適用於 MySQL 和 MariaDB 的 Amazon RDS for MySQL 的監控和警示工具和最佳實務

AWS 規定指引

AWS 規定指引: 適用於 MySQL 和 MariaDB 的 Amazon RDS for MySQL 的監控和警示工具和最佳實務

Table of Contents

適用於 MySQL 和 MariaDB 的亞馬遜 RDS 的監控和警示工具和最佳實務

伊戈爾·奧布拉多維奇，亞馬遜 Web 服務（AWS）

二零二三年六月(文件歷史)

資料庫監督是測量、追蹤和評估資料庫的可用性、效能和功能的程序。監控和警示解決方案可協助組織確保其資料庫服務，以及其相關應用程式和工作負載的安全性、高效能、彈性且有效率。在 AWS 上，您可以收集和分析工作負載日誌、指標、事件和追蹤，以便了解工作負載的運作狀態，並從一段時間內的操作獲得見解。

您可以監控資源以確保資源能如預期般運作，並在問題影響客戶之前偵測並修復問題。您應該使用監視的指標、記錄檔、事件和追蹤，在違反閾值時引發警示。

本指南說明 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫的資料庫可觀察性和監控工具以及最佳實務。本指南著重於 MySQL 和 MariaDB 資料庫，雖然大部分資訊也適用於其他亞馬遜 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、DBA、資深DevOps工程師和其他團隊成員，負責為在 AWS 雲端中執行的資料庫工作負載設計、實作和管理監控和觀察性解決方案。

內容

概觀

監控和警示包括在 AWS Well-Architected 的框架的四個支柱中。

- 卓越營運支柱規定您的工作負載應該包括遙測和監控。 AWS Amazon 關聯式資料庫服務 (Amazon RDS) 等服務提供了解工作負載內部狀態 (例如指標、日誌、事件和追蹤) 所需的資訊。當您操作 Amazon RDS 資料庫時，您需要瞭解資料庫執行個體的運作狀態、偵測操作事件，並能夠回應計劃和未計劃的事件。AWS 提供的監控工具可協助您判斷組織和業務成果何時有風險，或可能存在風險，以便您在適當的時間採取適當的動作。
- 效能效率支柱規定您應該透過即時收集、彙總和處理與效能相關的指標來監控資源 (例如 Amazon RDS 資料庫執行個體) 的效能。您可以識別效能降低並修復因素 (例如，未最佳化的 SQL 查詢或組態參數不足)。當測量值超出預期的邊界時，您可以自動提高警報。我們建議您不僅針對通知使用警報，還可以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來評估收集的指標，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，您可以在一段時間內收集和分析`cpuUtilization.total`指標。在 CPU 使用率達到硬性限制之前主動發出警示，可協助您在問題影響客戶之前解決問題。
- 可靠性支柱將監控和警示定義為關鍵，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檢測故障。當它檢測到問題或故障時，其主要目的是在這些問題上提醒。對於雲端中的彈性架構而言，實作持續的觀察性和監控實務至關重要。若要改善您的工作負載，您必須能夠測量工作負載並瞭解其狀態和健康狀況。從故障自動復原、橫向延展性和容量佈建的設計原則，取決於準確的監控和警示服務。
- 安全性支柱討論偵測和預防意外或不必要的組態變更，以及未預期的行為。您可以使用 MariaDB 稽核外掛程式設定 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。該插件將數據庫活動記錄存儲在日誌文件中，可以將其集成並導入到監視和警報工具中。系統會即時分析記錄檔，找出資料庫中是否有未預期或可疑的行為。這種意外或可疑的行為可能表明您的 Amazon RDS 資料庫執行個體已遭到入侵，這表示您的業務可能帶來的風險。如果監控工具偵測到此類事件，就會啟動警示以啟動對安全性事件的回應，進而協助處理可疑和惡意活動。

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具有高效能、彈性、高效率、安全且成本最佳化的基礎架構。您可以使用可觀察性工具，即時收集、儲存和視覺化指標、事件、追蹤和記錄，以觀察和分析資料庫健全狀況和效能的全貌，進而防止相關聯的 IT 服務降級或中斷。如果仍然

發生意外降級或服務中斷，監視和警示工具可協助您及時偵測問題、升級、反應，以及快速調查和解決問題。適用於雲端資料庫工作負載的全方位監控和警示解決方案，可協助您達成下列業務成果：

- 改善客戶體驗。可靠的服務可改善客戶的體驗。數據庫通常是數字服務的關鍵組成部分，例如 Web 和移動應用程序，媒體流，支付， business-to-business （B2B）API 和集成服務。如果您可以監控並設定資料庫上的警示，以便快速偵測問題、有效率地調查問題，並儘快加以修復，將停機時間和其他干擾降到最低，您就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。更好的性能和更流暢的用戶體驗有助於贏得客戶的信任，從而在您的平台上創造更多業務。例如，提供可靠線上服務的付款處理服務供應商可以期待較高的客戶信任度和忠誠度，從而導致更多的客戶和更好的保留率、可計費交易的增加，以及可產生更多收入的創新服務。
- 避免財務損失。資料庫基礎結構中任何非預期的停機時間都會影響客戶使用應用程式執行的商業交易。在某些情況下，這可能會導致巨大的經濟損失。違反服務等級協議 (SLA) 可能會導致客戶信任喪失，因此損失收入。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賠償。根據軟件公司 Atlassian 公司的一項研究，服務中斷的平均成本在每小時 140K$540K 的範圍內，具體取決於業務的類型和規模。穩定的資料庫環境是防止長時間中斷和業務損失的關鍵。
- 擴展值。監控和警示機制可協助您設計、開發和操作高可用性、彈性、可靠、高效能、符合成本效益且安全的數位服務，但這只是個開始。您將希望您的組織隨著時間的推移擴展和蓬勃發展，增強現有的雲端工作負載，並推出新服務。新服務為您的客戶提供額外的價值，並為您的業務帶來更多收益，從而為您的業務增長帶來飛輪效應。
- 提高開發人員生產力具有生產力和高效率，並且在開發任務中沒有遇到問題和瓶頸的開發人員可以在更短的時間內交付高品質的產品。然而，軟體工程和 IT 作業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之間的效能和一致性，開發人員需要能夠提供相關指標和追蹤的工具。這些有助於儘快識別缺陷的程式碼構件和基礎結構元件，並協助判斷對使用者的影響。正確的監控和警示工具套件可協助開發人員更快速地編寫程式碼和測試。
- 提高營運效率和效率。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 future 的容量需求，並且可以利用 AWS 雲端可節省的成本。了解 Amazon RDS 工作負載和營運健康狀態可協助您回應事件、修正問題並規劃改進。

一般最佳做法

下列最佳實務可協助您充分掌握 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。

- 識別重要績效指標。根據所需的業務成果識別關鍵績效指標 (KPI)。評估 KPI 以確定工作負載是否成功。例如，如果您的核心業務是電子商務，那麼您理想的業務成果之一可能是您的電子商店全天候為您的客戶提供購物。為了實現該業務成果，您可以為電子商店應用程式使用的後端 Amazon RDS 資料庫定義可用性關鍵績效指標，並每週將基準 KPI 設定為 99.99%。根據基準值評估實際可用性 KPI，可協助您判斷是否符合所需的資料庫可用性 99.99%，進而達成擁有全天候服務的業務成果。
- 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。評估指標以確定工作負載是否達到所需的結果，並瞭解工作負載的健康狀況。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正常運行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)
  ```

  量度代表有時間順序的資料點集合。量度也可以包含維度，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`，測量主機亞馬遜彈性運算雲端 (Amazon EC2) 執行個體的記憶體總量。監控工具應定期對收集的指標進行主動分析，以識別趨勢並確定是否需要任何適當的響應。
- 建立工作負載指標基準。建立測量結果的基準線，以定義預期值，以及識別良好或不良的臨界值。例如，您可以定義的基準線`ReadIOPS`在正常的數據庫操作下最多為 1,000。然後，您可以使用此基準進行比較，以及識別過度使用率。如果您的新指標始終顯示讀取 IOPS 在 2,0003,000 的範圍內，則您已經確定了可能觸發調查，干預和改進的響應的偏差。
- 在工作負載結果有風險時發出警示。當您確定業務結果處於風險之中時，請提出警報。然後，您可以在問題影響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，建立工作負載活動的模式，以識別未預期的行為，並在必要時使用適當的動作回應。AWS提供監控工具應用統計和機器學習算法來分析指標並檢測異常。
- 偵測到工作負載異常時發出警示。在 Amazon RDS 工作負載的操作中偵測到異常時，請提出警示，以便您可以在必要時使用適當的動作做出回應。

- 檢閱和修改 KPI 和指標。確認您的 Amazon RDS 資料庫符合您定義的需求，並找出可能改善的區域，以達成您的業務目標。驗證測量指標的有效性並評估 KPI，並在必要時對其進行修改。例如，假設您為並行資料庫連線的最佳數目設定了 KPI，並監視有關嘗試連線和失敗的連線，以及建立和執行中的使用者執行緒的測量結果。您的資料庫連線可能比 KPI 基準線所定義的資料庫連線數量多。通過分析當前指標，您可以檢測結果，但可能無法確定根本原因。如果是這樣，您應該修改指標並加入其他監視措施，例如表格鎖定的計數器。新的量度有助於判斷增加的資料庫連線數目是否是因為非預期的資料表鎖定所造成。

監控工具

我們建議您使用可觀察性、監視和警示工具來：

- 深入瞭解您的 Amazon RDS 環境的效能
- 偵測意外和可疑行為
- 規劃容量並做出有關配置 Amazon RDS 執行個體的決策
- 分析指標和日誌以主動預測潛在問題
- 在超出閾值時產生警示，以便在使用者受到影響之前進行疑難排解並解決問題

您有不同的選項和解決方案可供選擇，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。以下各節將討論其中一些工具。

若要判斷哪種工具最適合您的需求，請根據您組織的需求比較每個工具的功能。我們也建議您評估這些工具，以便於部署、組態與整合、軟體更新與維護、部署方法 (例如硬體或無伺服器)、授權、價格，以及組織特定的任何其他因素。

章節

Amazon RDS 中包含的工具

Amazon Relational Database Service 服務 (Amazon RDS) 是 AWS 雲端中的受管資料庫服務。由於 Amazon RDS 是受管服務，因此可讓您免於大部分的管理任務，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 此外，還提供一組全方位的工具，可讓您為 Amazon RDS 資料庫執行個體建立完整的可觀察性解決方案。

Amazon RDS 服務中包含、預先設定和自動啟用某些監控工具。一旦您啟動新的 Amazon RDS 執行個體，就可以使用兩種自動化工具：

- Amazon RDS 執行個體狀態提供有關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 建議可針對資料庫執行個體、僅供讀取複本和資料庫參數群組提供自動化建議。這些建議是透過分析資料庫執行個體使用情況、效能資料和組態來提供，並作為指導提供。例如，Engine 版本過期的建議表明您的資料庫執行個體並未執行最新版本的資料庫軟體，您應該升級資料庫執行個體，以便從最新的安全性修正和其他改進中獲益。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 整合 CloudWatch，這是針對在 AWS 上執行的雲端資源和應用程式的監控和警示服務。Amazon RDS 會自動收集有關資料庫執行個體的操作、使用率、效能和運作狀態的指標、記錄檔、追蹤和事件，並將其傳送至以 CloudWatch 進行長期儲存、分析和警示。

適用於 MySQL 的 Amazon RDS 和適用於 MariaDB 的 Amazon RDS 會 CloudWatch在一分鐘內自動發佈一組預設指標，而無需額外付費。這些指標會收集到兩個命名空間中，這些命名空間是量度的容器：

- AWS/RDS 命名空間包含資料庫執行個體層級度量。範例包括 `BinLogDiskUsage` (二進位記錄所佔用的磁碟空間量)、`CPUUtilization` (CPU 使用率的百分比)、`DatabaseConnections` (資料庫執行個體的用戶端網路連線數目) 等等。
- AWS/ 使用量命名空間包含帳戶層級使用量指標，用於判斷您是否在 Amazon RDS 服務配額內操作。範例包括 `DBInstances` (AWS 帳戶或區域中的資料庫執行個體數量)、`DBSubnetGroups` (您帳戶或區域中的資料庫子網路群組數量)，以及 `ManualSnapshots` (您 AWS 帳戶或區域中手動建立的 AWS 資料庫快照數量)。

CloudWatch 如下所示保留測量結果資料：

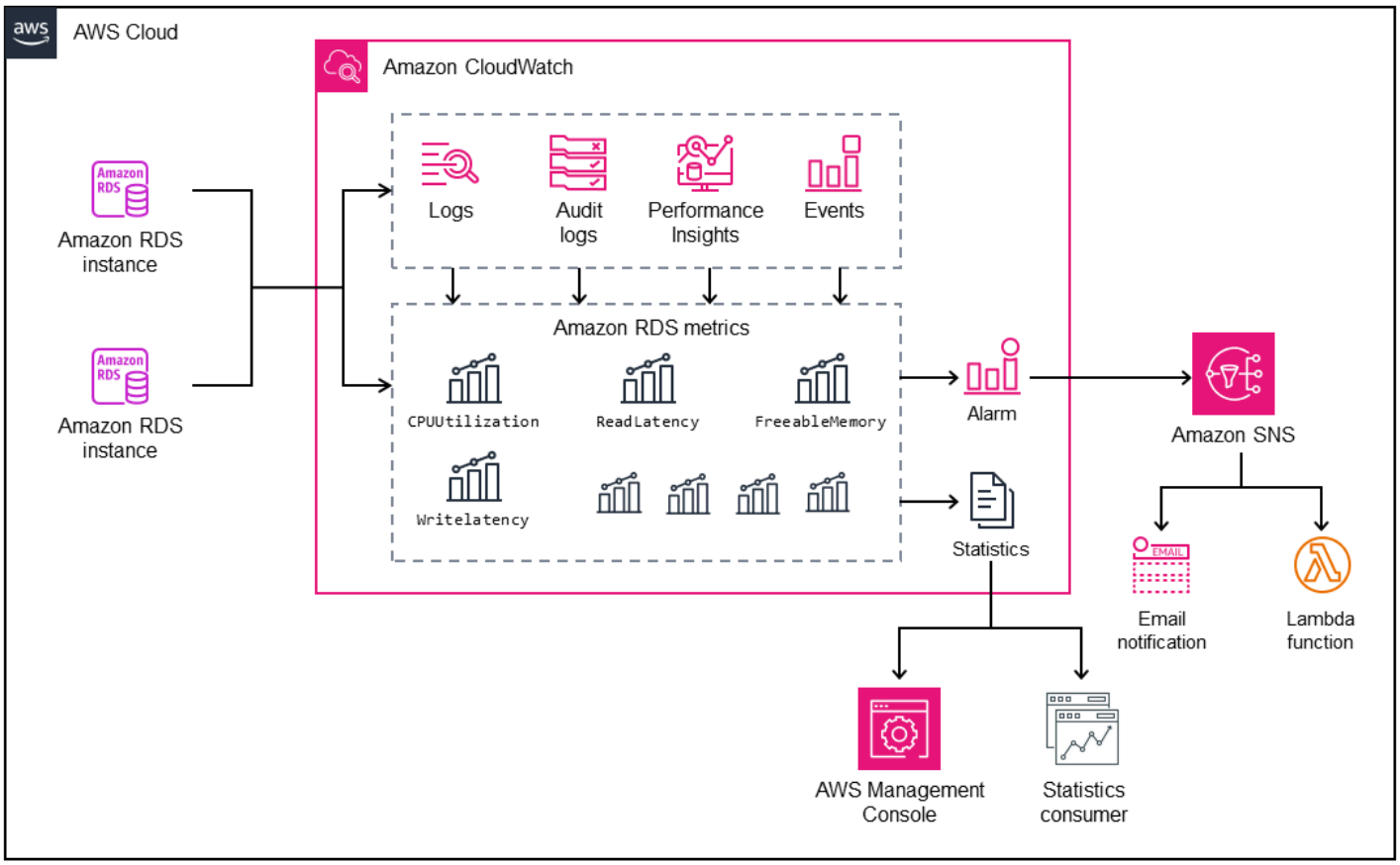
- 3 小時：高解析度自訂指標 (期間少於 60 秒) 會保留 3 小時。3 小時後，資料點會彙總為 1 分鐘期間量度，並保留 15 天。
- 15 天：期間為 60 秒（1 分鐘）的資料點會保留 15 天。15 天後，資料點會彙總為 5 分鐘的期間量度，並保留 63 天。

- 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 小時期間量度，並保留 15 個月。
- 15 個月：期間 3,600 秒（1 小時）的資料點可使用 15 個月（455 天）。

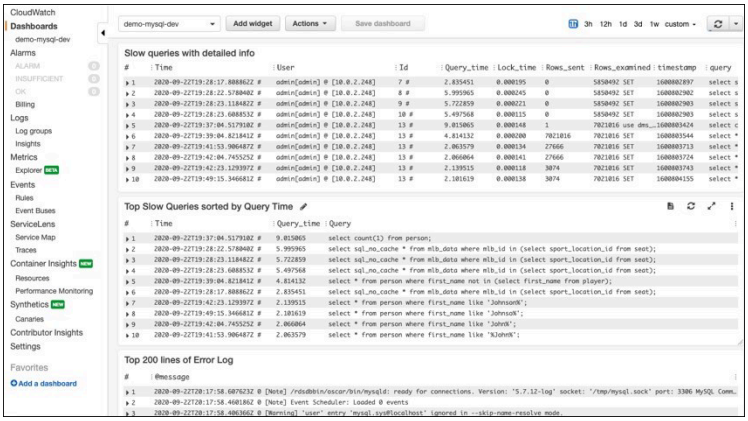
如需詳細資訊，請參閱 CloudWatch 文件中的量度。

CloudWatch 警報和儀表板

您可以使用 Amazon CloudWatch 警示來觀看一段時間內的特定 Amazon RDS 指標。例如，您可以監視並執行一或多個動作`FreeStorageSpace`，如果量度的值違反您設定的閾值。如果您將臨界值設定為 250 MB，且可用儲存空間為 200 MB (小於臨界值)，警示將會啟動，並可觸發動動作，為 Amazon RDS 資料庫執行個體自動佈建額外儲存。警示也可以使用亞馬遜簡單通知服務 (Amazon SNS)，將通知簡訊傳送至 DBA。下圖說明此程序。

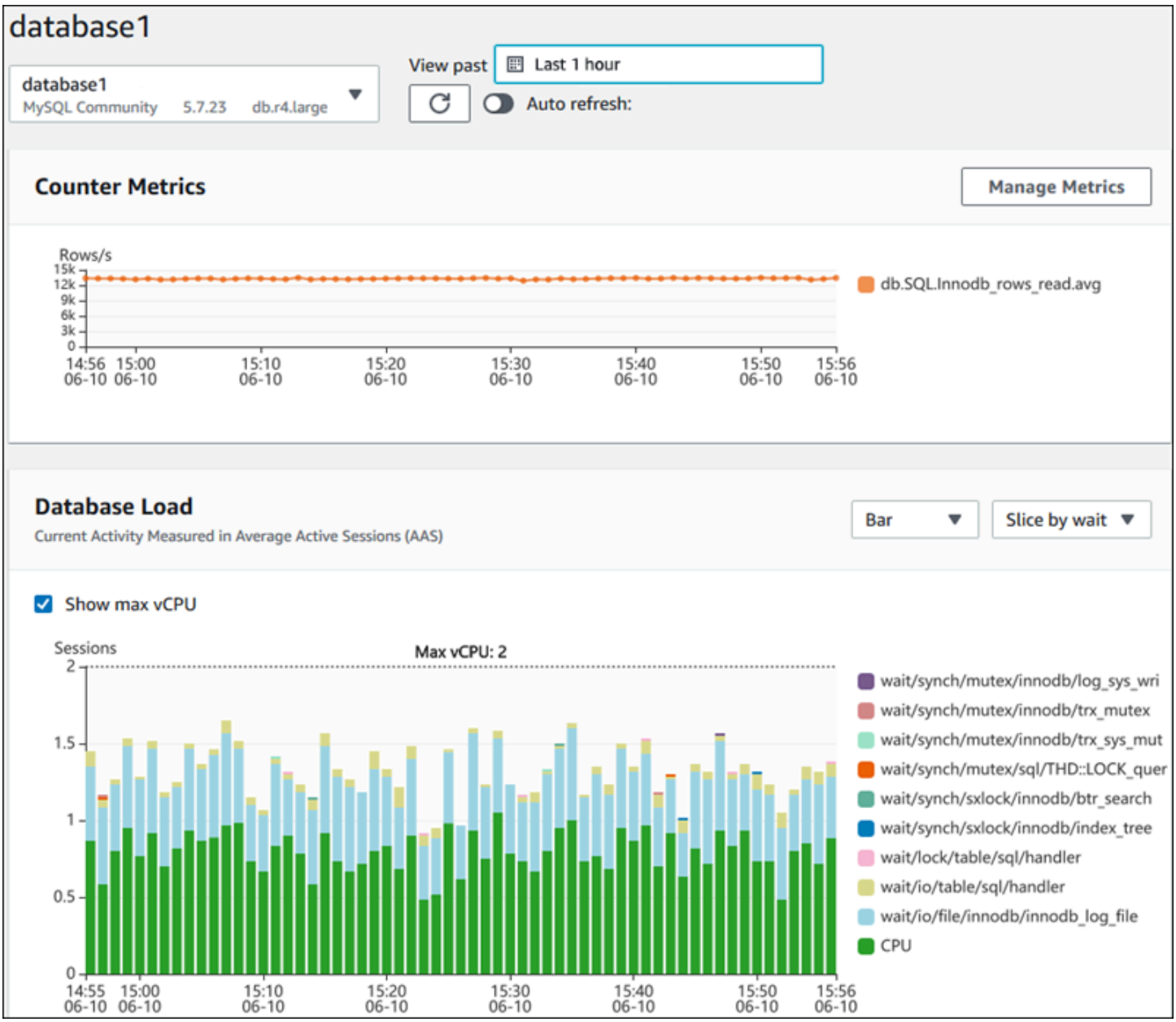


CloudWatch 也提供儀表板，您可以用來建立、自訂、與之互動，以及儲存量度的自訂檢視 (圖形)。您也可以使用 CloudWatch Logs Insights 建立儀表板來監視慢速查詢記錄檔和錯誤記錄，並在這些記錄檔中偵測到特定模式時接收警示。下面的屏幕顯示了一個示例 CloudWatch儀表板。



Amazon RDS Performance Insights

Amazon RDS Performance Insights 是一種資料庫效能調整和監控工具，可擴展 Amazon RDS 監控功能。透過視覺化資料庫執行個體負載，並透過等待、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，協助您識別資料庫執行個體可能存在的瓶頸類型，例如鎖定等待、高 CPU 消耗或 I/O 延遲，並判斷哪些 SQL 敘述句造成瓶頸。下面的屏幕顯示了一個示例可視化。



您必須在資料庫執行個體建立程序期間啟用 Performance Insights，才能收集帳戶中 Amazon RDS 資料庫執行個體的指標。免費方案包括每月 7 天的效能資料歷程記錄和一百萬個 API 請求。您也可以選擇購買較長的保留期間。如需有關費用的資訊，請參閱 Performance Insights 定價。

如需如何使用 Performance Insights 來監控資料庫執行個體的詳細資訊，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 Performance Insights 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、或 CloudWatch API 來檢查 Performance Insights 指標。 AWS CLI您也可以新增 CloudWatch警示，就像任何其他量度一

樣。例如，您可能想要觸發 SMS 通知給 DBA，或者在DBLoad指標違反您設定的閾值時採取更正動作。您也可以將「Performance Insights」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，可針對執行 Amazon RDS 資料庫執行個體的作業系統 (OS) 即時擷取指標。這些指標可為 CPU、記憶體、Amazon RDS 和作業系統處理序、檔案系統和磁碟 I/O 資料等提供高達一秒的精細度。您可以在 Amazon RDS 主控台中存取和分析這些指標。與 Performance Insights 一樣，增強型監控指標是從 Amazon RDS 傳送到 CloudWatch，您可以從中受益於其他功能，例如長期保留指標以進行分析、建立指標篩選器、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，增強型監控會停用。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 日誌的資料量以及儲存費率而定。視啟用「增強型監控」的資料庫執行個體數量而定，部分監控資料可包含在免費 CloudWatch 記錄方案中。如需完整的定價詳細資訊，請參閱 Amazon CloudWatch 定價。如需有關此工具的詳細資訊，請參閱 Amazon RDS 文件和增強型監控常見問答集。

附加 AWS 服務

AWS 提供數種支援服務，這些服務也與 Amazon RDS 整合 CloudWatch，以及進一步增強資料庫的可觀察性。這些措施包括 Amazon EventBridge，Amazon CloudWatch 日誌和 AWS CloudTrail.

- Amazon EventBridge 是一種無伺服器事件匯流排，可從您的應用程式和 AWS 資源 (包括 Amazon RDS 資料庫執行個體) 接收、篩選、轉換、路由和交付事件。Amazon RDS 事件表示 Amazon RDS 環境中的變化。例如，當資料庫執行個體的狀態從「可用」變更為「已停止」時，Amazon RDS 就會產生該事件`RDS-EVENT-0087 / The DB instance has been stopped`。Amazon RDS 以近乎即時的方式 EventBridge 向 CloudWatch 活動提供活動。使用 EventBridge 和 CloudWatch 事件，您可以定義規則以針對感興趣的特定 Amazon RDS 事件傳送警示，並在事件符合規則時自動執行的動作。有多種目標可用於回應事件，例如可以執行更正動作的 AWS Lambda 函數，或可傳送電子郵件或 SMS 以通知 DBA 或 DevOps 工程師有關事件的 Amazon SNS 主題。
- Amazon CloudWatch 日誌是一項服務，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此功能，Amazon RDS 會自動將下列日誌發佈到 CloudWatch 日誌：
  - 錯誤日誌
  - 慢查詢日誌
  - 一般日誌
  - 稽核日誌

您可以使用 CloudWatch 日誌見解來查詢和分析日誌資料。此功能包含專門建置的查詢語言，可協助您搜尋符合您定義之模式的記錄事件。例如，您可以監視下列模式的錯誤記錄檔，以追蹤 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"`過濾的日誌數據可以轉換為 CloudWatch 指標。然後，您可以使用指標來建立包含圖形或表格資料的儀表板，或者在違反定義的閾值時設定警示。這在使用稽核記錄檔時特別有用，因為如果偵測到任何未預期或可疑的行為，您可以自動監控、傳送警示以及採取更正動作。您可以使用管理主控台、Amazon RDS API 或日誌專用 AWS CLI AWS 開發套件來存取和 AWS 管理資料庫 CloudWatch 日誌。

- AWS CloudTrail記錄並持續監控 AWS 帳戶中的使用者和 API 活動。它可協助您對 Amazon RDS for MySQL 或 MariaDB 資料庫執行個體進行稽核、安全監控和操作故障診斷。 CloudTrail 與 Amazon RDS 集成。所有動作都可以記錄，並 CloudTrail 提供 Amazon RDS 中使用者、角色或 AWS 服務所採取的動作記錄。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，而日誌中包含所請求動作 (`"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"}`) 等相關資訊。記錄的事件 CloudTrail 包括來自 Amazon RDS 主控台的呼叫和使用 Amazon RDS API 的程式碼呼叫。

第三方監控工具

在某些情況下，除了為 Amazon RDS 提供的完整雲端原生觀察性和監控工具套件之外，您可能還想使用其他軟體廠商 AWS 提供的監控工具。這類案例包括混合部署，您可能會在內部部署資料中心中執行數個資料庫，而在 AWS 雲端. 如果您已經建立公司的可觀察性解決方案，則可能需要繼續使用現有的工具，並將其擴展到 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 做為雲端管理服務所強加的保護措施。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，因為資料庫主機的存取遭到拒絕。不過，您可以透過建置在其他 AWS 雲端 服務之 CloudWatch 上，將許多第三方監控解決方案與 Amazon RDS 整合。例如，可以匯出 Amazon RDS 指標、日誌、事件和追蹤，然後匯入第三方監控工具，以進行進一步的分析、視覺化和警示。其中一些第三方解決方案包括 Prometheus，Grafana 和佩爾科納。

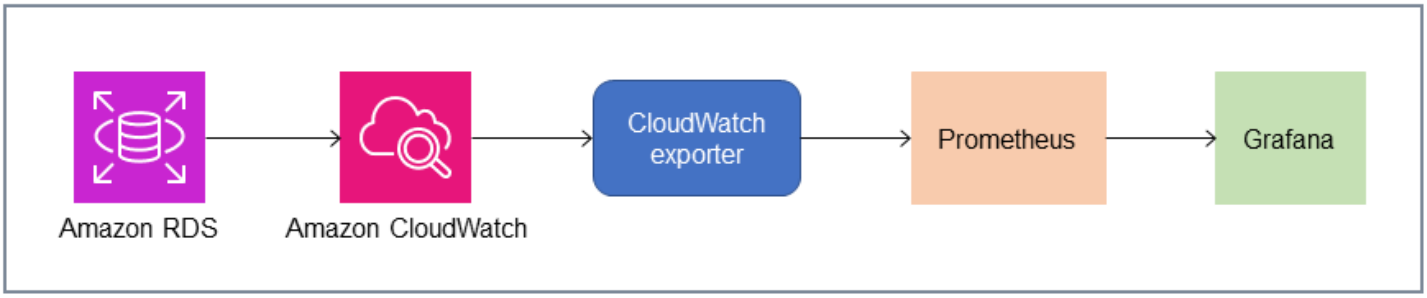
Prometheus 和 Grafana

Prometheus 是一種開放原始碼監視解決方案，可在指定的時間間隔從設定的目標收集指標。它是一種通用的監視解決方案，可以監視任何應用程序或服務。當您監控 Amazon RDS 資料庫執行個體時，請從 Amazon RDS CloudWatch 收集指標。然後會使用開放原始碼匯出程式 (例如 YACE 匯出程式或匯出程式)，將度量匯出至 Prometheus 伺服器。 CloudWatch

- YACE 匯出程式會在單一要求中擷取 API 的多個指標，藉此 CloudWatch 最佳化資料匯出工作。測量結果儲存在 Prometheus 伺服器之後，伺服器會評估規則運算式，並在觀察到指定的條件時產生警示。
- CloudWatch 出口商由 Prometheus 正式維護。它通過 CloudWatch API 檢索 CloudWatch 指標，並通過使用 REST API 請求到 HTTP 端點以與 Prometheus 兼容的格式將它們存儲在 Prometheus 服務器上。

當您選擇匯出器、設計部署模型並設定匯出程式執行個體時，請考慮CloudWatch並CloudWatch記錄服務和 API 配額，因為 CloudWatch 指標匯出至 Prometheus 伺服器是在 API 之上實作的。CloudWatch 例如，在單一 AWS 帳戶 和區域中部署多個 CloudWatch 匯出器執行個體以監控數百個 Amazon RDS 資料庫執行個體，可能會導致節流錯誤 (ThrottlingException) 和程式碼 400 錯誤。若要克服此類限制，請考慮使用 YACE 匯出程式，該匯出器經過最佳化，可在單一要求中收集多達 500 個不同的量度。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執行個體 AWS 帳戶，而不是將工作負載集中到一個執行個體 AWS 帳戶，並限制每 AWS 帳戶個執行個體中的匯出器執行個體數量。

警報由 Prometheus 服務器生成，並由警報管理器處理。該工具負責刪除重複，分組和路由警報到正確的接收者，例如電子郵件，SMS 或 Slack，或啟動自動響應操作。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 Grafana 提供豐富的視覺化 Widget，例如進階圖形、動態儀表板和分析功能，例如臨機查詢和動態深入分析。它還可以搜索和分析日誌，並包含警報功能以持續評估指標和日誌，並在數據與警報規則匹配時發送通知。



佩爾科納

Percona 監控和管理（PMM）是一個免費的開放源代碼數據庫監控，管理和觀察性解決方案，適用於 MySQL 和 MariaDB。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，例如資料庫健康狀態評估的自動建議程式。您可以使用 PMM 來監控 Amazon RDS。但是，PMM 用戶端 (代理程式) 未安裝在 Amazon RDS 資料庫執行個體的基礎主機上，因為它無法存取主機。此工具會改為連線至 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 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 工具已設定為進行資料庫監視，並收集比 Prometheus 更多的資料庫特定測量結果。若要使用 PMM 查詢分析儀表板，您必須將效能結構描述設定為查詢來源，因為 Amazon RDS 並未安裝查詢分析代理程式，而且無法讀取緩慢的查詢日誌。相反地，它會直接`performance_schema`從 MySQL 和 MariaDB 資料庫執行個體查詢，以取得指標。PMM 的其中一個突出特點是它能夠針對工具在其資料庫中識別的問題提出警示和建議。PMM 提供了一組檢查，可以檢測常見的安全威脅，性能降低，數據丟失和數據損壞。

除了這些工具之外，市場上還有多種可與 Amazon RDS 整合的商業觀察性和監控解決方案。範例包括資料庫監控、Amazon RDS 監控和資料庫監控。AppDynamics

數據庫實例監控

一個數據庫實例是亞馬遜 RDS 的基本構建塊。它是在雲端中執行的隔離資料庫環境。對於 MySQL 和 MariaDB 資料庫，資料庫執行個體為神秘的程序，也稱為 MySQL 服務器，其中包括多個線程和組件，如 SQL 解析器，查詢優化器，線程/連接處理程序，系統和狀態變量，以及一個或多個可插拔的存儲引擎。每個儲存引擎都是為了支援特殊的使用案例而設計。預設和建議的儲存引擎為創新數據庫，這是符合原子性、一致性、隔離、耐久性 (ACID) 模型的交易式通用關聯式資料庫引擎。創新資料庫功能記憶體內結構（緩衝池，更改緩衝區，自適應哈希索引，日誌緩衝區）以及磁碟上結構(表格空間、表格、索引、還原日誌、重做日誌、雙重寫入緩衝區檔案)。為了確保您的數據庫緊密粘附 ACID 模型，InnoDB 儲存引擎實現了眾多功能保護您的數據，包括交易，提交，回滾，崩潰恢復，行級鎖定和多版本並發控制（MVCC）。

資料庫執行個體的所有這些內部元件共同運作，以協助維持資料在預期和令人滿意的效能等級的可用性、完整性和安全性。視您的工作負載而定，每個元件和功能可能會增加 CPU、記憶體、網路和儲存區子系統的資源需求。當特定資源的需求激增超過佈建的容量或該資源的軟體限制 (由組態參數或軟體設計強加) 時，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，測量和監視這些內部元件、將它們與定義的基準值進行比較，並在監督的值與預期值不同時產生警示非常重要。

如前所述，您可以使用不同的工具來監視你的 MySQL 和瑪麗亞德 B 實例。我們建議您使用亞馬遜 RDS 性能洞見和CloudWatch用於監控和警示的工具，因為這些工具已與 Amazon RDS 整合，可收集高解析度指標、以近乎即時的方式呈現最新的效能資訊，以及產生警示。

無論您喜歡哪種監視工具，我們都建議您開啟效能綱要在您的 MySQL 和瑪麗亞資料庫執行個體中。該效能綱要是一項選用功能，可在低層級監視 MySQL 伺服器 (資料庫執行個體) 的作業，其設計目的是將對整體資料庫效能的影響降到最低。您可以使用`performance_schema`參數。雖然此參數是選用的，但您必須使用它來收集 Amazon RDS 效能洞見收集高解析度 (一秒) 每個 SQL 指標、作用中工作階段指標、等待事件以及其他詳細的低階監控資訊。

部分

- 資料庫執行個體的效能洞見指
- CloudWatch資料庫執行個體指標
- 將效能洞察指標發佈至CloudWatch

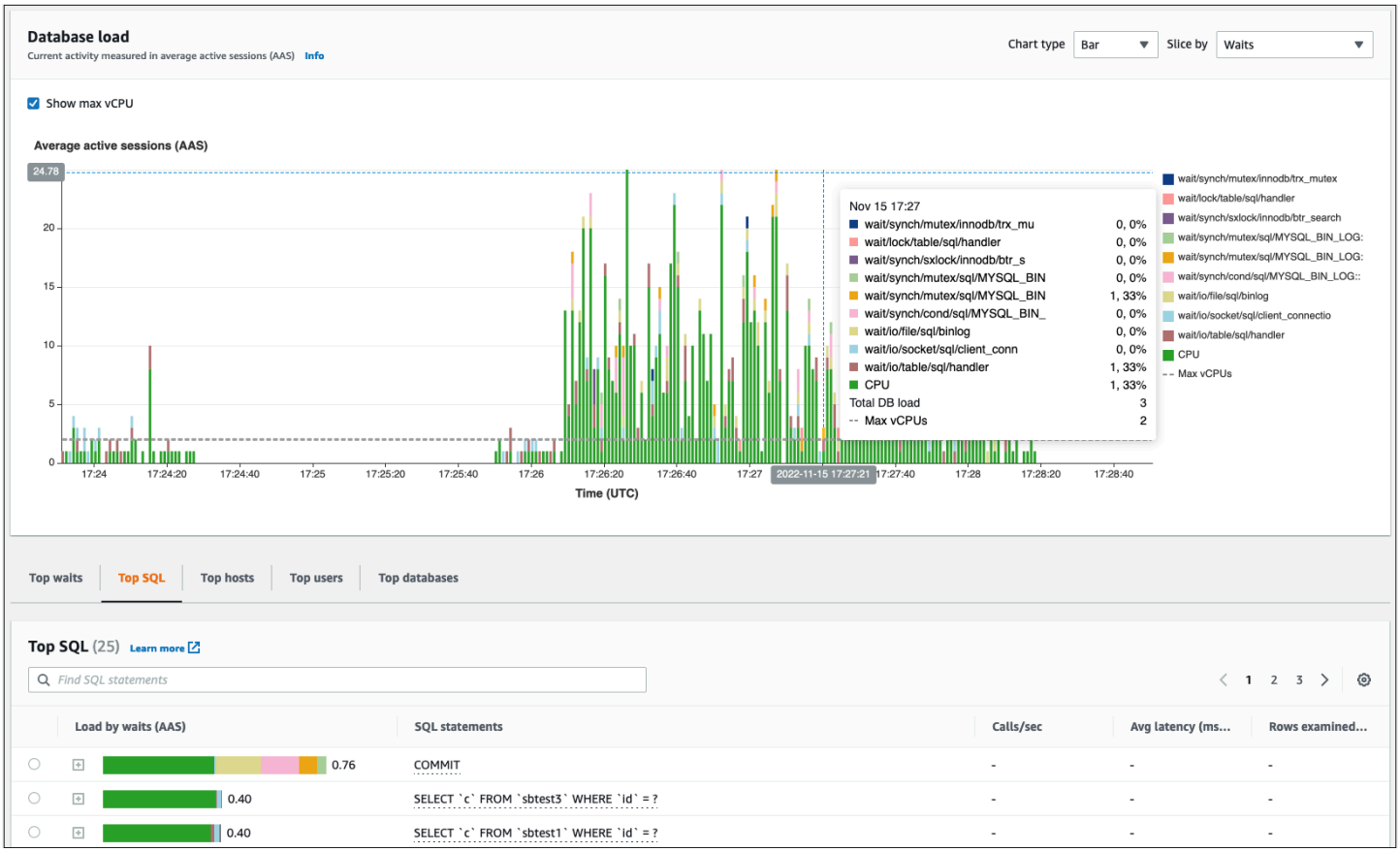
資料庫執行個體的效能洞見指

效能洞見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「效能洞見」中的關鍵指標，可測量資料庫中的活動層級。每秒收集一次，並自動發佈到亞馬遜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，也就是同時執行 SQL 查詢的工作階段數目。該DBLoad測量結果與其他時間序列測量結果不同，因為測量結果可以使用下列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公制。您可以將它們用作通過切片分類來表示數據庫負載的不同特徵。有關我們如何計算數據庫負載的詳細說明，請參閱資料庫載入在亞馬遜 RDS 文檔中。

下列畫面圖例顯示「效能洞見」工具。



維度

- 等待事件是資料庫階段作業等待資源或其他作業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`如果此表比分配的 InnoDB 緩衝池大得多，則您的會話很可能會等待`wait/io/file/innodb/innodb_data_file`等待事件，這是由數據文件上的物理 I/O 操作引起的。等待事件是資料庫監督的重要維度，因為它們指出可能的效能瓶頸。等待事件指出您在工作階段中執行的 SQL 敘述句花費最多時間等待的資源和作業。例如，`wait/synch/mutex/innodb/trx_sys_mutex`當資料庫活動含有大量交易時，就會發生事件，以及`wait/synch/`

`mutex/innodb/buf_pool_mutex`當執行緒取得 InnoDB 緩衝集區上的鎖以存取記憶體中的頁面時，就會發生事件。有關所有 MySQL 和 MariaDB 等待事件的信息，請參閱等待事件摘要表格在 MySQL 文檔中。若要瞭解如何解譯工具名稱，請參閱效能綱要儀器命名慣例在 MySQL 文檔中。

- SQL顯示哪些 SQL 敘述句對總資料庫負載的貢獻最大。該頂部尺寸表，這是位於資料庫載入圖表中的亞馬遜 RDS 性能洞察，是互動的。您可以按一下 SQL 敘述句中的列，取得與 SQL 敘述句相關之等待事件的詳細清單依等待負載 (AAS)欄。當您在清單中選取 SQL 敘述句時，效能洞見會在資料庫載入圖表和中的 SQL 敘述句文字SQL 文字部分。SQL 統計資料會顯示在右側頂部尺寸表。
- 主機顯示已連線用戶端的主機名稱。此維度可協助您識別哪些從屬端主機將大部分負載傳送至資料庫。
- 使用者由登錄到數據庫的用戶對數據庫負載進行分組。
- 資料庫按客戶端連接到的數據庫名稱對數據庫負載進行分組。

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。計數器量度的值無法減少為先前的值。這些指標代表一個單調增加的計數器。

- 原生計數器是由資料庫引擎定義的指標，而不是由 Amazon RDS 定義的指標。例如：
  - `SQL.Innodb_rows_inserted`表示插入 InnoDB 表中的行數。
  - `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`表示 InnoDB 引擎無法從緩衝池中檢索並且必須直接從磁盤讀取的邏輯讀取數。
  - `Cache.Innodb_buffer_pool_read_requests`代表邏輯讀取請求的數目。

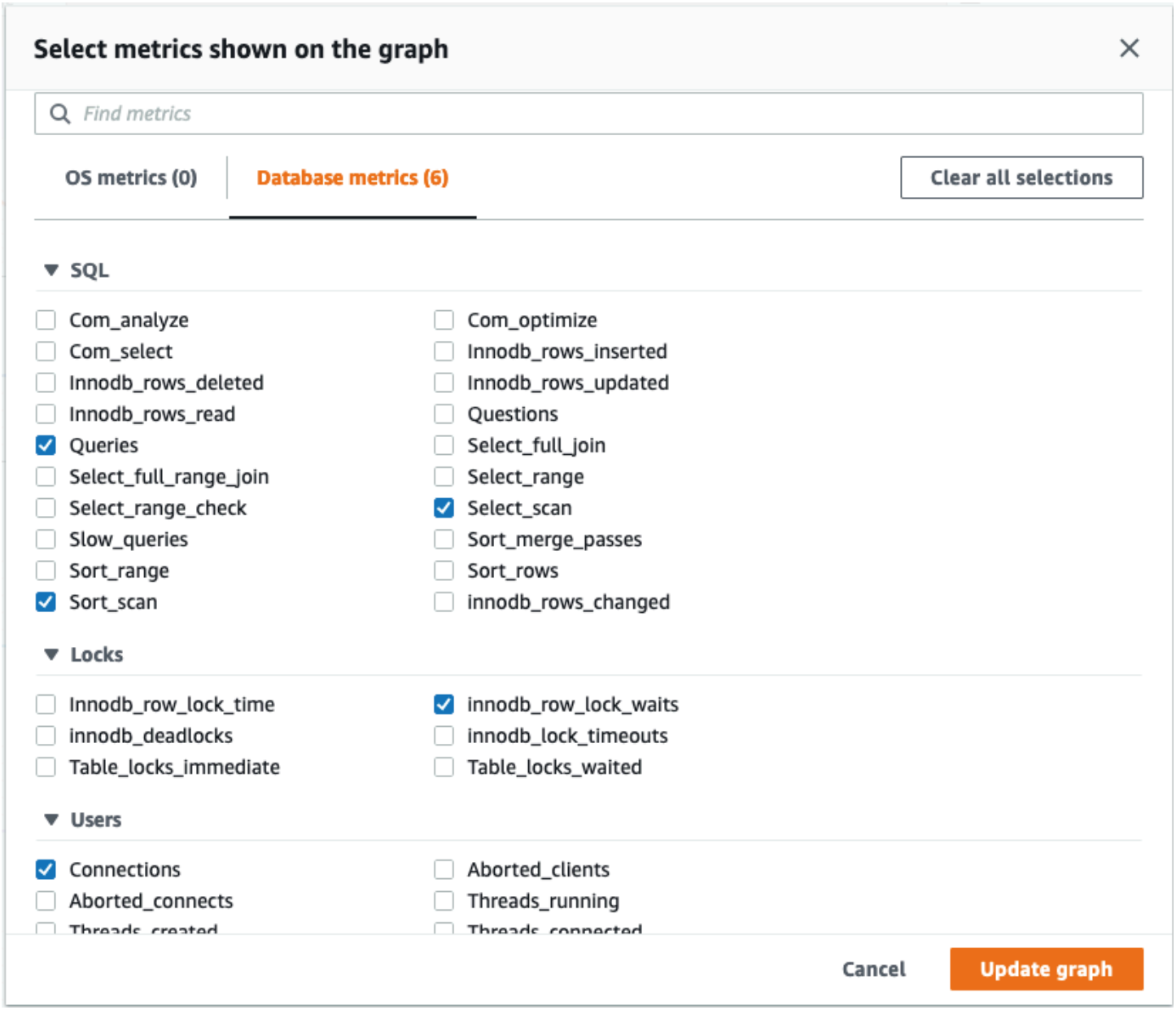
  如需所有原生量度的定義，請參閱伺服器狀態變數在 MySQL 文檔中。
- 非原生計數器由亞馬遜 RDS 定義。您可以使用特定查詢來取得這些量度，也可以在計算中使用兩個或多個原生量度來衍生這些量度。非原生計數器量度可以代表延遲、比率或命中率。例如：
  - `Cache.innoDB_buffer_pool_hits`表示 InnoDB 可以在不使用磁盤的情況下從緩衝池中檢索讀操作的數量。它是根據原生計數器量度計算的，如下所示：

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

  - `IO.innoDB_datafile_writes_to_disk`表示 InnoDB 資料檔案寫入磁碟作業的數量。它只會擷取資料檔案上的作業，而不會擷取雙寫或重做記錄寫入作業。它的計算方式如下：

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

您可以直接在效能洞見儀表板中視覺化資料庫執行個體指標。選擇管理指標，選擇資料庫指標標籤，然後選取感興趣的量度，如下圖所示。



選擇合適的更新圖形按鈕以顯示您選取的測量結果，如下圖所示。

SQL Statistics

效能洞見會針對查詢執行的每秒和每個 SQL 呼叫，收集與 SQL 查詢相關的效能相關測量結果。一般而言，效能洞見會收集SQL 統計資料在語句和摘要級別。但是，對於 MariaDB 和 MySQL 資料庫執行個體，只會在摘要層級收集統計資料。

- 摘要統計資料是具有相同樣式但最終具有不同常值之所有查詢的複合度量。摘要會以變數取代特定的常值，例如：

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

- 有表示統計數據的指標每秒對於每個消化的 SQL 語句。例如，`sql_tokenized.stats.count_star_per_sec`代表每秒呼叫次數 (也就是每秒執行 SQL 陳述式的次數)。
- 效能洞見也包含可提供的指標每次通話SQL 敘述句的統計資料。例如，`sql_tokenized.stats.sum_timer_wait_per_call`顯示每次呼叫的 SQL 敘述句平均延遲，以毫秒為單位。

SQL 統計資料可在 [效能洞見] 儀表板中取得前幾個 SQL的索引標籤頂部尺寸表。

CloudWatch資料庫執行個體指標

亞馬遜CloudWatch也包含 Amazon RDS 自動發佈的指標。駐留在中的量度AWS/RDS命名空間是執行個體層級量度，這是指 Amazon RDS (服務) 執行個體 (也就是在雲端中執行的隔離資料庫環境)，而不是資料庫執行個體，從嚴格意義上講神秘的過程。因此，大多數這些預設量度屬於操作系統指標的類別，在術語的嚴格定義。範例包括：CPUUtilization,WriteIOPS,SwapUsage，和其他人。不過，還有一些資料庫執行個體指標適用於 MariaDB 和 MySQL：

- BinLogDiskUsage— 二進位記錄所佔用的磁碟空間量。
- 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量。

將效能洞察指標發佈至CloudWatch

Amazon RDS 效能洞見可監控大部分資料庫執行個體指標和維度，並透過AWS管理主控台。此儀表板非常適合用於資料庫疑難排解和根本原因分析。但是，無法針對效能相關指標在效能洞見中建立警示。若要根據效能洞察指標建立警示，您必須將這些指標移至CloudWatch。具有度量CloudWatch還使您可以訪問高級監視功能，例如CloudWatch異常偵測,公制數學，以及統計資料，您可以將指標導出到外部監視工具，例如普羅米修斯和格拉法納。

效能洞見指標不會自動發佈至CloudWatch(除了資料庫載入度量). 將資料庫執行個體指標從效能洞見發佈到CloudWatch，您可以使用效能洞察 API擷取指標，以及CloudWatchAPI將量度發佈至CloudWatch。要自動化流程，您可以創建一個 Lambda 函數並在亞馬遜中對其進行排程EventBridge在指定的時間段執行，例如，每兩分鐘執行一次。您可以指定要發佈到哪些「效能洞見」指標CloudWatch。Lambda 函數會從所有已啟用效能洞見的 Amazon RDS 執行個體取得這些指標，並將指標儲存在CloudWatch。如需有關此程序的詳細資訊，請參閱有關的部落格文章提供效能洞見計數器指標CloudWatch。

系統監控

適用於 MySQL 或 MariaDB 的亞馬遜 RDS 中的資料庫執行個體在 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在很大程度上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令並管理其他系統資源。如果 CPU 過度使用 (也就是說，如果負載所需的 CPU 電力超過資料庫執行個體佈建的能力)，則此問題會影響資料庫的效能和穩定性，以及因此影響應用程式的效能和穩定性。

數據庫引擎動態分配和釋放內存。當 RAM 中沒有足夠的記憶體來執行目前的工作時，系統會將記憶體分頁寫入置換記憶體，該記憶體位於磁碟上。由於磁碟比記憶體慢得多，即使磁碟是以 SSD NVMe 技術為基礎，記憶體配置過多會導致效能降低。高記憶體使用率會導致資料庫回應延遲增加，因為分頁檔案的大小會增加以支援額外的記憶體。如果記憶體配置太高，以致於耗盡 RAM 和交換記憶體空間，則資料庫服務可能無法使用，而且使用者可能會觀察到錯誤，例如`[ERROR] mysqld: Out of memory (Needed xyz bytes)`。

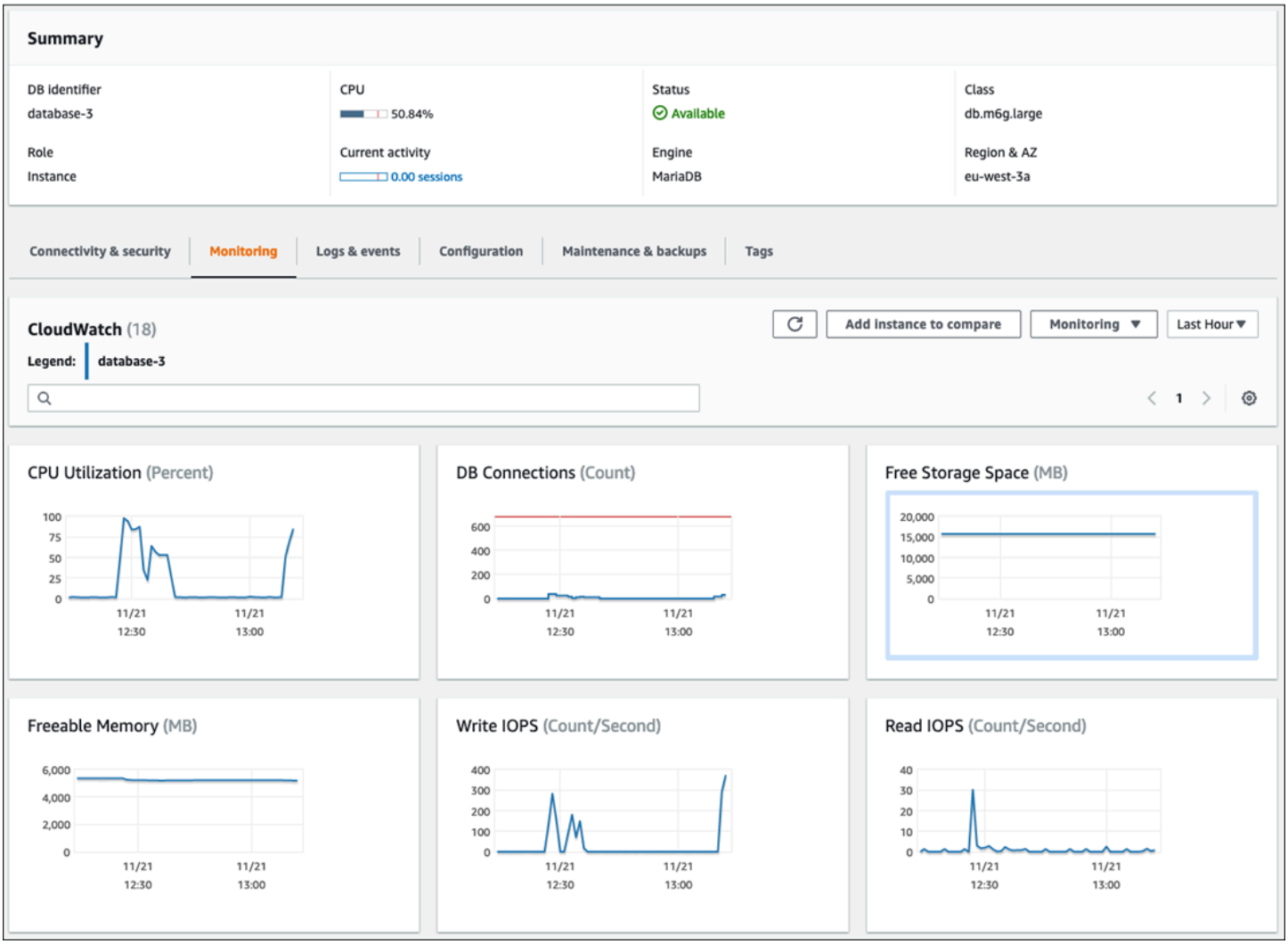
MySQL 和 MariaDB 的數據庫管理系統利用存儲子系統，它由存儲磁盤組成磁碟上結構例如表格、索引、二進位日誌、重做日誌、還原日誌和雙重寫入緩衝區檔。因此，與其他類型的軟體相比，資料庫必須執行大量的磁碟活動。為了達到最佳的資料庫作業，請務必監視和調整磁碟 I/O 使用率和磁碟空間配置。當資料庫達到磁碟支援的最大 IOPS 或輸送量限制時，資料庫效能可能會受到影響。例如，索引掃描造成的隨機存取突發可能會導致每秒大量 I/O 作業，最終可能會觸及基礎儲存區的限制。完整資料表掃描可能不會達到 IOPS 限制，但可能會造成以每秒 MB 為單位的高輸送量。監視和生成磁盤空間分配警報至關重要，因為錯誤如`OS error code 28: No space left on device`可能會造成資料庫無法使用和損毀。

Amazon RDS 可即時為執行資料庫執行個體的作業系統提供指標。Amazon RDS 會自動將一組作業系統指標發佈到CloudWatch。您可以在 Amazon RDS 主控台中顯示和分析這些指標，以及CloudWatch儀表板，您可以在中設置所選指標的警報CloudWatch。範例包括：

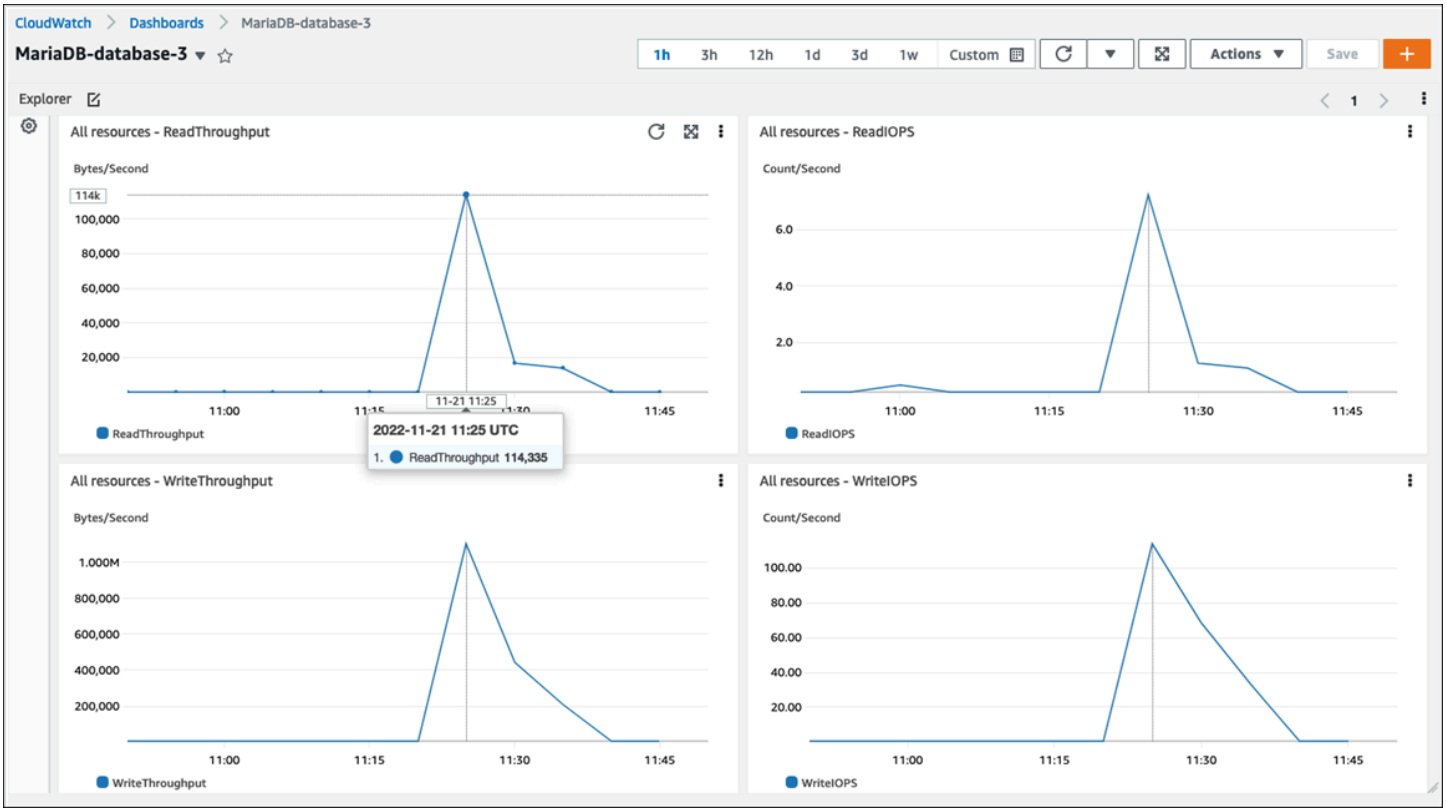
- `CPUUtilization`— CPU 使用率的百分比。
- `BinLogDiskUsage`— 二進位記錄所佔用的磁碟空間量。
- `FreeableMemory`— 可用隨機存取記憶體的數量。這代表的價值`MemAvailable`的欄位`/proc/meminfo`。
- `ReadIOPS`— 每秒的平均磁碟讀取 I/O 作業數。
- `WriteThroughput`— 本機儲存體每秒寫入磁碟的平均位元組數。
- `NetworkTransmitThroughput`— 資料庫節點上的傳出網路流量，結合了用於監控和複寫的資料庫流量和 Amazon RDS 流量。

如需 Amazon RDS 發佈的所有指標的完整參考資料CloudWatch，請參閱亞馬遜CloudWatch亞馬遜 RDS 的指標在亞馬遜 RDS 文檔中。

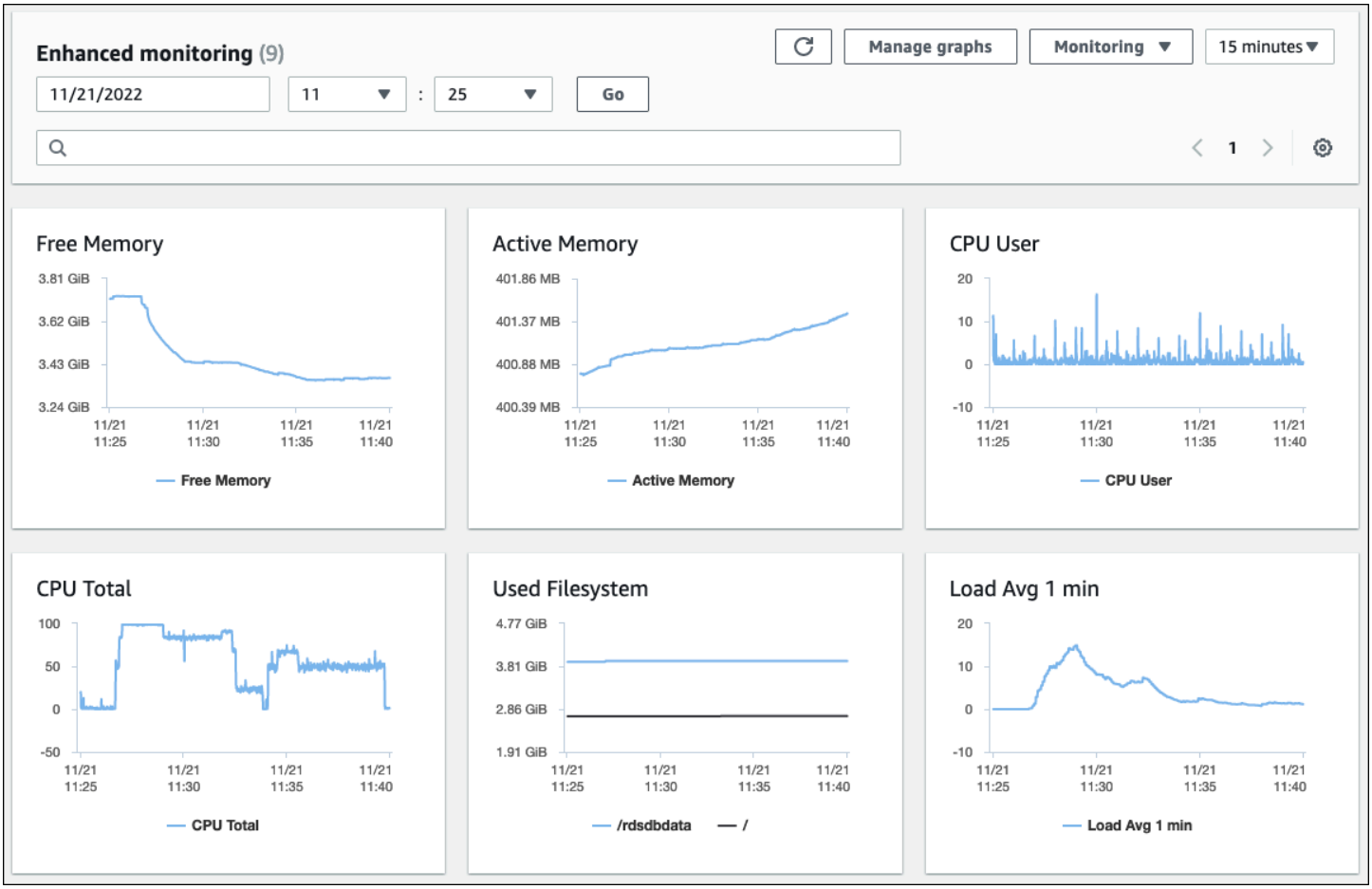
下圖顯示了實例CloudWatch顯示在亞馬遜 RDS 主控台上的亞馬遜 RDS 指標。



下列圖表顯示的類似測量結果CloudWatch儀表板。



另一組作業系統測量結果是由增強型監控對於亞馬遜 RDS。此工具提供即時系統指標和作業系統程序資訊，可讓您更深入瞭解 Amazon RDS for MariaDB 和 Amazon RDS for MySQL 資料庫執行個體的運作狀態。當你啟用增強型監控在資料庫執行個體上設定所需的粒度，此工具會收集作業系統指標和程序資訊，您可以在亞馬遜 RDS 控制台，如下面的屏幕。



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`— 使用者程式正在使用的 CPU 百分比。
- `memory.active`— 分配的內存量，以千字節為單位。
- `memory.cached`— 用於快取檔案系統型 I/O 的記憶體量。
- `loadAverageMinute.one`— 最後一分鐘內要求 CPU 時間的處理序數目。

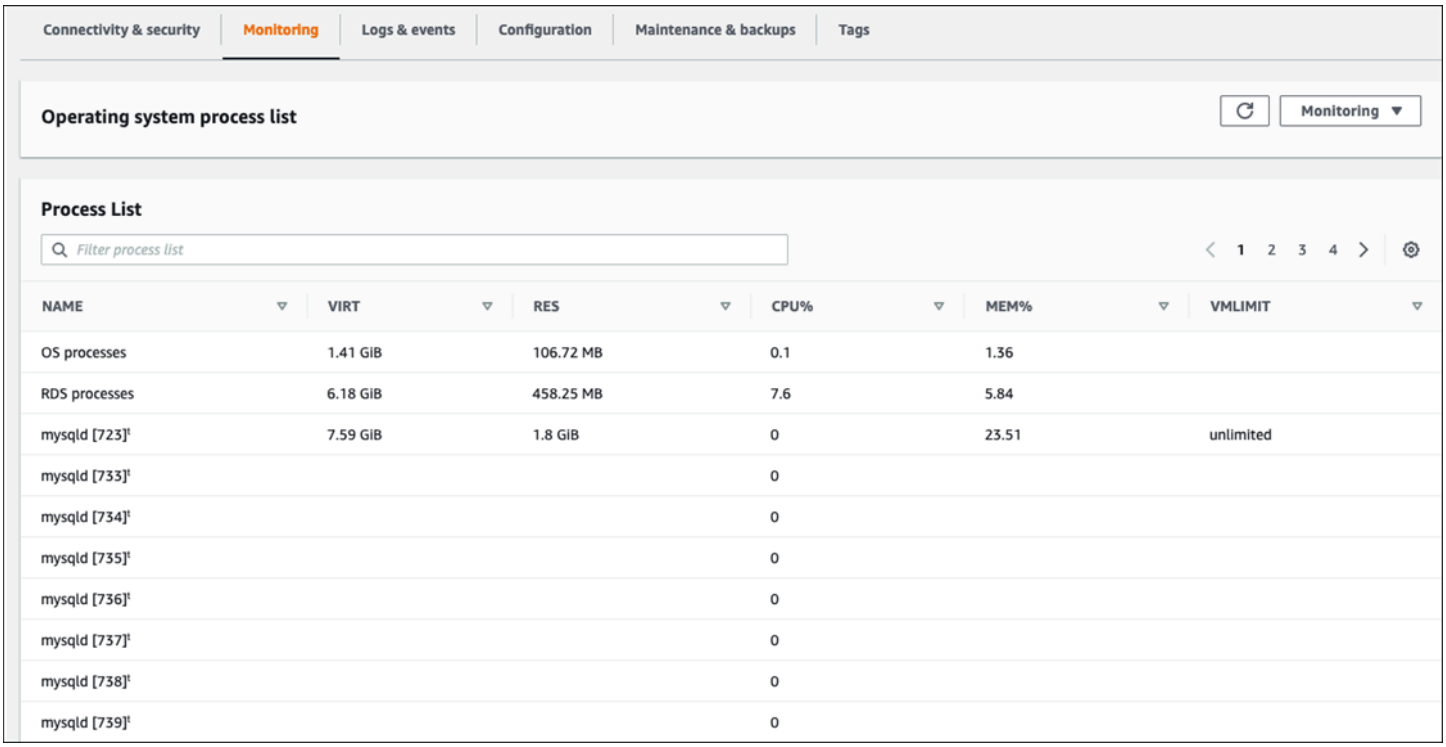
如需量度的完整清單，請參閱增強型監控中的 OS 指標在亞馬遜 RDS 文檔中。

在 Amazon RDS 主控台上，作業系統處理序清單會針對資料庫執行個體中執行的每個程序提供詳細資訊。該清單分為三個部分：

- OS 程序– 本節表示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— 本節代表的摘要AWS支援 Amazon RDS 資料庫執行個體所需的程序。例如，它包括 Amazon RDS 管理代理程式、監控和診斷程序以及類似程序。

- RDS 子處理程序— 本節顯示支援資料庫執行個體的 Amazon RDS 程序摘要 — 在本例中為mysqld進程及其線程。該mysqld線程嵌套在父項下方mysqld過程。

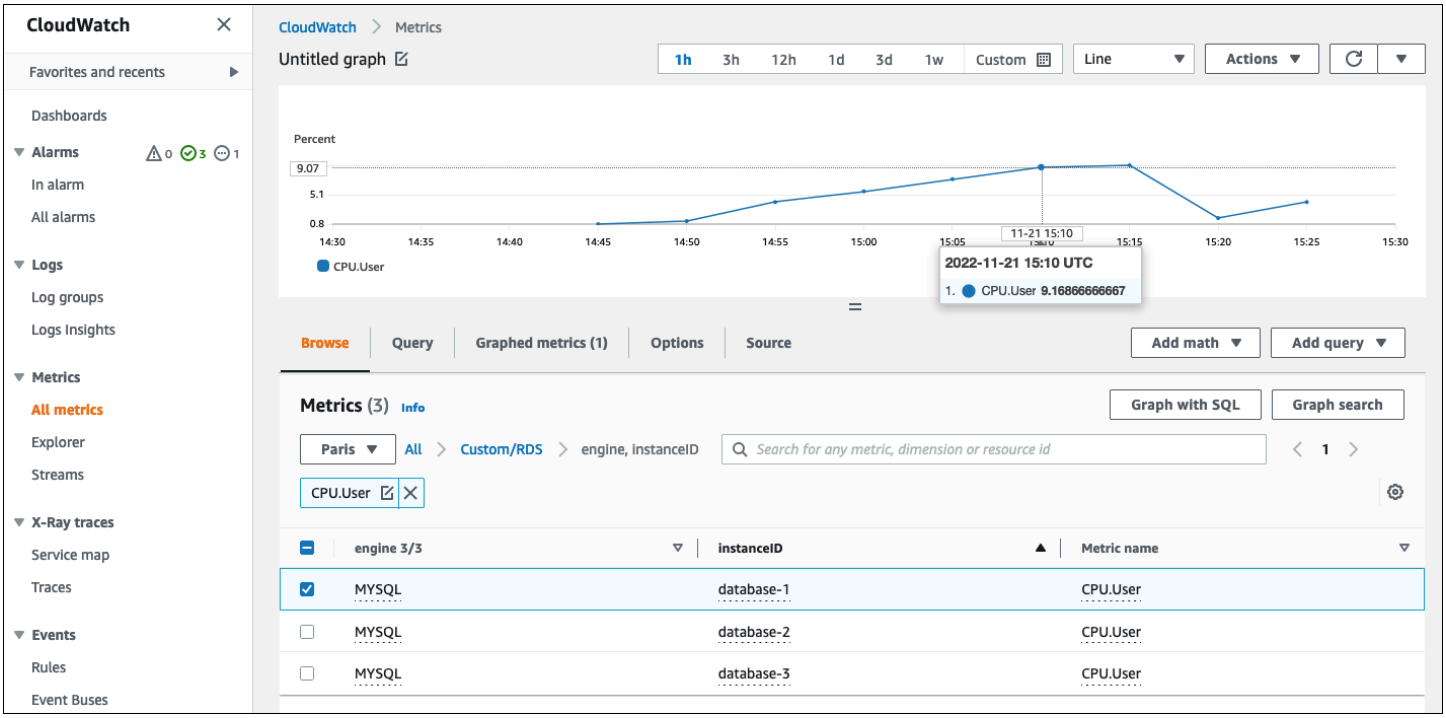
下列畫面圖例顯示 Amazon RDS 主控台中的作業系統程序清單。



Amazon RDS 將增強型監控中的指標交付到您的CloudWatch日誌帳戶。Amazon RDS 主控台上顯示的監控資料會從中擷取CloudWatch記錄檔。你也可以擷取資料庫執行個體的指標做為日誌串流從CloudWatch記錄檔。這些量度以 JSON 格式儲存。您可以從中使用增強型監控 JSON 輸出CloudWatch登入您選擇的監控系統。

為了在圖形上顯示CloudWatch儀表板並創建警報，該警報將在指標違反定義的閾值時啟動操作，您必須在中創建指標過濾器CloudWatch從CloudWatch記錄檔。如需詳細指示，請參閱AWS RE: 發表文章關於如何篩選增強型監控CloudWatch為 Amazon RDS 產生自動化自訂指標的日誌。

下列範例說明自訂量度CPU.User在Custom/RDS命名空間。此自訂量度是透過篩選cpuUtilization.user增強的監控量度CloudWatch記錄檔。



當測量結果在CloudWatch存儲庫，您可以在其中顯示和分析它CloudWatch儀表板、套用進一步的數學運算和查詢作業，並設定警示以監控此特定量度，並在觀察到的值不符合定義的警示條件時產生警示。

事件、記錄和稽核追蹤

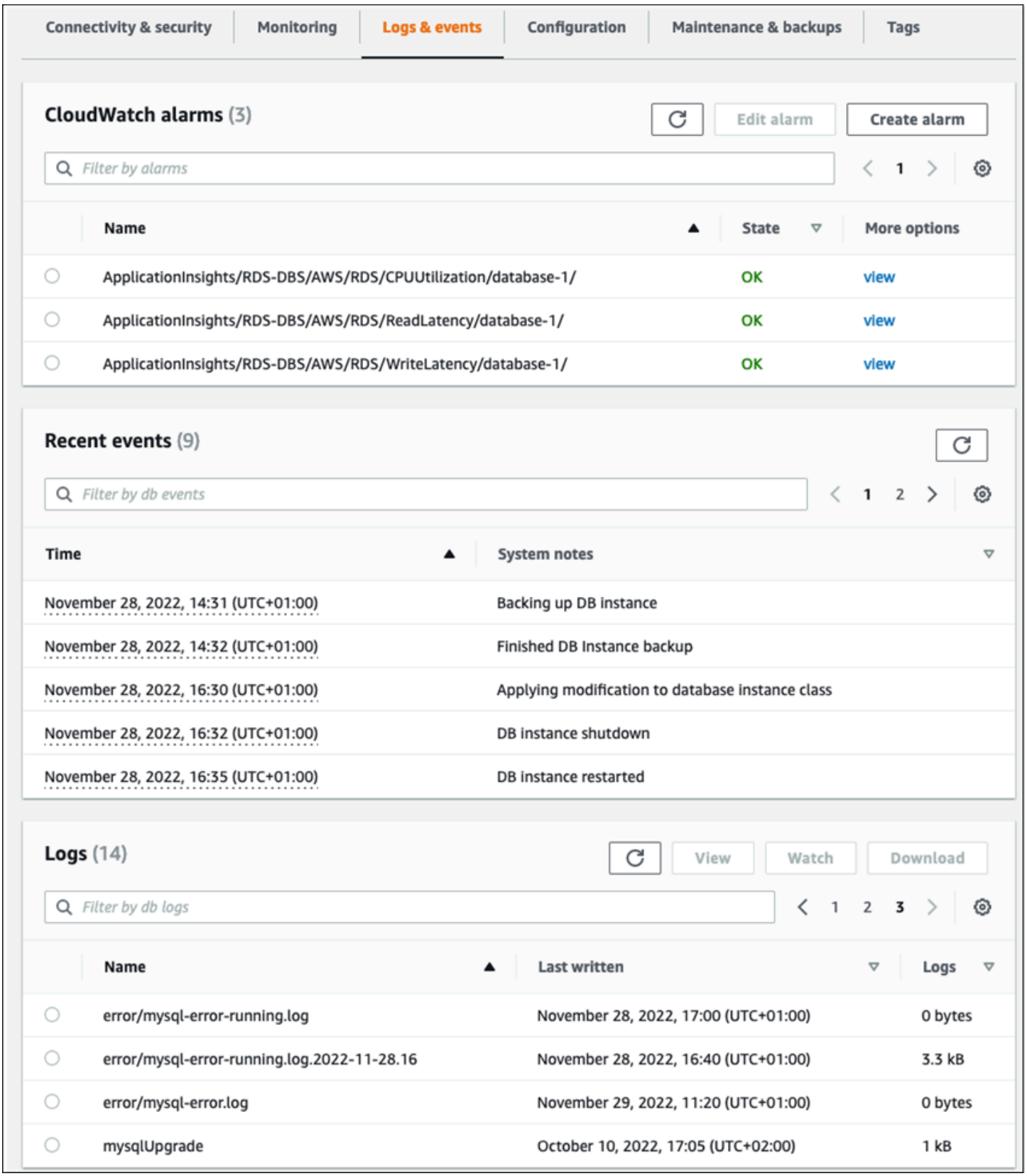
監控DB 執行個體指標和作業系統度、分析趨勢並將指標與基準值進行比較，並在值違反定義的閾值時產生警示，以協助您實現並維護 Amazon RDS 資料庫執行個體的可靠性、可用性、效能和安全性。但是，完整的解決方案還必須監視 MySQL 和 MariaDB 數據庫的數據庫事件，日誌文件和審計跟踪。

部分

- 亞馬遜 RDS 活動
- 資料庫記錄
- 稽核追蹤

亞馬遜 RDS 活動

一個亞馬遜 RDS 事件表示亞馬遜 RDS 環境中的變化。例如，當資料庫執行個體狀態從開始至可用，亞馬遜 RDS 生成的事件`RDS-EVENT-0088 The DB instance has been started`。亞馬遜 RDS 向亞馬遜交付活動EventBridge在接近實時的情況下。您可以透過亞馬遜 RDS 主控台存取事件 AWS CLI命令描述事件，或者亞馬遜 RDS API 操作DescribeEvents。下列畫面圖例顯示 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 事件和藍/綠部署事件。資訊包括：

- 來源名稱與來源型態；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"]

如需完整的參考資料，請參閱亞馬遜 RDS 事件類別和事件消息在亞馬遜 RDS 文檔中。

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的可用性、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、故障事件、對安全群組的修改以及許多其他通知的狀態變更。例如，如果您已設定僅供讀取複本資料庫執行個體以提供增強的資料庫效能和耐久性，建議您監控僅讀取複本資料庫執行個體關聯的事件類別。這是因為事件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。向負責小組發生此類事件的通知可協助及時緩解問題。亞馬遜EventBridge以及其他 AWS 服務，例如AWS LambdaAmazon 簡單佇列服務 (Amazon SQS) 和 Amazon 簡單通知服務 (Amazon SNS) 可協助您自動回應系統事件，例如資料庫可用性問題或資源變更。

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或使用 Amazon RDS API 來檢視事件，您可以使用描述事件命令如下。

```
$ 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"
        }
    ]
}
```

如果要長期存儲事件，直到指定的到期時間或永久存儲，則可以使用CloudWatch日誌記錄有關亞馬遜 RDS 生成的事件的信息。若要實作此解決方案，您可以使用 Amazon SNS 主題接收 Amazon RDS 事件通知，然後呼叫 Lambda 函數來記錄事件CloudWatch記錄檔。

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記錄檔。CloudWatch日誌與 Lambda 整合，並提供方便的方式來記錄事件資訊，方法是使用列印功能`stdout`。
2. 建立具有 Lambda 函數 (集合) 訂閱的 SNS 主題協議到拉姆達），並設置端點到您在上一個步驟中建立的 Lambda 函數的亞馬遜資源名稱 (ARN)。
3. 設定您的 SNS 主題以接收 Amazon RDS 事件通知。如需詳細指示，請參閱AWSRE: 發表文章關於如何讓您的亞馬遜 SNS 主題接收亞馬遜 RDS 通知。
4. 在 Amazon RDS 主控台上，建立新的事件訂閱。設置目標至 ARN，然後選取先前建立的 SNS 主題。設置來源類型和要包含的活動類別根據您的要求。如需詳細資訊，請參閱訂閱亞馬遜 RDS 事件通知在亞馬遜 RDS 文檔中。

資料庫記錄

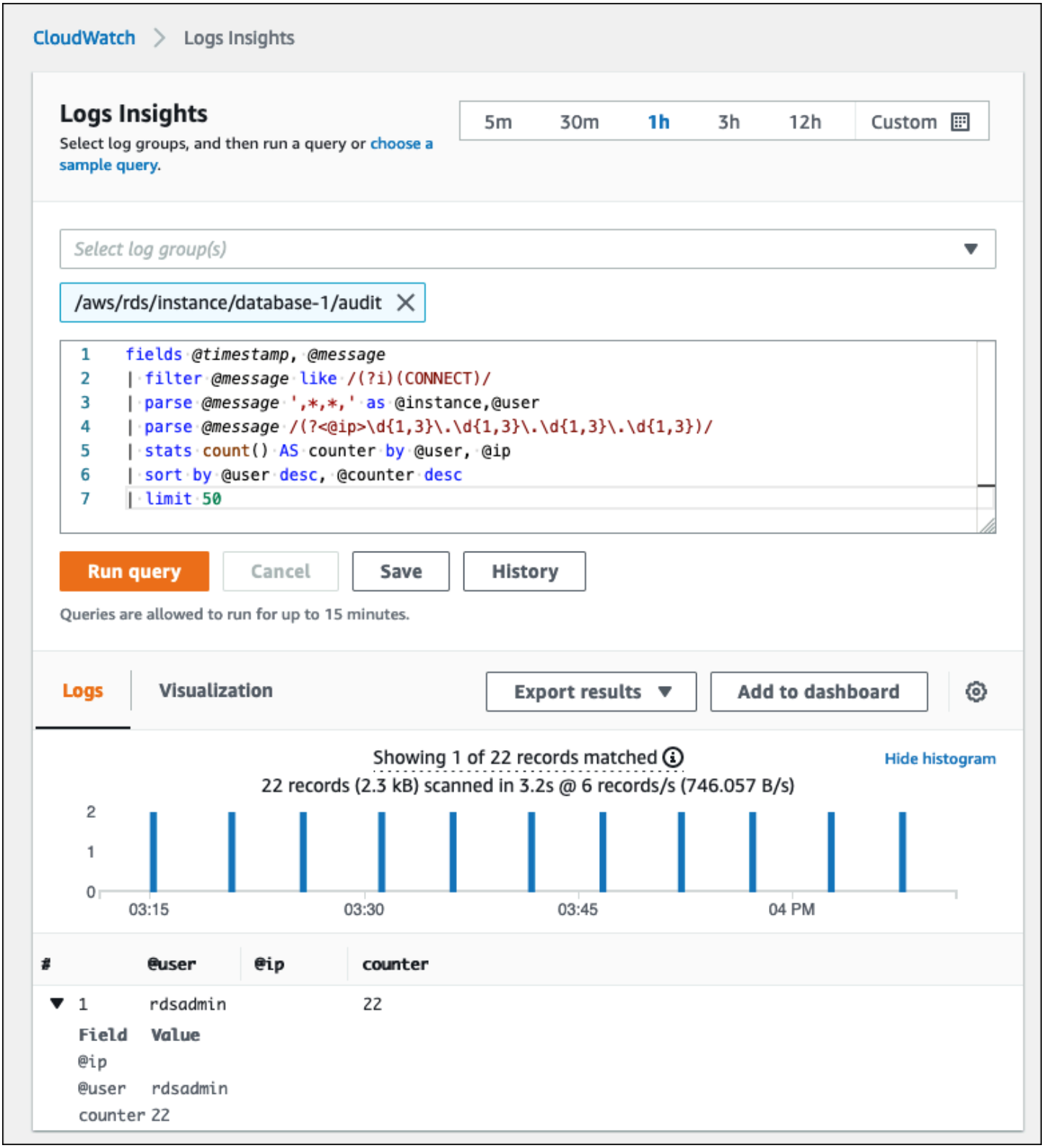
MySQL 和 MariaDB 資料庫會產生記錄，供您存取稽核和疑難排解。這些日誌是：

- 審計— 稽核追蹤是記錄伺服器活動的一組記錄。對於每個用戶端工作階段，它會記錄連線到伺服器的人員 (使用者名稱和主機)、執行了哪些查詢、存取了哪些資料表，以及變更了哪些伺服器變數。
- 錯誤— 此防護記錄包含伺服器的 (`mysqld`) 啟動和關閉時間，以及在伺服器啟動和關閉期間，以及伺服器執行期間發生的錯誤、警告和注意事項等診斷訊息。
- 將軍— 此日誌記錄的活動`mysqld`，包括每個用戶端的連線和中斷連線活動，以及從用戶端接收的 SQL 查詢。當您懷疑錯誤並想確切知道客戶端發送到哪些內容時，一般查詢日誌可能非常有用`mysqld`。
- 緩慢的查詢— 此記錄檔會提供花費很長時間才能執行的 SQL 查詢記錄。

作為最佳實踐，您應該將資料庫日誌從亞馬遜 RDS 發佈到亞馬遜CloudWatch日誌。同CloudWatch日誌，您可以對日誌數據進行實時分析，將數據存儲在高度耐用的存儲中，並使用CloudWatch記錄代理程式。你可以訪問並觀看您的數據庫日誌從亞馬遜 RDS 控制台。您也可以使用CloudWatch日誌見解以交互方式搜索和分析日誌數據CloudWatch記錄檔。下列範例說明稽核記錄檔上的查詢，該查詢會檢查多少次CONNECT事件會出現在記錄檔、連線者以及連線的用戶端 (IP 位址) 中。稽核記錄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
```

日誌見解查詢範例顯示rdsadmin連接到數據庫localhost每 5 分鐘一次，共 22 次，如下圖所示。這些結果表明活動源自內部 Amazon RDS 程序，例如監控系統本身。



記錄事件通常包含您要計數的重要訊息，例如與 MySQL 和 MariaDB 資料庫執行個體相關聯的作業的警告或錯誤。例如，如果作業失敗，可能會發生錯誤，並記錄到錯誤記錄檔中，如下所示：ERROR

1114 (HY000): The table zip_codes is full。您可能想要監視這些項目，以瞭解錯誤的趨勢。你可以建立自訂CloudWatch使用篩選器來自亞馬遜 RDS 日誌的指標啟用 Amazon RDS 資料庫日誌的自動監控，以監控特定記錄中的特定模式，並在違反預期行為時產生警示。例如」中，為記錄群組建立度量篩選器/aws/rds/instance/database-1/error這將監視錯誤日誌並搜索特定模式，例如ERROR。設定過濾器模式至ERROR和測量結果值至1。過濾器將檢測每個具有關鍵字的日誌記錄ERROR，它會為每個包含「ERROR」的日誌事件增加 1 的計數。創建過濾器後，您可以設置警報以在 MySQL 或 MariaDB 錯誤日誌中檢測到錯誤時通知您。

若要深入瞭解如何透過建立CloudWatch儀表板和使用CloudWatch日誌見解，請參閱部落格文章創建一個亞馬遜CloudWatch儀表板監控亞馬遜 RDS 和亞馬遜極光 MySQL。

稽核線索

稽核記錄 (或稽核日誌) 會提供 AWS 帳戶中與安全性相關且按時間順序排列的事件記錄。其中包括 Amazon RDS 的事件，提供影響您資料庫或雲端環境之活動順序的文件證明。在適用於 MySQL 或 MariaDB 的亞馬遜 RDS 中，使用稽核追蹤包括：

- 監視資料庫執行個體稽核記錄
- 監控亞馬遜 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：
  - 對參數或安全性組態執行的修改
  - 在資料庫結構描述、表格或列中執行的動作，或影響特定內容的動作
- 入侵偵測與調查
- 可疑活動偵測與調查
- 檢測授權問題；例如，識別普通或特權用戶濫用訪問權限

資料庫稽核追蹤會嘗試回答下列一般問題：誰查看或修改了數據庫中的敏感數據？ 這是什麼時候發生的？ 特定用戶從哪裡訪問數據？ 特權使用者是否濫用其無限制存取權限？

MySQL 和 MariaDB 都會使用 MariaDB 稽核外掛程式來實作資料庫執行個體稽核追蹤功能。這個插件記錄數據庫活動，如用戶登錄到數據庫和對數據庫運行的查詢。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，請參閱對於 MySQL 的瑪麗亞德審計插件的支持在亞馬遜 RDS 文檔中。稽核記錄中的記錄會以外掛程式所定義的特定格式儲存。您可以在MariaDB 服務器文檔。

該AWS 雲端您的稽核追蹤AWS帳戶由AWS CloudTrail服務。CloudTrail以事件形式擷取亞馬遜 RDS 的 API 呼叫。所有亞馬遜 RDS 動作都會記錄下來。CloudTrail提供使用者、角色或其他角色在 Amazon RDS 中執行的動作記錄AWS服務。事件包括在AWS管理主控台、AWS CLI，以及AWS軟體開發套件和 API。

範例

在典型的稽核案例中，您可能需要合併AWS CloudTrail追蹤資料庫稽核日誌和 Amazon RDS 事件監控功能。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，您的任務是識別誰進行了修改、變更的內容以及發生變更的時間。

若要完成工作，請依照下列步驟執行：

1. 列出發生在資料庫執行個體的 Amazon RDS 事件`database-1`並確定該類別中是否存在事件`configuration change`有消息`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若要搜尋CloudTrail事件在該地區database-1在步驟 1 中探索到的 Amazon RDS 事件周圍的期間內部署，以及在哪裡EventName=ModifyDBParameterGroup。

```
$ 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"
}
```


該CloudTrail事件顯示User1與角色Role1從AWS帳戶 111122223333 修改了數據庫參數組mariadb10-6-test，這是由資料庫執行個體使用database-1上2022-12-01 at 09:18:19 h。已修改兩個參數，並將其設定為下列值：

- innodb_log_buffer_size = 8388612
- innodb_write_io_threads = 8

附加CloudTrail和CloudWatch日誌功能

您可以透過檢視疑難排解過去 90 天的營運和安全性事件事件歷史在CloudTrail控制台。若要延長保留期限並利用其他查詢功能，您可以使用AWS CloudTrail湖。同AWS CloudTrailLake，您可以在事件資料存放區中保留事件資料長達七年。此外，此服務還支援複雜的 SQL 查詢，這些查詢提供的事件檢視比中的簡單索引鍵值查詢所提供的檢視更深入且更可自訂的事件檢視事件歷史。

若要監視您的稽核追蹤、設定警示，並在特定活動發生時收到通知，您需要配置CloudTrail將其追蹤記錄傳送至CloudWatch日誌。追蹤記錄儲存為之後CloudWatch記錄檔，您可以定義量度篩選器，以評估

記錄事件以符合字詞、片語或值，並將指標指派給量度篩選器。此外，您可以創建CloudWatch根據您指定的臨界值和時間週期產生的警示。例如，您可以設定將通知傳送給負責團隊的警示，以便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 基礎架構和 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。他們會通知並通知您的 IT 團隊持續發生的安全威脅、中斷、效能問題或系統故障。

資訊技術基礎架構程式庫 (ITIL)，特別是 IT 服務管理 (ITSM) 做法，會在監控與事件管理和事件管理最佳做法的焦點設定自動警示。

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 (針對可自動執行的項目) 有關 IT 環境中的變更、高風險動作或故障的通知。IT 警示是防範系統中斷或變更的第一道防線，可能會變成重大事件。藉由自動監控系統並針對中斷和風險變更產生警示，IT 團隊可以將停機時間降至最低，並降低隨附的高成本。

作為最佳做法，AWS架構良好的框架規定你使用監控產生警報式通知，以及主動監控和警報。使用CloudWatch或協力廠商監控服務來設定警示，以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、關閉和事件後審查活動，建立有效率且標準化的程序，以處理 IT 相關事件和事件。

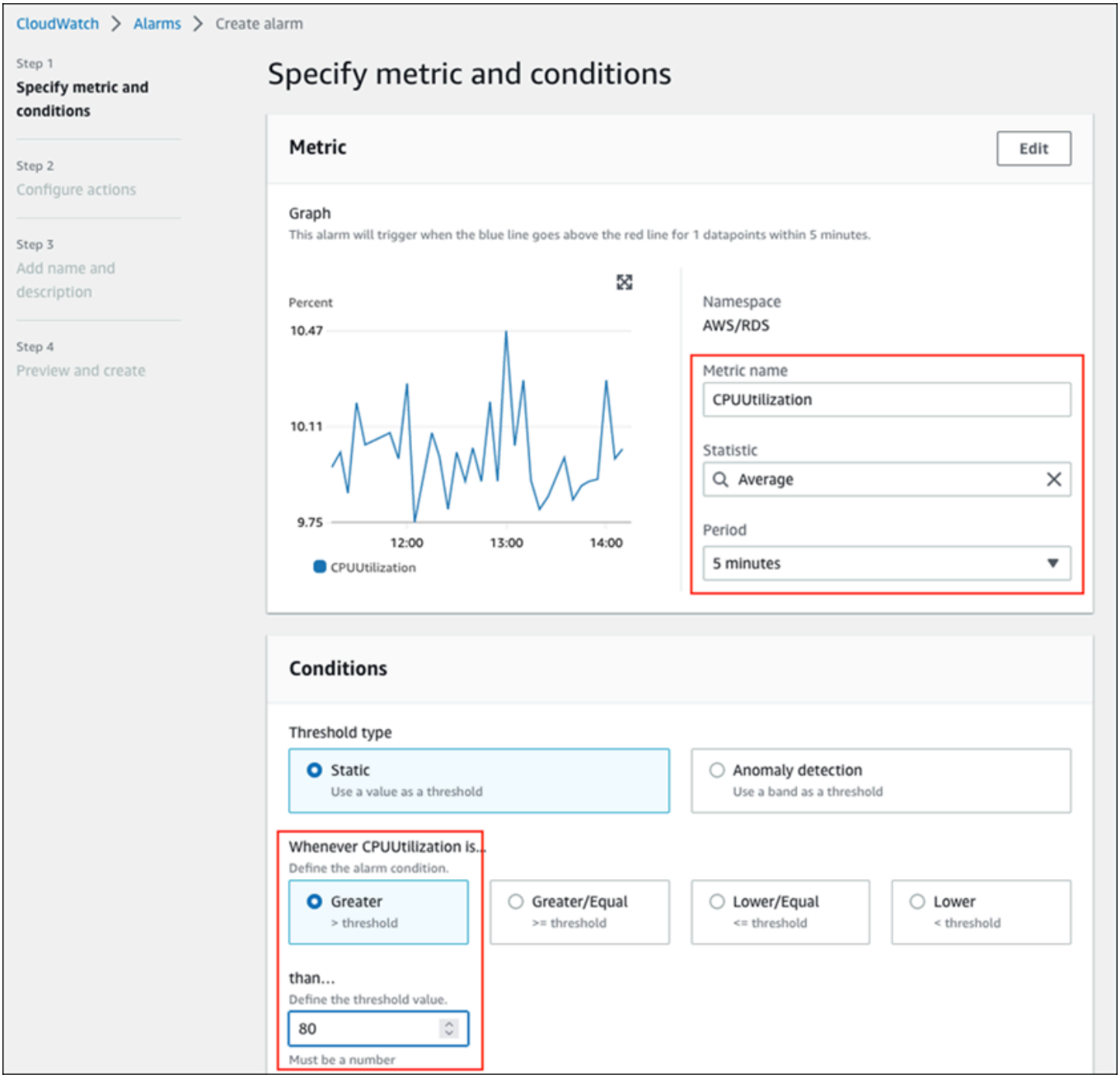
部分

- CloudWatch 警示
- EventBridge規則
- 指定動作、啟用及停用警示

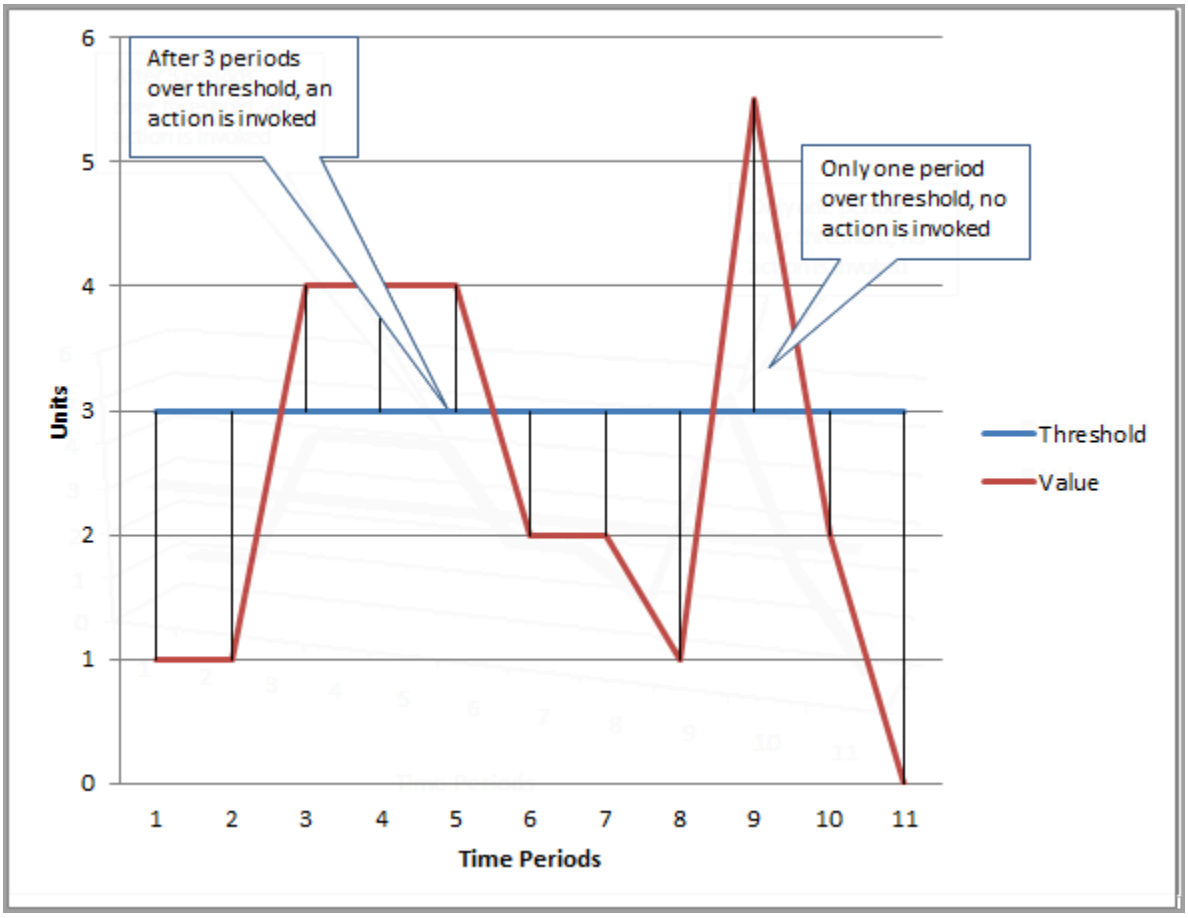
CloudWatch 警示

當您操作 Amazon RDS 資料庫執行個體時，您想要監控並產生不同類型的指標、事件和追蹤的警示。對於 MySQL 和 MariaDB 數據庫，信息的關鍵來源是DB 執行個體指標,作業系統度,事件、記錄檔和稽核追蹤。我們建議您使用CloudWatch警報，以監視您指定期間內的單一量度。

下列範例說明如何設定警示來監視CPUUtilization您所有 Amazon RDS 資料庫執行個體的指標 (CPU 使用率百分比)。您可以將任何資料庫執行個體的 CPU 使用率在 5 分鐘的評估期間超過 80% 時觸發警示。



這意味著警報進入ALARM說明您的任何資料庫是否有 5 分鐘以上的 CPU 使用率 (超過 80%)。警報仍保留在OK狀態 CPU 是否偶爾在短時間內突發到 80% 以上的使用率，然後再次降至臨界值以下。下圖說明了此邏輯。



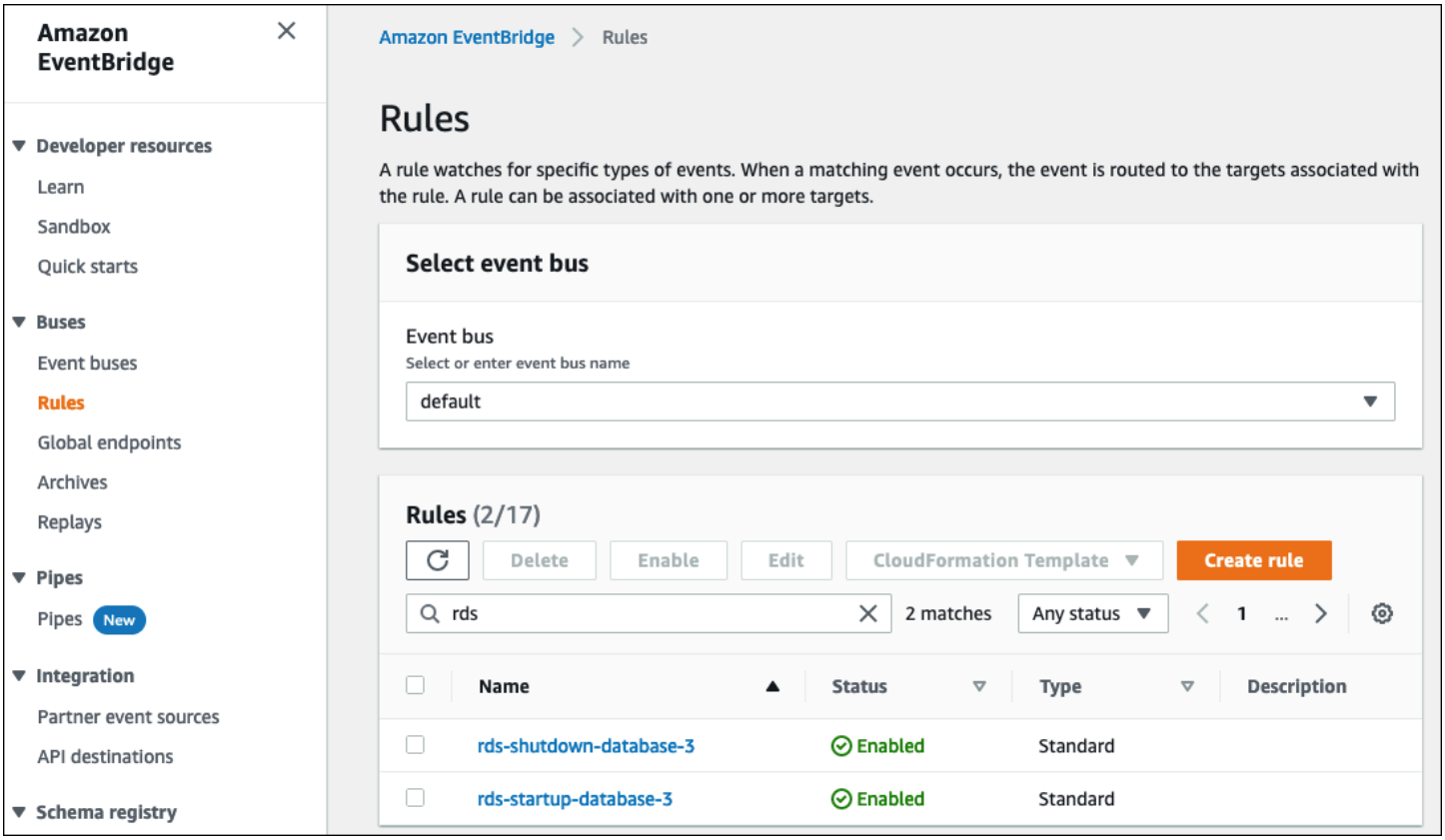
CloudWatch警報支援度量和複合警報。

- 一個公制報警手錶單CloudWatch度量，並且可以在度量上執行數學表達式。指標警示可以傳送 Amazon SNS 訊息，而這些訊息又可以根據指定臨界值在多個時段內相對於指定閾值的指標值採取一或多個動作。
- 一個複合報警以規則運算式為基礎，此運算式會評估多個警示的狀態，並進入ALARM只有在符合規則的所有條件時才會狀態。複合警報通常用於減少不必要的警示數目。例如，您可能有一個複合警示，其中包含數個已設定為永不採取動作的度量警示。當複合體中的所有個別度量警示都已在ALARM

CloudWatch鬧鐘只能觀看CloudWatch度量標準。如果您要根據錯誤、緩慢查詢或一般記錄建立警示，則必須建立CloudWatch來自日誌的指標。您可以完成此操作，如前面所述系統監控和事件、記錄和稽核追蹤區段, 使用篩選從記錄事件建立指標。同樣地，若要警示增強型監控指標，您必須在CloudWatch從CloudWatch記錄檔。

EventBridge 規則

亞馬遜 RDS 活動送到亞馬遜EventBridge，並且您可以使用EventBridge規則對這些事件做出反應。例如，您可以建立EventBridge規則會在某個特定資料庫執行個體停止或啟動時通知您並採取動作，如下列畫面所示。

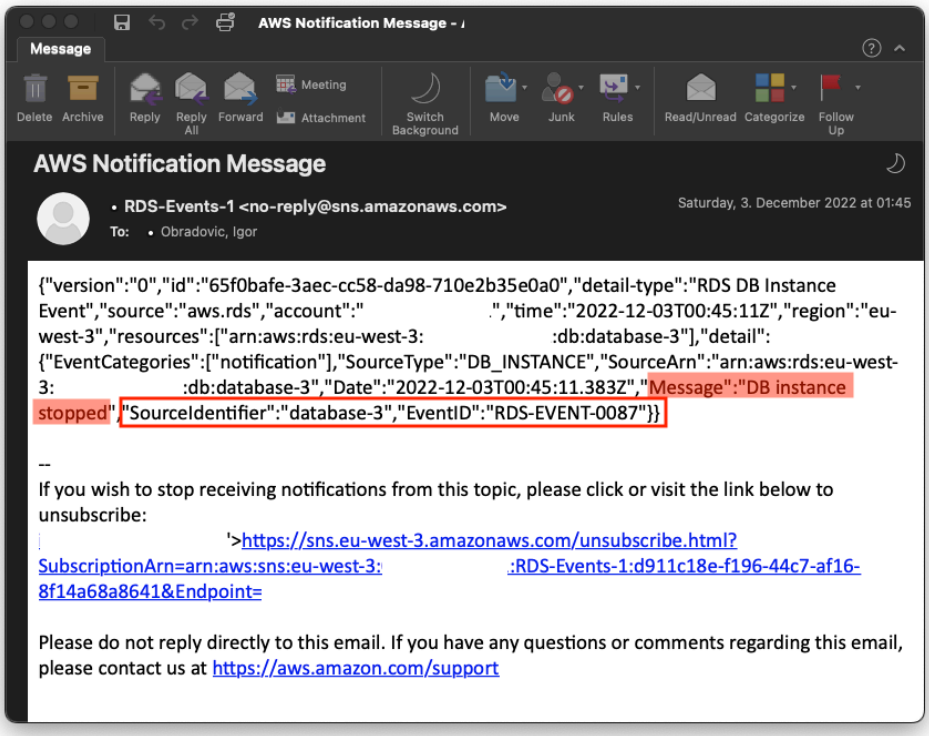


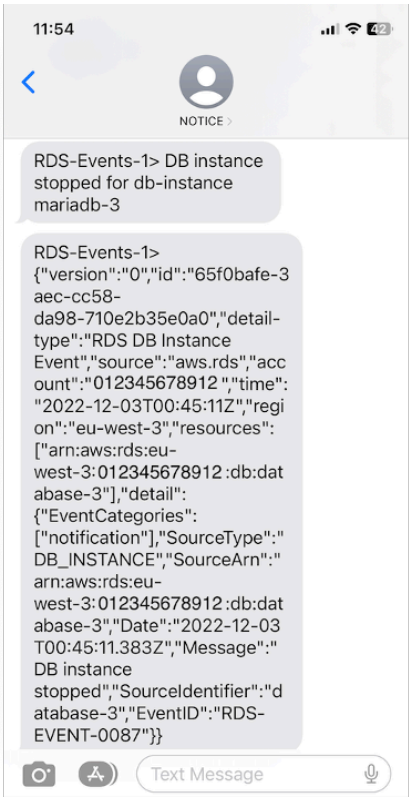
偵測到的規則The DB instance has been stopped活動具有亞馬遜 RDS 事件識別碼RDS-EVENT-0087，所以你設置Event Pattern要執行下列作業的規則屬性：

```
{
  "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"]
  }
}
```

此規則會監控資料庫執行個體database-3只有，並且手錶RDS-EVENT-0087事件。何時EventBridge檢測到事件，它將事件發送到資源或端點，稱為目標。在這裡，您可以指定 Amazon RDS 執行個體

關閉時要採取的動作。您可以將事件傳送到許多可能的目標，包括 SNS 主題、Amazon 簡單佇列服務 (Amazon SQS) 佇列、AWS Lambda功能，AWS Systems Manager自動化AWS Batch工作，亞馬遜 API 閘道，事件管理器中的響應計劃，功能AWS Systems Manager，以及其他許多人。例如，您可以建立將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。如果亞馬遜 RDS 數據庫實例`database-3`已停止，亞馬遜 RDS 交付事件`RDS-EVENT-0087`至EventBridge，它被檢測到的地方。EventBridge然後呼叫目標，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、啟用及停用警示

您可以使用CloudWatch警報以指定警報在兩者之間發生變化時應採取的動作`OK`,`ALARM`，以及`INSUFFICIENT_DATA`狀態。CloudWatch內建了與 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 彈性運算雲端 (Amazon EC2) 動作或 Amazon EC2 自動擴展群組動作。EventBridge通常用於編寫規則和定義在 Amazon RDS 指標觸發警示時採取動作的目標。CloudWatch將事件傳送至EventBridge每次一次CloudWatch警報會變更其狀態。您可以使用這些警報狀態更改事件來觸發事件目標EventBridge。如需詳細資訊，請參閱警報事件和EventBridge在CloudWatch文件。

您可能還需要管理警報；例如，在規劃的組態變更或測試期間自動停用警示，然後在計劃的動作結束時重新啟用警示。例如，如果您有規劃的排程資料庫軟體升級，且需要停機，而且您有警示會在資料庫無

法使用時啟動，您可以使用 API 動作來停用和啟用警示DisableAlarmActions和EnableAlarmActions，或disable-alarm-actions和enable-alarm-actions中的指令AWS CLI。您也可以檢視警報的歷史記錄CloudWatch主控台或使用DescribeAlarmHistoryAPI 動作或describe-alarm-history」中的指令AWS CLI。CloudWatch 會保留警示歷史記錄 2 週。在「」CloudWatch控制台，您可以選擇我的最愛和最近導航窗格中的菜單，用於設置和訪問您最喜歡的和最近訪問的警報。

後續步驟和資源

如需有關將關聯式資料庫移轉至AWS 雲端，請參閱下列策略AWS規定指導網站：

- 關聯式資料庫的移轉策略

你可以探索資料庫移轉模式為了step-by-step有關在中執行的特定關聯式資料庫的指示AWS 雲端，包括與監視、移轉和資料管理相關的工作。

使用該頁面上的過濾器查找模式AWS服務 (例如，移轉至 Amazon RDS 或亞馬遜極光)、按工作負載 (例如開放原始碼，其中包括 MySQL 和 MariaDB 資料庫)，或按計劃使用 (生產或試驗) 進行服務。

如需其他資源，請參閱下列內容：

- 亞馬遜關聯式資料庫服務使用
- 亞馬遜CloudWatch使用者指南
- 亞馬遜 RDS 常見問
- 效能洞見問答集
- 使用 Amazon 將 Amazon RDS 效能洞見計數器指標交付給第三方應用程式效能監控服務供應商CloudWatch度量資料流(AWS博客文章）
- 創建一個亞馬遜CloudWatch儀表板監控亞馬遜 RDS 和亞馬遜極光 MySQL(AWS博客文章）
- 使用效能洞見調整適用於 MySQL 的亞馬遜 RDS(AWS博客文章）

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
更新資訊	更新了有關出口商的信息，並添加了選擇導出器的準則。	2024年6月13日
初次出版	—	2023 年 6 月 30 日

AWS 規定指引詞彙

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

數字

7 R

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

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的內部部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Relational Database Service 服務 (Amazon RDS)，適用於 AWS 雲端中的 Oracle。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將現場部署 Oracle 資料庫遷移至 AWS 雲端 EC2 執行個體上的 Oracle。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。此移轉案例適用於 VMware Cloud on AWS，支援內部部署環境與之間的虛擬機器 (VM) 相容性和工作負載可攜性 AWS。在將基礎設施遷移至 VMware Cloud on AWS時，您可以使用內部部署資料中心的 VMware Cloud Foundation 技術。範例：將裝載 Oracle 資料庫的虛擬機器管理程序重新定位至 VMware 雲端。 AWS
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱以屬性為基礎的存取控制。

抽象的服務

請參閱受管理服務。

酸

請參閱原子性、一致性、隔離性、耐用性。

主動-主動式遷移

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

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。目標資料庫在遷移期間不接受任何交易。

聚合函數

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

AI

請參閱人工智慧。

艾奧運

請參閱人工智慧作業。

匿名化

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

反模式

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

應用控制

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

應用程式組合

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

人工智慧 (AI)

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

人工智慧操作 (AIOps)

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

非對稱加密

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

原子性、一致性、隔離性、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

組織遷移到 AWS 雲端時通常會經歷的四個階段：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)
- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段是 Stephen Orban 在雲端企業策略部落格文章「邁向 AWS 雲端優先的旅程與採用階段」部落格文章中定義的。如需其與 AWS 移轉策略之間關聯的詳細資訊，請參閱移轉準備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲存儲庫包括 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 ML 模型預測中的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

透過集中式管理和控管，提供分散式、分散式資料擁有權的架構架構。

資料最小化

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

資料周長

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

資料預先處理

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

數據來源

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

資料主體

正在收集和處理資料的個人。

資料倉儲

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

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

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

深度學習

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

defense-in-depth

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層加入多個控制項，以協助保護資源。例如，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

自動化並管理企業的關鍵業務流程（例如會計、MES 和專案管理）的系統。

信封加密

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

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

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

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全史詩包括身份和訪問管理，偵探控制，基礎結構安全性，數據保護和事件響應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

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

F

事實表

星型架構中的中央表格。它存儲有關業務運營的定量數據。事實資料表通常包含兩種類型的資料欄：包含計量的資料欄，以及包含維度表格外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來減少開發生命週期的理念。這是敏捷方法的關鍵組成部分。

故障隔離邊界

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

功能分支

請參閱分支。

特徵

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

功能重要性

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

特徵轉換

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

FGAC

請參閱精細的存取控制。

精細的存取控制 (FGAC)

使用多個條件來允許或拒絕訪問請求。

閃切遷移

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

G

地理阻塞

請參閱地理限制。

地理限制 (地理封鎖)

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

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被認為是遺留的，基於主幹的工作流程是現代的首選方法。

綠地策略

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

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。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，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

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

IIoT

請參閱工業物聯網。

不可變基礎設施

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

傳入 (輸入) VPC

在 AWS 多帳戶架構中，VPC 可接受、檢查和路由來自應用程式外部的網路連線。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

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

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

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

工業物聯網 (IIoT)

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

檢查 VPC

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

物聯網 (IoT)

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

可解釋性

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

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

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

IT 服務管理 (ITSM)

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

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤式存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中每個使用者和資料本身都明確指派一個安全性標籤值。使用者安全性標籤與資料安全性標籤之間的交集決定了使用者可以看到哪些列與欄。

登陸區域

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

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱以標示為基礎的存取控制。

最低權限

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

隨即轉移

見 7 盧比

小端序系統

首先儲存最低有效位元組的系統。另請參閱 「位元順序」。

較低的環境

請參閱環境。

M

機器學習 (ML)

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

主要分支

請參閱分支。

惡意軟體

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

受管理服務

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

製造執行系統

用於跟踪，監控，記錄和控制生產過程的軟件系統，可在現場將原材料轉換為成品。

MAP

請參閱 Migration Acceleration Program。

機制

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

成員帳戶

屬於 AWS 帳戶 中組織的管理帳戶以外的所有帳戶 AWS Organizations。一個帳戶一次只能是一個組織的成員。

MES

請參閱製造執行系統。

郵件佇列遙測傳輸 (MQTT)

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

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服

務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用 AWS 無伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱上 AWS的實作微服務。

Migration Acceleration Program (MAP)

提供諮詢支援、訓練和服務的 AWS 計畫，協助組織為移轉至雲端建立穩固的營運基礎，並協助抵消移轉的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

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

遷移工廠

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

遷移中繼資料

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

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使 AWS 用應用程式遷移服務將遷移重新託管到 Amazon EC2。

遷移組合評定 (MPA)

這是一種線上工具，可提供驗證商業案例以移轉至 AWS 雲端的資訊。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。所有 AWS 顧問和 APN 合作夥伴顧問均可免費使用 MPA 工具 (需要登入)。

遷移準備程度評定 (MRA)

使用 AWS CAF 獲得有關組織雲端準備狀態的見解、識別優勢和弱點，以及建立行動計劃以縮小已識別差距的過程。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

將工作負載移轉至 AWS 雲端時所使用的方法。如需詳細資訊，請參閱本詞彙表中的 7 Rs 項目，並參閱動員您的組織以加速大規模移轉。

機器學習 (ML)

請參閱機器學習。

現代化

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

現代化準備程度評定

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

單一應用程式 (單一)

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

MPA

請參閱移轉組合評估。

MQTT

請參閱佇列遙測傳輸的郵件。

多類別分類

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

可變的基礎

一種模型，用於更新和修改生產工作負載的現有基礎結構。為了提高一致性，可靠性和可預測性，AWS Well-Architected 框架建議使用不可變的基礎結構作為最佳實踐。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

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

OI

請參閱作業整合。

OLA

請參閱作業層級協定。

線上遷移

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

OPCA

請參閱開放程序通訊-統一架構。

開放程序通訊-統一架構 (OPC-UA)

用於工業自動化的 machine-to-machine (M2M) 通訊協定。OPC-UA 提供數據加密，身份驗證和授權方案的互操作性標準。

操作水準協議 (OLA)

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

操作準備程度檢討 (ORR)

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

操作技術

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

操作整合 (OI)

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

組織追蹤

由建立的追蹤 AWS CloudTrail 記錄中組織 AWS 帳戶 中所有人的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱CloudTrail文件中的為組織建立追蹤。

組織變更管理 (OCM)

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

原始存取控制 (OAC)

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

原始存取身分 (OAI)

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

ORR

請參閱作業整備檢閱。

OT

請參閱操作技術。

傳出 (輸出) VPC

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

P

許可界限

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

個人識別資訊 (PII)

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

PII

請參閱個人識別資訊。

手冊

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

公司

請參閱可編程邏輯控制器

PLM

請參閱產品生命週期管理

政策

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

混合持久性

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

組合評定

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

述詞

傳回`true`或的查詢條件`false`，通常位於子`WHERE`句中。

謂詞下推

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

預防性控制

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

委託人

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

隱私設計

一種系統工程方法，在整個工程過程中將隱私權納入考量。

私有託管區域

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

主動控制

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

產品生命週期管理 (PLM)

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

生產環境

請參閱環境。

可編程邏輯控制器 (PLC)

在製造業中，一台高度可靠且適應性強的計算機，可監控機器並自動化製造過程。

化名化

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

發布/訂閱 (發布/訂閱)

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

Q

查詢計劃

一系列步驟，如指示，用來存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

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

R

拉齐矩阵

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

回應性控制

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

保留

見 7 盧比

退休

見 7 盧比

旋轉

定期更新密碼以使攻擊者更難以存取認證的程序。

資料列與資料行存取控制 (RCAC)

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

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

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

S

SAML 2.0

許多身份提供者（IdPs）使用的開放標準。此功能可啟用聯合單一登入 (SSO)，因此使用者可以登入 AWS Management Console 或呼叫 AWS API 作業，而不必為組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

斯卡達

請參閱監督控制和資料擷取。

SCP

請參閱服務控制策略。

秘密

您以加密形式儲存的機密或受限制資訊，例如密碼或使用者認證。 AWS Secrets Manager它由秘密值及其中繼資料組成。密碼值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱秘密管理員說明文件中的秘密。

安全控制

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

安全強化

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

安全資訊與事件管理 (SIEM) 系統

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

安全回應自動化

預先定義且程式化的動作，其設計用來自動回應或修復安全性事件。這些自動化作業可做為偵探或回應式安全控制項，協助您實作 AWS 安全性最佳實務。自動回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

在其目的地的數據加密，通 AWS 服務 過接收它。

服務控制政策 (SCP)

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

服務端點

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

服務水準協議 (SLA)

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

服務等級指示器 (SLI)

對服務效能層面的測量，例如錯誤率、可用性或輸送量。

服務等級目標 (SLO)

代表服務狀況的目標測量結果，由服務層次指示器測量。

共同責任模式

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

暹

請參閱安全性資訊和事件管理系統。

單點故障 (SPF)

應用程式的單一重要元件發生故障，可能會中斷系統。

SLA

請參閱服務等級協議。

SLI

請參閱服務層級指示器。

SLO

請參閱服務等級目標。

split-and-seed 模型

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

痙攣

請參閱單一故障點。

星型綱要

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

Strangler Fig 模式

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

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監督控制與資料擷取 (SCADA)

在製造業中，使用硬體與軟體來監控實體資產與生產作業的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

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

T

標籤

作為組織 AWS 資源的中繼資料的索引鍵值配對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

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

任務清單

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

測試環境

請參閱環境。

訓練

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

傳輸閘道

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

主幹型工作流程

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

受信任的存取權

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

調校

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

雙比薩團隊

一個小 DevOps 團隊，你可以餵兩個比薩餅。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

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

無差別的任務

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

較高的環境

請參閱環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

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

漏洞

會危及系統安全性的軟體或硬體瑕疵。

W

暖快取

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

溫暖的數據

不常存取的資料。查詢此類資料時，通常可以接受中度緩慢的查詢。

視窗功能

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

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

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

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。