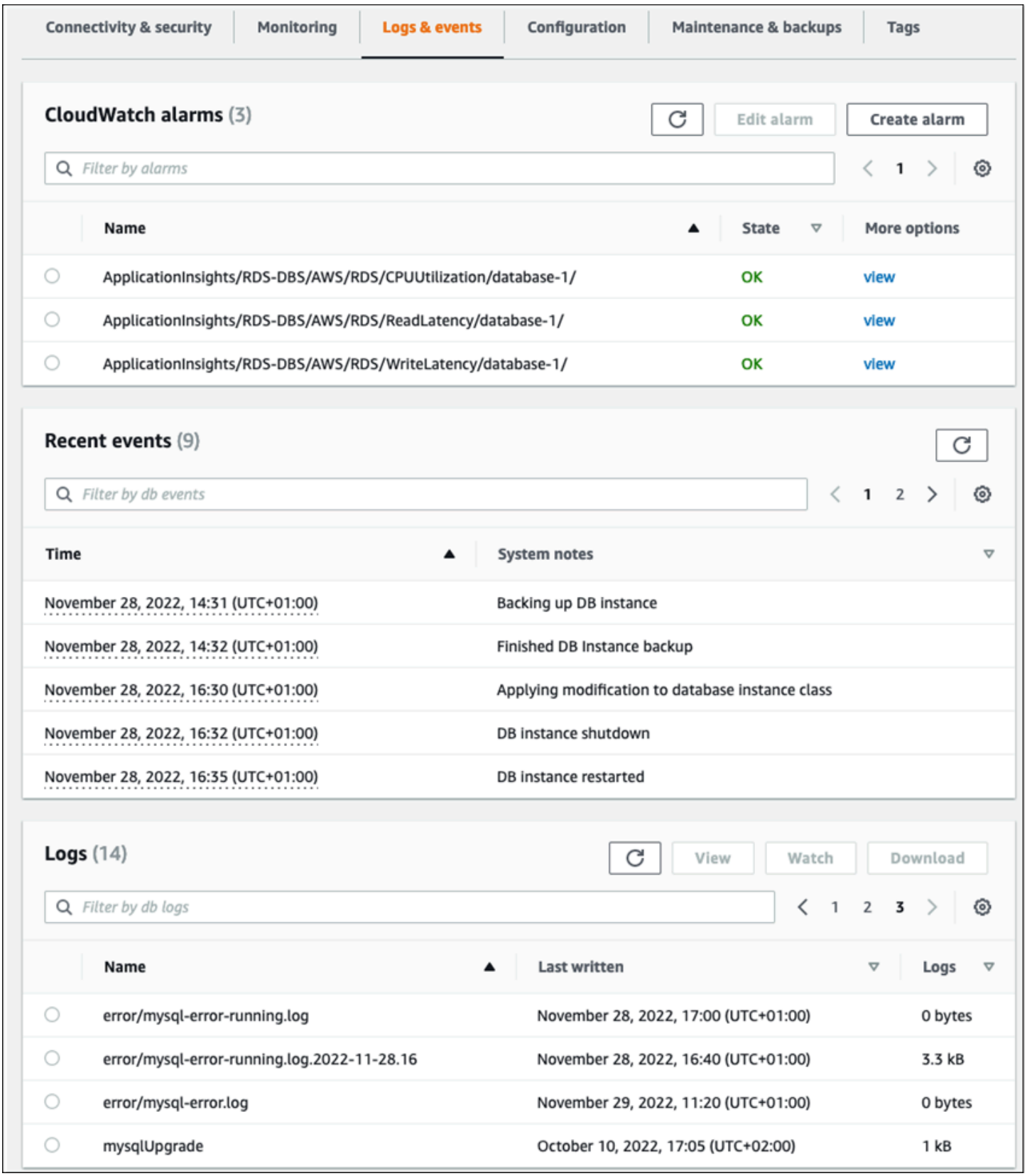
事件、日誌和稽核追蹤

監控資料庫執行個體指標和作業系統指標、分析趨勢並將指標與基準值進行比較，以及在值超出定義的閾值時產生警示，這些都是協助您實現和維護 Amazon RDS 資料庫執行個體可靠性、可用性、效能和安全性的必要最佳實務。不過，完整的解決方案也必須監控 MySQL 和 MariaDB 資料庫的資料庫事件、日誌檔案和稽核線索。

章節

Amazon RDS 事件

Amazon RDS 事件表示 Amazon RDS 環境中的變更。例如，當資料庫執行個體狀態從開始變更為可用時，Amazon RDS 會產生事件 `RDS-EVENT-0088 The DB instance has been started`。Amazon RDS 會以近乎即時的方式將事件交付至 Amazon EventBridge。您可以透過 Amazon RDS 主控台、 AWS CLI 命令 describe-events 或 Amazon RDS API 操作 DescribeEvents 存取事件。下列畫面圖顯示 Amazon RDS 主控台上顯示的事件和日誌。


Connectivity & security
Monitoring
Logs & events
Configuration
Maintenance & backups
Tags
CloudWatch alarms (3)
Edit alarm
Create alarm
Filter by alarms
1
Name
State
More options
ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/
OK
view
Recent events (9)
Filter by db events
1
2
Time
System notes
November 28, 2022, 14:31 (UTC+01:00)
Backing up DB instance
November 28, 2022, 14:32 (UTC+01:00)
Finished DB Instance backup
November 28, 2022, 16:30 (UTC+01:00)
Applying modification to database instance class
November 28, 2022, 16:32 (UTC+01:00)
DB instance shutdown
November 28, 2022, 16:35 (UTC+01:00)
DB instance restarted
Logs (14)
View
Watch
Download
Filter by db logs
1
2
3
Name
Last written
Logs
error/mysql-error-running.log
November 28, 2022, 17:00 (UTC+01:00)
0 bytes
error/mysql-error-running.log.2022-11-28.16
November 28, 2022, 16:40 (UTC+01:00)
3.3 kB
error/mysql-error.log
November 29, 2022, 11:20 (UTC+01:00)
0 bytes
mysqlUpgrade
October 10, 2022, 17:05 (UTC+02:00)
1 kB

Amazon RDS 會發出不同類型的事件，包括資料庫執行個體事件、資料庫參數群組事件、資料庫安全群組事件、資料庫快照事件、RDS Proxy 事件，以及藍/綠部署事件。資訊包括：

- 來源名稱和來源類型；例如：`"SourceIdentifier": "database-1", "SourceType": "db-instance"`
- 事件的日期和時間；例如：`"Date": "2022-12-01T09:20:28.595000+00:00"`
- 與事件相關聯的訊息；例如：`"Message": "Finished updating DB parameter group"`
- 事件類別；例如：`"EventCategories": ["configuration change"]`

如需完整參考，請參閱 Amazon RDS 文件中的 Amazon RDS 事件類別和事件訊息。

我們建議您監控 Amazon RDS 事件，因為這些事件指出資料庫執行個體可用性的狀態變更、組態變更、僅供讀取複本狀態變更、備份和復原事件、容錯移轉動作、失敗事件、安全群組的修改，以及許多其他通知。例如，如果您已設定僅供讀取複本資料庫執行個體，為資料庫提供增強的效能和耐用性，我們建議您監控與資料庫執行個體相關聯的僅供讀取複本事件類別的 Amazon RDS 事件。這是因為等事件`RDS-EVENT-0057 Replication on the read replica was terminated`表示您的僅供讀取複本不再與主要資料庫執行個體同步。向負責團隊通知此類事件已發生，有助於及時緩解問題。Amazon EventBridge 和其他 AWS 服務，例如 AWS Lambda Amazon Simple Queue Service (Amazon SQS) 和 Amazon Simple Notification Service (Amazon SNS)，可協助您自動回應資料庫可用性問題或資源變更等系統事件。

在 Amazon RDS 主控台上，您可以擷取過去 24 小時內的事件。如果您使用 AWS CLI 或 Amazon RDS API 來檢視事件，您可以使用 describe-events 命令擷取過去 14 天內的事件，如下所示。

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "CloudWatch Logs Export enabled for logs [audit, error, general,
 slowquery]",
            "EventCategories": [],
            "Date": "2022-12-01T09:20:28.595000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        },
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
```

```
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

如果您想要長期存放事件，直到指定的過期期間或永久存放，您可以使用 CloudWatch Logs 記錄 Amazon RDS 所產生事件的相關資訊。若要實作此解決方案，您可以使用 Amazon SNS 主題來接收 Amazon RDS 事件通知，然後呼叫 Lambda 函數在 CloudWatch Logs 中記錄事件。

1. 建立將在事件上呼叫的 Lambda 函數，並將事件中的資訊記錄到 CloudWatch Logs。CloudWatch Logs 已與 Lambda 整合，並透過將列印函數用於 ，提供記錄事件資訊的便利方式`stdout`。
2. 建立訂閱 Lambda 函數 （將通訊協定設定為 Lambda) 的 SNS 主題，並將端點設定為您在上一個步驟中建立的 Lambda 函數的 Amazon Resource Name (ARN)。
3. 設定您的 SNS 主題以接收 Amazon RDS 事件通知。如需詳細說明，請參閱 AWS re：Post 文章，了解如何取得 Amazon SNS 主題以接收 Amazon RDS 通知。
4. 在 Amazon RDS 主控台上，建立新的事件訂閱。將目標設定為 ARN，然後選取您先前建立的 SNS 主題。根據您的需求設定要包含的來源類型和事件類別。 如需詳細資訊，請參閱 Amazon RDS 文件中的訂閱 Amazon RDS 事件通知。

資料庫日誌

MySQL 和 MariaDB 資料庫會產生您可以存取的日誌，以進行稽核和故障診斷。這些日誌包括：

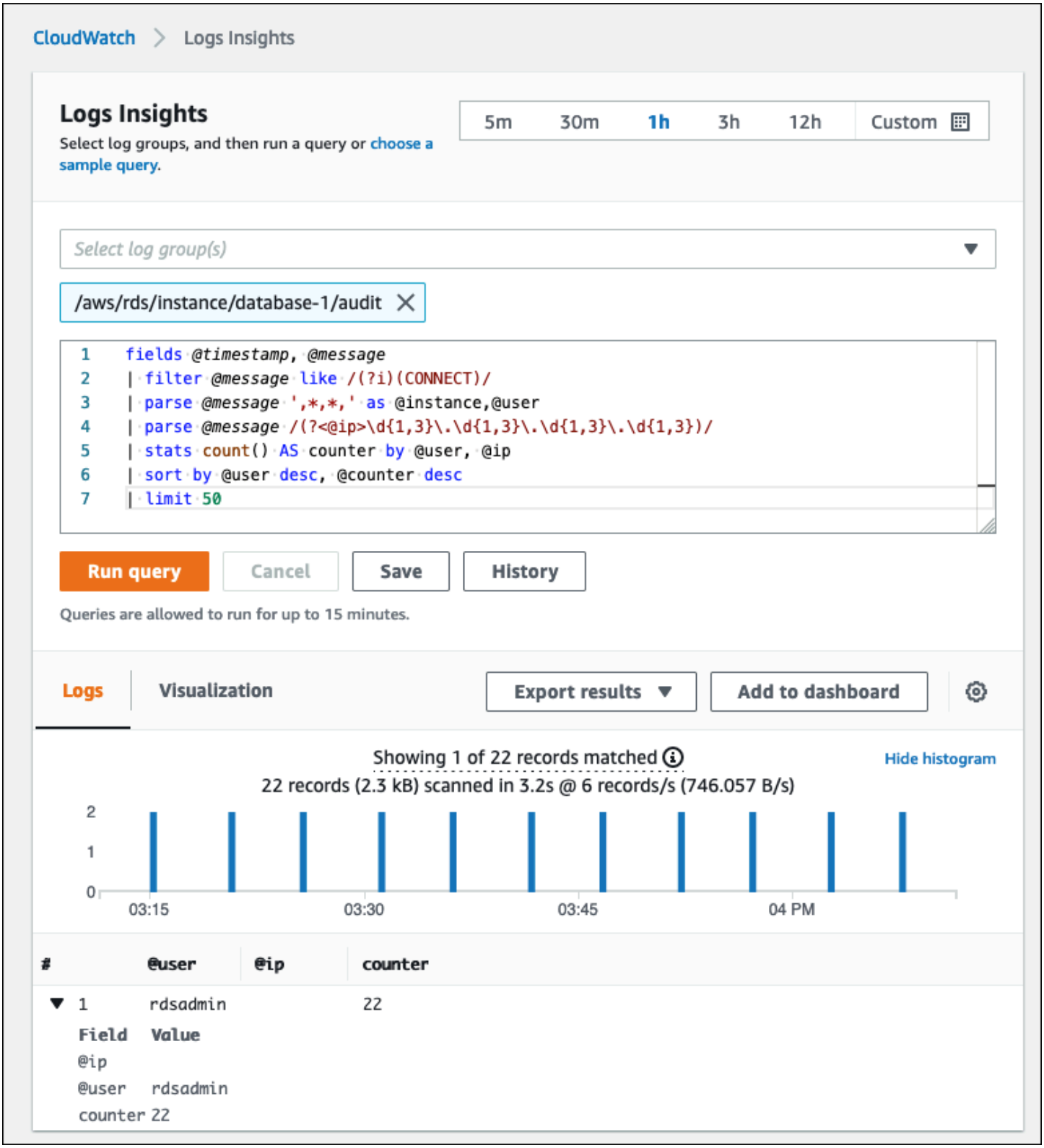
- 稽核 – 稽核線索是一組記錄伺服器活動的記錄。對於每個用戶端工作階段，它會記錄連線至伺服器的人員 （使用者名稱和主機）、執行的查詢、存取的資料表，以及變更的伺服器變數。
- 錯誤 – 此日誌包含伺服器的 (`mysqld`) 啟動和關閉時間，以及診斷訊息，例如在伺服器啟動和關閉期間，以及伺服器執行期間的錯誤、警告和備註。
- 一般 – 此日誌會記錄 的活動`mysqld`，包括每個用戶端的連線和中斷連線活動，以及從用戶端收到的 SQL 查詢。當您懷疑發生錯誤並想知道用戶端傳送至 的內容時，一般查詢日誌非常有用`mysqld`。
- 慢查詢 – 此日誌提供 SQL 查詢的記錄，這些查詢需要很長時間才能執行。

最佳實務是，您應該將資料庫日誌從 Amazon RDS 發佈至 Amazon CloudWatch Logs。使用 CloudWatch Logs，您可以執行日誌資料的即時分析、將資料存放在高耐用性的儲存體中，以及使用

CloudWatch Logs 代理程式管理資料。您可以從 Amazon RDS 主控台存取和監看資料庫日誌。您也可以使用 CloudWatch Logs Insights 以互動方式搜尋和分析 CloudWatch Logs 中的日誌資料。下列範例說明稽核日誌上的查詢，該查詢會檢查CONNECT事件在日誌中出現的次數、連接的對象，以及它們連線的用戶端 (IP 地址）。稽核日誌中的摘錄可能如下所示：

```
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,CONNECT,,,0,SOCKET
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,DISCONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,CONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,DISCONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,CONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,DISCONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,CONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,DISCONNECT,,,0,SOCKET
```

Log Insights 查詢範例顯示`localhost`每 5 分鐘`rdsadmin`連線至資料庫一次，總共 22 次，如下圖所示。這些結果表示活動源自內部 Amazon RDS 程序，例如監控系統本身。



日誌事件經常包含您要計數的重要訊息，例如有關與 MySQL 和 MariaDB 資料庫執行個體相關聯操作的警告或錯誤。例如，如果 操作失敗，可能會發生錯誤，並會記錄到錯誤日誌檔案中，如下所

示：ERROR 1114 (HY000): The table zip_codes is full。您可能想要監控這些項目，以了解您錯誤的趨勢。您可以使用篩選條件從 Amazon RDS 日誌建立自訂 CloudWatch 指標，以啟用 Amazon RDS 資料庫日誌的自動監控，以監控特定模式的特定日誌，並在違反預期行為時產生警示。例如，為日誌群組建立指標篩選條件/aws/rds/instance/database-1/error，以監控錯誤日誌並搜尋特定模式，例如 ERROR。將篩選條件模式設定為 ERROR，並將指標值設定為 1。篩選條件會偵測具有關鍵字 的每個日誌記錄ERROR，並為每個包含 "ERROR" 的日誌事件將計數增加 1。建立篩選條件後，您可以設定警示，在 MySQL 或 MariaDB 錯誤日誌中偵測到錯誤時通知您。

若要進一步了解如何透過建立 CloudWatch 儀表板和使用 CloudWatch Logs Insights 來監控慢查詢日誌和錯誤日誌，請參閱部落格文章建立 Amazon CloudWatch 儀表板以監控 Amazon RDS 和 Amazon Aurora MySQL。

稽核線索

稽核追蹤 （或稽核日誌） 提供 中事件的安全相關時間記錄 AWS 帳戶。它包含 Amazon RDS 的事件，可提供一系列影響資料庫或雲端環境的活動的文件證據。在 Amazon RDS for MySQL 或 MariaDB 中，使用稽核線索涉及：

- 監控資料庫執行個體稽核日誌
- 在 中監控 Amazon RDS API 呼叫 AWS CloudTrail

對於 Amazon RDS 資料庫執行個體，稽核的目標通常包括：

- 啟用下列項目的責任：
  - 在參數或安全組態上執行的修改
  - 在資料庫結構描述、資料表或資料列中執行的動作，或影響特定內容的動作
- 入侵偵測和調查
- 可疑活動偵測和調查
- 偵測授權問題；例如，識別一般或特殊權限使用者濫用的存取權

資料庫稽核線索會嘗試回答下列典型問題：誰檢視或修改了資料庫中的敏感資料？ 何時發生這種情況？ 特定使用者從何處存取資料？ 特殊權限使用者是否濫用其無限制的存取權？

MySQL 和 MariaDB 都使用 MariaDB 稽核外掛程式來實作資料庫執行個體稽核追蹤功能。此外掛程式會記錄資料庫活動，例如使用者登入資料庫，以及對資料庫執行的查詢。資料庫活動的記錄會儲存在日誌檔中。若要存取稽核記錄，資料庫執行個體必須使用含有選項 MARIADB_AUDIT_PLUGIN 的自訂選

項群組。如需詳細資訊，請參閱 Amazon RDS 文件中的 MariaDB 稽核外掛程式對 MySQL 的支援。稽核日誌中的記錄會以特定格式儲存，如 外掛程式所定義。您可以在 MariaDB Server 文件中找到有關稽核日誌格式的詳細資訊。

您 AWS 帳戶的 AWS 雲端 稽核線索是由 AWS CloudTrail服務提供。CloudTrail 會擷取 Amazon RDS 的 API 呼叫當作事件。會記錄所有 Amazon RDS 動作。CloudTrail 提供由使用者、角色或其他 AWS 服務在 Amazon RDS 中執行的動作記錄。事件包括在 AWS 管理主控台中採取的動作 AWS CLI，以及 AWS SDKs和 APIs。

範例

在典型的稽核案例中，您可能需要結合 AWS CloudTrail 追蹤與資料庫稽核日誌和 Amazon RDS 事件監控。例如，您可能會遇到 Amazon RDS 資料庫執行個體的資料庫參數 （ 例如 `database-1`) 已修改的情況，而您的任務是識別修改的人員、變更的內容，以及變更發生的時間。

若要完成任務，請遵循下列步驟：

1. 列出資料庫執行個體發生的 Amazon RDS 事件，`database-1`並判斷類別中是否有`configuration change`具有訊息 的事件`Finished updating DB parameter group`。

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

2. 識別資料庫執行個體正在使用的資料庫參數群組：

```
$ aws rds describe-db-instances --db-instance-identifier database-1 --query
 'DBInstances[*].[DBInstanceIdentifier,Engine,DBParameterGroups]'
[
    [
```

```
        "database-1",
        "mariadb",
        [
            {
                "DBParameterGroupName": "mariadb10-6-test",
                "ParameterApplyStatus": "pending-reboot"
            }
        ]
    ]
]
```

3. 使用 AWS CLI 在部署的 區域中、步驟 1 中探索的 Amazon RDS 事件前後的期間內，以及 所在的中搜尋 CloudTrail 事件EventName=ModifyDBParameterGroup。database-1

```
$ aws cloudtrail --region eu-west-3 lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=ModifyDBParameterGroup --start-time
 "2022-12-01, 09:00 AM" --end-time "2022-12-01, 09:30 AM"

{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Role1",
                "accountId": "111122223333",
                "userName": "User1"
            }
        }
    },
    "eventTime": "2022-12-01T09:18:19Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "ModifyDBParameterGroup",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "parameters": [
            {
                "isModifiable": false,
```

```
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_log_buffer_size",
                "parameterValue": "8388612"
            },
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_write_io_threads",
                "parameterValue": "8"
            }
        ],
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "responseElements": {
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "requestID": "fdf19353-de72-4d3d-bf29-751f375b6378",
    "eventID": "0bba7484-0e46-4e71-93a8-bd01ca8386fe",
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```


CloudTrail 事件顯示，User1帳戶 111122223333 Role1中 AWS 具有 角色的 已修改資料庫參數群組 mariadb10-6-test，該群組由 database-1上的資料庫執行個體使用2022-12-01 at 09:18:19 h。已修改兩個參數，並設定為下列值：

- innodb_log_buffer_size = 8388612
- innodb_write_io_threads = 8

其他 CloudTrail 和 CloudWatch Logs 功能

您可以在 CloudTrail 主控台上檢視事件歷史記錄，對過去 90 天內的操作和安全性事件進行疑難排解。若要延長保留期並利用其他查詢功能，您可以使用 AWS CloudTrail Lake。使用 AWS CloudTrail Lake，您可以在事件資料存放區中保留事件資料長達七年。此外，此服務支援複雜的 SQL 查詢，可提供比事件歷史記錄中簡單鍵值查詢提供的檢視更深入且更可自訂的事件檢視。

若要監控稽核線索、設定警示，並在特定活動發生時取得通知，您需要設定 CloudTrail 將其線索記錄傳送至 CloudWatch Logs。將追蹤記錄儲存為 CloudWatch Logs 之後，您可以定義指標篩選條件來評估日誌事件以符合詞彙、片語或值，並將指標指派給指標篩選條件。此外，您可以建立 CloudWatch 警示，這些警示會根據您指定的閾值和期間產生。例如，您可以設定警示，將通知傳送給負責的團隊，讓他們可以採取適當的動作。您也可以設定 CloudWatch 自動執行動作，以回應警示。

提醒

在 IT 基礎設施和 IT 服務的安全性、可用性、效能和可靠性方面，警示是最重要的資訊來源之一。它們會通知並通知 IT 團隊持續的安全威脅、中斷、效能問題或系統故障。

Information Technology Infrastructure Library (ITIL)，特別是 IT 服務管理 (ITSM) 實務，在監控和事件管理和事件管理最佳實務的焦點設定自動提醒。

事件警示是指監控工具產生警示，以通知您的團隊和自動化工具（適用於可自動採取行動的項目）有關 IT 環境中的變更、高風險動作或故障。IT 警示是防範系統中斷或可能成為重大事件變更的第一道防線。透過自動監控系統和產生中斷和風險變更的提醒，IT 團隊可以將停機時間降至最低，並降低伴隨的昂貴成本。

做為最佳實務， AWS Well-Architected Framework 會指定您使用監控來產生警示型通知，並主動監控和警示。使用 CloudWatch 或第三方監控服務來設定警示，指出指標何時超出預期界限。

警示管理的目的是透過記錄、分類、動作定義和實作、關閉和事件後審核活動，建立高效且標準化的程序來處理 IT 相關事件和事件。

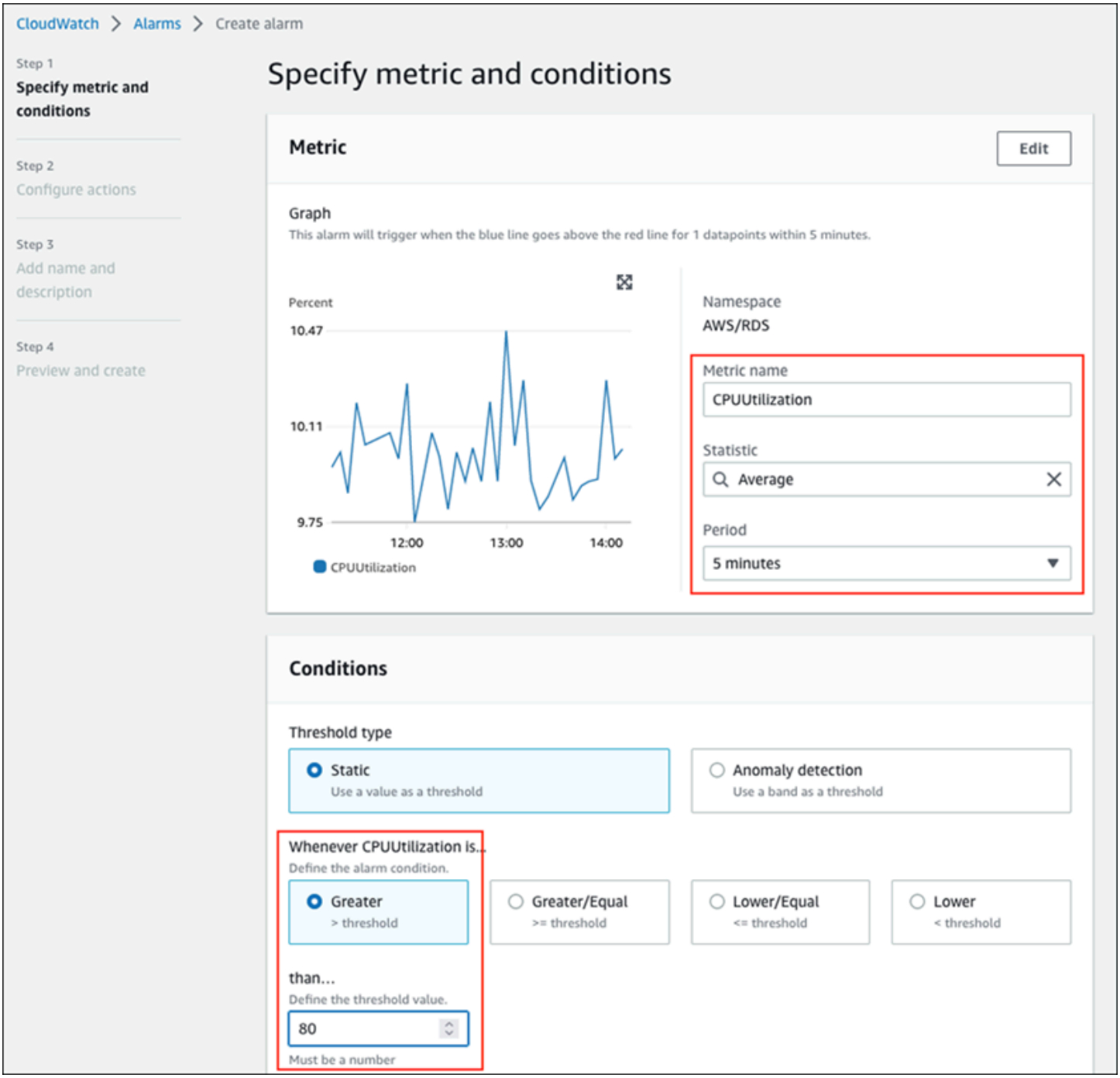
章節

- CloudWatch 警示
- EventBridge 規則
- 指定動作、啟用和停用警示

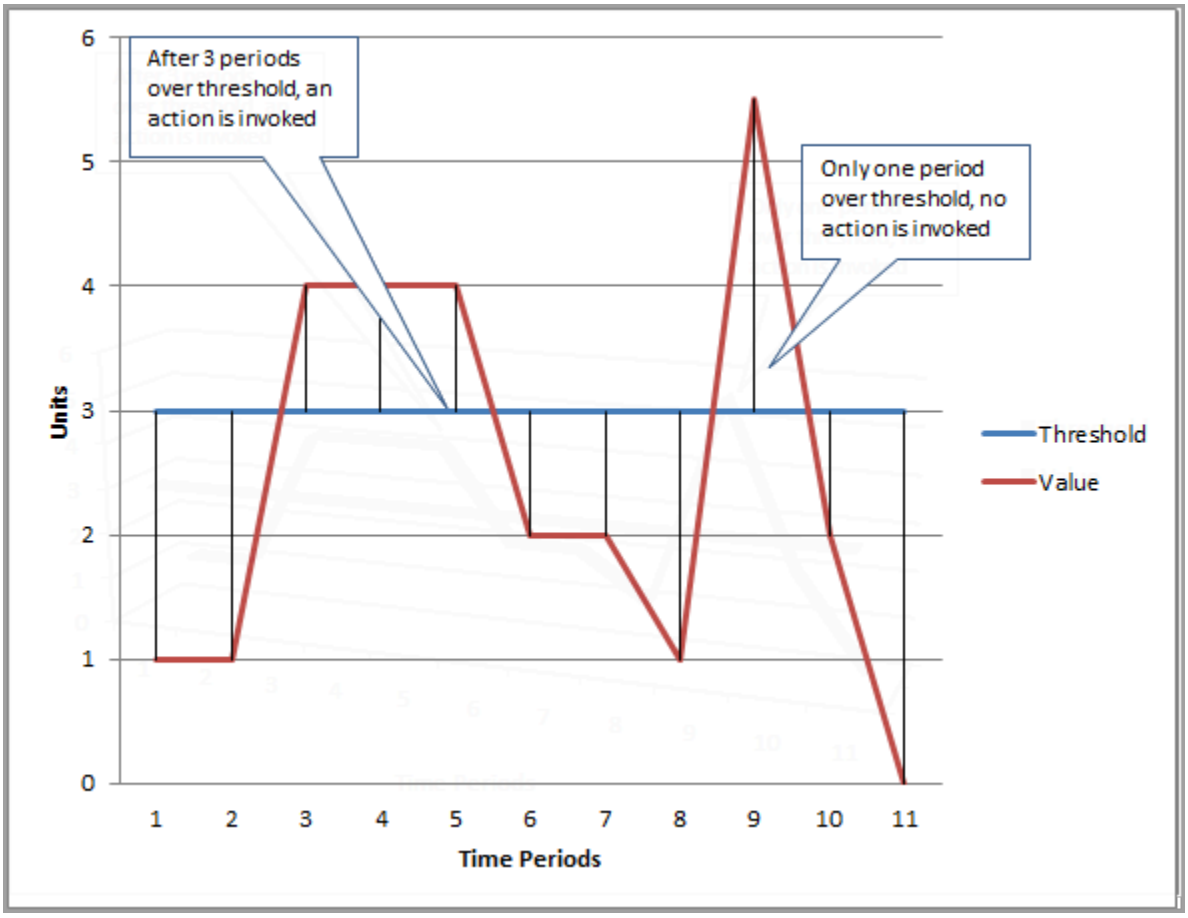
CloudWatch 警示

當您操作 Amazon RDS 資料庫執行個體時，您想要監控和產生不同類型指標、事件和追蹤的提醒。對於 MySQL 和 MariaDB 資料庫，關鍵資訊來源是資料庫執行個體指標、作業系統指標、事件、日誌和稽核線索。我們建議您使用 CloudWatch 警示，在您指定的期間內監看單一指標。

下列範例說明如何設定警示，以監控所有 `CPUUtilization` Amazon RDS 資料庫執行個體上的指標 (CPU 使用率百分比）。如果任何資料庫執行個體上的 CPU 使用率在 5 分鐘的評估期間內大於 80%，您可以將警示設定為觸發。



這表示如果您的任何資料庫經歷 5 分鐘或更長時間的高 CPU 使用率 （超過 80%），警示會進入 ALARM 狀態。如果 CPU 在短時間內偶爾爆增到超過 80% 的使用率，然後再次低於閾值，則警示會保持在 OK 狀態。下圖說明此邏輯。



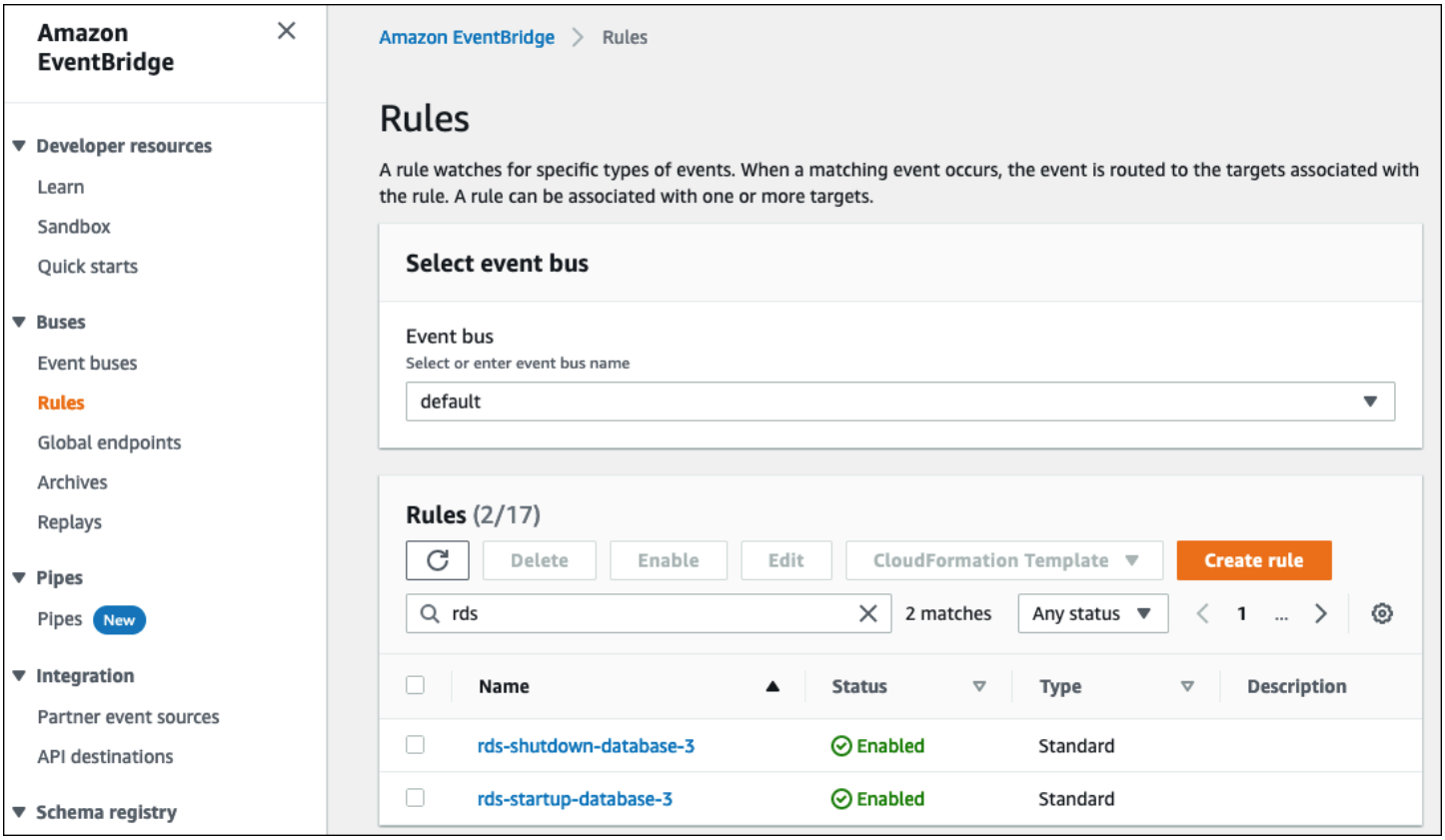
CloudWatch 警示支援指標和複合警示。

- 指標警示會監看單一 CloudWatch 指標，並可在指標上執行數學表達式。指標警示可以傳送 Amazon SNS 訊息，進而根據指標在多個期間內相對於指定閾值的值，採取一或多個動作。
- 複合警示是以規則表達式為基礎，該表達式會評估多個警示的狀態，並且只有在符合規則的所有條件時，才會進入 ALARM 狀態。複合警示通常用於減少不必要的警示數量。例如，您可能有一個複合警示，其中包含數個已設定永遠不會採取動作的指標警示。當複合中的所有個別指標警示都已在 中時，複合警示會傳送警示 ALARM

CloudWatch 警示只能監看 CloudWatch 指標。如果您想要根據錯誤、慢查詢或一般日誌建立警示，您必須從日誌建立 CloudWatch 指標。您可以使用篩選條件從日誌事件建立指標，如先前在作業系統監控和事件、日誌和稽核追蹤區段中所討論。同樣地，若要提醒增強型監控指標，您必須在 CloudWatch Logs 的 CloudWatch 中建立指標篩選條件。

EventBridge 規則

Amazon RDS 事件會交付至 Amazon EventBridge，您可以使用 EventBridge 規則來回應這些事件。例如，您可以建立 EventBridge 規則來通知您，並在某個特定資料庫執行個體停止或啟動時採取動作，如下畫面所示。

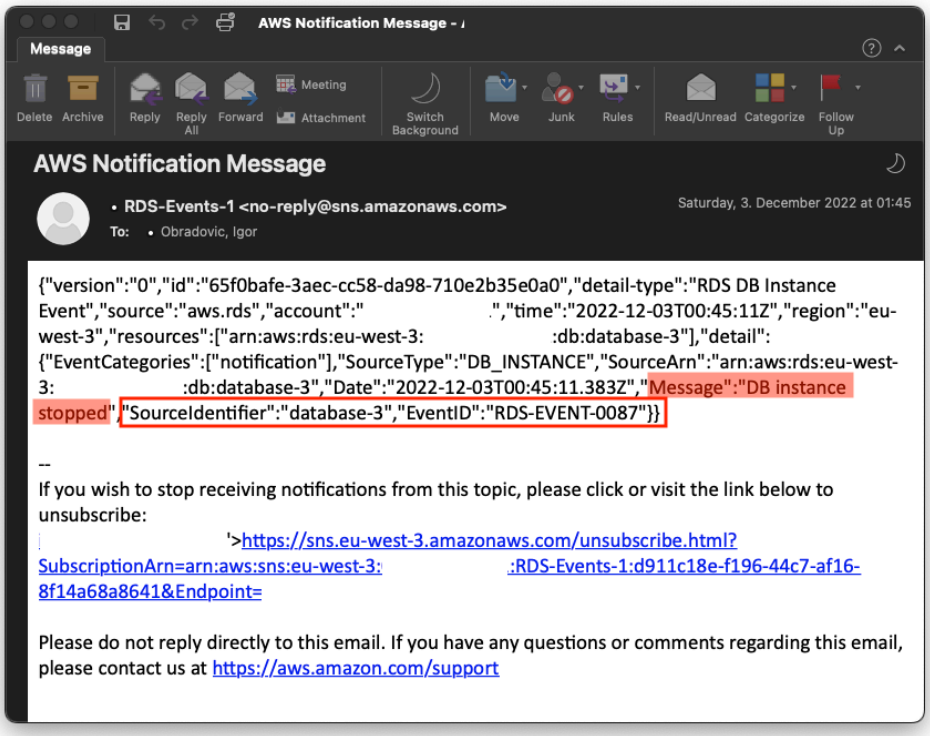


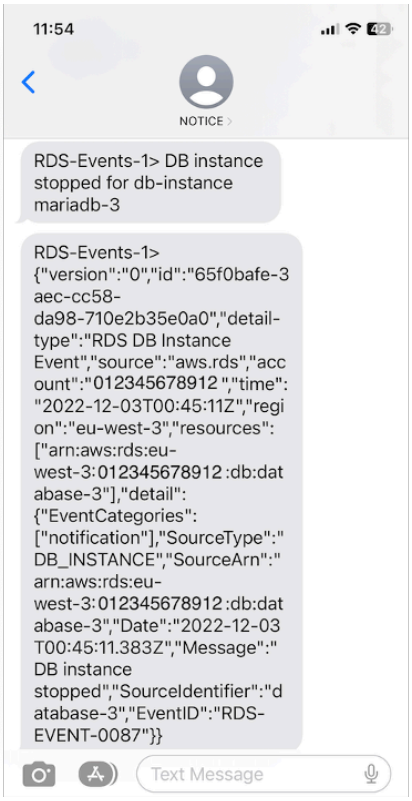
偵測The DB instance has been stopped事件的規則具有 Amazon RDS 事件 ID RDS-EVENT-0087，因此您可以將規則的 Event Pattern 屬性設定為：

```
{
  "source": ["aws.rds"],
  "detail-type": ["RDS DB Instance Event"],
  "detail": {
    "SourceArn": ["arn:aws:rds:eu-west-3:111122223333:db:database-3"],
    "EventID": ["RDS-EVENT-0087"]
  }
}
```

此規則database-3只會監控資料庫執行個體，並監看RDS-EVENT-0087事件。當 EventBridge 偵測到事件時，它會將事件傳送至資源或端點，稱為目標。您可以在此指定在 Amazon RDS 執行個

體關閉時要採取的動作。您可以將事件傳送至許多可能的目標，包括 SNS 主題、Amazon Simple Queue Service (Amazon SQS) 佇列、 AWS Lambda 函數、 AWS Systems Manager Automation、AWS Batch 任務、Amazon API Gateway 等。例如，您可以建立傳送通知電子郵件和 SMS 的 SNS 主題，並將該 SNS 主題指派為 EventBridge 規則的目標。如果 Amazon RDS 資料庫執行個體`database-3`已停止，Amazon RDS 會將事件交付`RDS-EVENT-0087`至 EventBridge，並在其中偵測到事件。EventBridge 接著會呼叫目標，也就是 SNS 主題。SNS 主題設定為傳送電子郵件 （如下圖所示） 和 SMS。





指定動作、啟用和停用警示

您可以使用 CloudWatch 警示來指定警示在 `OK`、 `ALARM`和 `INSUFFICIENT_DATA` 狀態之間變更時應採取的動作。CloudWatch 內建與 SNS 主題的整合，以及數個不適用於 Amazon RDS 指標的其他動作類別，例如 Amazon Elastic Compute Cloud (Amazon EC2) 動作或 Amazon EC2 Auto Scaling 群組動作。EventBridge 通常用於撰寫規則，並定義在 Amazon RDS 指標觸發警示時採取動作的目標。CloudWatch 每次 CloudWatch 警示變更其狀態時，都會將事件傳送至 EventBridge。您可使用這些警示狀態變更事件在 EventBridge 中觸發事件目標。如需詳細資訊，請參閱 CloudWatch 文件中的警示事件和 EventBridge。

您可能還需要管理警示；例如，在計劃的組態變更或測試期間自動停用警示，然後在計劃動作結束時重新啟用警示。例如，如果您有計劃、排程的資料庫軟體升級需要停機時間，而且有警示會在資料庫

無法使用時啟用，您可以使用 API 動作 DisableAlarmActions 和 EnableAlarmActions 或 中的 disable-alarm-actions 和 enable-alarm-actions 命令來停用和啟用警示 AWS CLI。您也可以在 CloudWatch 主控台或使用 DescribeAlarmHistory API 動作或 中的 describe-alarm-history 命令來檢視警示的歷史記錄 AWS CLI。CloudWatch 會保留警示歷史記錄 2 週。在 CloudWatch 主控台上，您可以選擇導覽窗格中的我的最愛和最近選單，以設定和存取您最愛的和最近瀏覽的警示。

後續步驟和資源

如需將關聯式資料庫遷移至 的詳細資訊 AWS 雲端，請參閱 AWS 規範指引網站上的下列策略：

- 關聯式資料庫的遷移策略

您可以在AWS 規範性指引中探索資料庫遷移模式，以取得在 中執行之特定關聯式資料庫step-by-step說明 AWS 雲端，包括與監控、遷移和資料管理相關的任務。

如需其他資源，請參閱下列內容：

- Amazon Relational Database Service 使用者指南
- 《Amazon CloudWatch 使用者指南》https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
- Amazon RDS FAQs
- 績效詳情FAQs
- 使用 Amazon CloudWatch Metrics Stream 將 Amazon RDS Performance Insights 計數器指標交付給第三方應用程式效能監控服務提供者 (AWS 部落格文章）
- 建立 Amazon CloudWatch 儀表板來監控 Amazon RDS 和 Amazon Aurora MySQL (AWS 部落格文章）
- 使用績效詳情調校 Amazon RDS for MySQL (AWS 部落格文章）

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
已更新績效詳情的相關資訊	以最新資訊更新有關將績效詳情指標發佈至 CloudWatch 的章節。	2025 年 3 月 11 日
更新匯出工具的相關資訊	更新匯出工具的相關資訊，並新增選擇匯出工具的指導方針。	2024 年 6 月 13 日
初次出版	—	2023 年 6 月 30 日

AWS 規範性指引詞彙表

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

數字

7 R

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

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

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

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

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，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。目標資料庫在遷移期間不接受任何交易。

彙總函數

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

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

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

反模式

經常用於經常性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

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

人工智慧 (AI)

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

人工智慧操作 (AIOps)

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

非對稱加密

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

原子性、一致性、隔離性、耐久性 (ACID)

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

屬性型存取控制 (ABAC)

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

授權資料來源

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

可用區域

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

AWS 雲端採用架構 (AWS CAF)

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

AWS 工作負載資格架構 (AWS WQF)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

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

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

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

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

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

機器人

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

殭屍網路

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

分支

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

碎片存取

在特殊情況下，並透過核准的程序，讓使用者快速取得他們通常無權存取 AWS 帳戶 之 的存取權。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

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

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

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

業務連續性規劃 (BCP)

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

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

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

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

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

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行試驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

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

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

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

雲端運算

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

雲端操作模型

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

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)

- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

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

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

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

冷快取

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

冷資料

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

電腦視覺 (CV)

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

組態偏離

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

組態管理資料庫 (CMDB)

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

一致性套件

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

持續整合和持續交付 (CI/CD)

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

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

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

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

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

資料周邊

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

資料預先處理

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

資料來源

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

資料主體

正在收集和處理其資料的個人。

資料倉儲

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

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

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

深度學習

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

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

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

deployment

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

開發環境

請參閱 環境。

偵測性控制

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

開發值串流映射 (DVSM)

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

數位分身

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

維度資料表

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

災難

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

災難復原 (DR)

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

DML

請參閱資料庫處理語言。

領域驅動的設計

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

DR

請參閱災難復原。

偏離偵測

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

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

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

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

將人類可讀取的純文字資料轉換為加密文字的運算程序。

加密金鑰

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

端序

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

端點

請參閱 服務端點。

端點服務

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

企業資源規劃 (ERP)

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

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

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

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實資料表

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

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

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

功能分支

請參閱分支。

特徵

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

功能重要性

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

特徵轉換

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

少量擷取提示

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

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

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

FM

請參閱基礎模型。

基礎模型 (FM)

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

G

生成式 AI

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

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

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

Gitflow 工作流程

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

黃金影像

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

綠地策略

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

防護機制

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

H

HA

請參閱高可用性。

異質資料庫遷移

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

高可用性 (HA)

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

歷史現代化

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

保留資料

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

異質資料庫遷移

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

熱資料

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

修補程序

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

超級護理期間

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

I

IaC

將基礎設施視為程式碼。

身分型政策

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

閒置應用程式

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

IIoT

請參閱工業物聯網。

不可變的基礎設施

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

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 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

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

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

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

工業物聯網 (IIoT)

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

檢查 VPC

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

物聯網 (IoT)

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

可解釋性

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

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

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

IT 服務管理 (ITSM)

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

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

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

登陸區域

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

大型語言模型 (LLM)

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

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

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

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

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

主要分支

請參閱分支。

惡意軟體

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

受管服務

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

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

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

成員帳戶

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

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

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

微服務

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

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行

更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

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

遷移工廠

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

遷移中繼資料

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

遷移模式

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

遷移組合評定 (MPA)

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

遷移準備程度評定 (MRA)

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

遷移策略

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

機器學習 (ML)

請參閱機器學習。

現代化

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

現代化準備程度評定

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

單一應用程式 (單一)

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

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

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

可變基礎設施

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

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

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

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

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

操作水準協議 (OLA)

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

操作整備審查 (ORR)

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

操作技術 (OT)

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

操作整合 (OI)

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

組織追蹤

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

組織變更管理 (OCM)

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

原始存取控制 (OAC)

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

原始存取身分 (OAI)

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

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

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

P

許可界限

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

個人身分識別資訊 (PII)

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

PII

請參閱個人身分識別資訊。

手冊

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

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

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

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則可以更輕鬆地實作並達到更好的效能和可擴展性。

組合評定

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

述詞

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

述詞下推

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

預防性控制

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

委託人

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

設計隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

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

主動控制

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

產品生命週期管理 (PLM)

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

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

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

擬匿名化

以預留位置值取代資料集中個人識別符的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

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

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

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

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強生成。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

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

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

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

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

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

迴歸

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

重新託管

請參閱 7 Rs。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新放置

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

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

資源型政策

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

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

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

回應性控制

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

保留

請參閱 7 個 R。

淘汰

請參閱 7 Rs。

檢索增強生成 (RAG)

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

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

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

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

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

S

SAML 2.0

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

斯卡達

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

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

依設計的安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

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

安全強化

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

安全資訊與事件管理 (SIEM) 系統

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

安全回應自動化

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

伺服器端加密

由 AWS 服務 接收資料的 在其目的地加密資料。

服務控制政策 (SCP)

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

服務端點

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

服務水準協議 (SLA)

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

服務層級指標 (SLI)

服務效能層面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

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

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

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

SPOF

請參閱單一故障點。

星狀結構描述

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

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

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

系統提示

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

T

標籤

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

目標變數

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

任務清單

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

測試環境

請參閱 環境。

訓練

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

傳輸閘道

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

主幹型工作流程

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

受信任的存取權

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

調校

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

雙比薩團隊

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

U

不確定性

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

未區分的任務

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

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

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

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

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

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等緩慢的查詢。

視窗函數

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

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

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

WORM

請參閱寫入一次，多次讀取。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

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

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

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

零鏡頭提示

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

殭屍應用程式

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

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。