AWS 事件偵測與回應概念和程序

AWS 事件偵測與回應使用者指南

版本 February 3, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 事件偵測與回應使用者指南: AWS 事件偵測與回應概念和程序

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS 事件偵測與回應？

AWS 事件偵測與回應為符合資格的 AWS Enterprise Support 客戶提供主動的事件參與，以減少失敗的可能性，並加速關鍵工作負載從中斷情況復原。事件偵測與回應可促進您與 AWS 協作，以開發針對每個上線工作負載自訂的執行手冊和回應計劃。

事件偵測與回應提供下列主要功能：

- 改善可觀測性：AWS 專家提供指引，協助您在工作負載的應用程式和基礎結構層之間定義指標和警示並使其相互關聯，以便及早偵測到中斷情形。
- 5 分鐘回應時間：事件管理工程師 (IME) 負責全年無休監控您的上線工作負載，以偵測關鍵事件。IME 會在警示觸發後 5 分鐘內回應，或回應您對事件偵測與回應提出的關鍵業務支援案例。
- 加速解決：IME 使用專為您工作負載開發的預先定義自訂執行手冊在 5 分鐘內回應、代表您建立支援案例，以及管理工作負載的事件。IME 為事件提供單一執行緒擁有權，並讓您與合適的 AWS 專家保持互動，直到事件解決為止。
- 降低失敗的可能性：解決之後，IME 會為您提供事件後檢討 (提出請求時)。此外，AWS 專家會與您一起運用學到的經驗來改善事件回應計畫和執行手冊。您也可以利用 AWS Resilience Hub 在工作負載上持續追蹤恢復能力。

主題

事件偵測與回應的使用條款

下列清單概述使用 AWS 事件偵測與回應的重要需求和限制。在您使用服務之前，務必確實了解此資訊，因為其內容涵蓋了支援計劃需求、上線程序和最短訂閱期間等層面。

- AWS 事件偵測與回應適用於直接和合作夥伴轉售的 Enterprise Support 帳戶。
- AWS 事件偵測與回應不適用於合作夥伴主導支援的帳戶。
- 您必須在事件偵測與回應服務期間內，隨時維護 AWS Enterprise Support。如需相關資訊，請參閱 Enterprise Support。終止 Enterprise Support 會同時從 AWS 事件偵測與回應服務中將其移除。

- AWS 事件偵測與回應上的所有工作負載都必須經過工作負載上線程序。
- 帳戶訂閱 AWS 事件偵測與回應的最短期間為九十 (90) 天。所有取消請求都必須在預定的取消生效日期前三十 (30) 天提交。
- AWS 會依照AWS 隱私權聲明中所述處理您的資訊。

> **Note**
>
> 如要了解事件偵測與回應帳單相關問題，請參閱取得 AWS 帳單的協助。

事件偵測與回應的架構

AWS 事件偵測與回應會與您現有的環境整合，如下圖所示。架構包含下列服務：

- Amazon EventBridge：Amazon EventBridge 是工作負載與 AWS 事件偵測與回應之間的唯一整合點。透過 Amazon EventBridge，即可使用 AWS 管理的預先定義規則從您的監控工具 (例如 Amazon CloudWatch) 擷取警示。若要允許事件偵測與回應建置和管理 EventBridge 規則，請安裝服務連結角色。若要進一步了解這些服務，請參閱什麼是 Amazon EventBridge 和 Amazon EventBridge 規則、什麼是 Amazon CloudWatch，以及使用 AWS Health 的服務連結角色。
- AWS Health：AWS Health 可讓您持續了解資源效能，以及 AWS 服務 和帳戶的可用性。事件偵測與回應會使用 AWS Health 來追蹤工作負載在 AWS 服務 上使用的事件，並且在收到工作負載發出的提醒時通知您。若要進一步了解 AWS Health，請參閱什麼是 AWS Health。
- AWS Systems Manager：Systems Manager 會提供統一的使用者介面，以便在您的 AWS 資源中進行自動化和任務管理。AWS 事件偵測與回應會託管工作負載的相關資訊，包括工作負載架構圖、警示詳細資訊，及其在 AWS Systems Manager 文件中對應的事件管理執行手冊 (如需詳細資訊，請參閱 AWS Systems Manager 文件)。若要進一步了解 AWS Systems Manager，請參閱什麼是 AWS Systems Manager。
- 您專屬的執行手冊：事件管理執行手冊定義 AWS 事件偵測與回應在事件管理期間執行的動作。您專屬的執行手冊會告訴 AWS 事件偵測與回應要聯絡的人員、如何取得聯絡，以及要提供哪些資訊。

事件偵測與回應方面的角色和責任

AWS 事件偵測與回應 RACI (負責、當責、備詢及通訊) 資料表概述了關於事件偵測與回應的各種活動的角色和責任。此資料表有助於定義客戶和 AWS 事件偵測與回應團隊在資料收集、營運準備情況審核、帳戶組態、事件管理和事件後檢討等任務方面的參與程度。

活動	客戶	事件偵測與回應
資料收集		
客戶和工作負載簡介	備詢	負責
架構	負責	當責
作業	負責	當責
決定要設定的 CloudWatch 警示	負責	當責
定義事件回應計畫	負責	當責
填寫加入問卷	負責	當責
營運準備情況審核		
對工作負載執行結構良好審核 (WAR)	備詢	負責
驗證事件回應	備詢	負責
驗證警示矩陣	備詢	負責
識別工作負載使用的主要 AWS 服務	當責	負責
帳戶組態		
在客戶帳戶中建立 IAM 角色	負責	通訊
使用建立的角色安裝受管 EventBridge 規則	通訊	負責
測試 CloudWatch 警示	負責	當責

活動	客戶	事件偵測與回應
確認客戶警示和事件偵測與回應連動	通訊	負責
更新警示	負責	備詢
更新執行手冊	備詢	負責
事件管理		
主動通知事件偵測與回應偵測到的事件	通訊	負責
提供事件回應	通訊	負責
提供事件解決方案/基礎結構還原	負責	備詢
事件後檢討		
請求事件後檢討	負責	通訊
提供事件後檢討	通訊	負責

事件偵測與回應的區域可用性

AWS 事件偵測與回應為託管於下列任何 AWS 區域 中的 AWS Enterprise Support 帳戶提供英文、日文、中文和韓文服務：

AWS 區域	名稱
美國東部 (維吉尼亞北部) 區域	us-east-1
美國東部 (俄亥俄) 區域	us-east-2
美國西部 (加利佛尼亞北部) 區域	us-west-1
美國西部 (奧勒岡) 區域	us-west-2
加拿大 (中部) 區域	ca-central-1

AWS 區域	名稱
加拿大西部 (卡加利) 區域	ca-west-1
南美洲 (聖保羅) 區域	sa-east-1
歐洲 (法蘭克福) 區域	eu-central-1
歐洲 (愛爾蘭) 區域	eu-west-1
歐洲 (倫敦) 區域	eu-west-2
歐洲 (巴黎) 區域	eu-west-3
歐洲 (斯德哥爾摩) 區域	eu-north-1
歐洲 (蘇黎世) 區域	eu-central-2
Europe (Milan) Region	eu-south-1
歐洲 (西班牙) 區域	eu-south-2
亞太地區 (孟買)	ap-south-1
亞太區域 (東京)	ap-northeast-1
亞太地區 (首爾)	ap-northeast-2
亞太區域 (新加坡)	ap-southeast-1
亞太區域 (雪梨)	ap-southeast-2
亞太地區 (香港)	ap-east-1
亞太地區 (大阪)	ap-northeast-3
亞太區域 (海德拉巴)	ap-south-2
亞太區域 (雅加達)	ap-southeast-3
亞太區域 (墨爾本)	ap-southeast-4

AWS 區域	名稱
亞太地區 (馬來西亞)	ap-southeast-5
非洲 (開普敦)	af-south-1
以色列 (特拉維夫)	il-central-1
中東 (阿拉伯聯合大公國)	me-central-1
中東 (巴林)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (美國西部)	us-gov-west-1

開始使用事件偵測與回應

工作負載和警示是 AWS 事件偵測與回應的核心。AWS 會與您密切合作，一起定義和監控對您的業務至關重要的特定工作負載。AWS 可協助您設定警示，讓您的團隊快速得知重大的效能問題或客戶影響。在事件偵測與回應內正確設定警示，對於主動監控和快速事件回應來說相當重要。

工作負載

您可以使用 AWS 事件偵測與回應來選取特定工作負載，以進行監控和關鍵事件管理。工作負載是一組資源和程式碼，搭配運作以提供商業價值。工作負載可能是構成銀行付款入口網站或客戶關係管理 (CRM) 系統的所有資源和程式碼。您可以將工作負載託管在單一 AWS 帳戶或多個 AWS 帳戶中。

例如，您可能將單體式應用程式託管在單一帳戶中 (例如，下圖中的員工績效應用程式)。您也可能將應用程式 (例如圖中的 Storefront Webapp) 分成多個微型服務，並分佈到不同的帳戶中。工作負載可能會與其他應用程式或工作負載共用資源，例如資料庫，如下圖所示。

若要從工作負載上線開始著手，請參閱工作負載上線和工作負載上線問卷。

警報

警示是事件偵測與回應中重要的一環，因為警示可讓您了解應用程式和基礎 AWS 基礎結構的效能。AWS 會與您一起定義適當的指標和警示閾值，只有在對您監控的工作負載產生重大影響時才會觸發。目標是讓警示與您指定的解決人員互動，接著解決人員就可與事件管理團隊協作，以快速緩解任何問題。警示應設定為，只有在效能顯著降低或客戶體驗需要立即關注時才進入警示狀態。一些重要的警示類型包括，指出業務影響的警示、Amazon CloudWatch Canary，以及監控相依性的彙總警示。

若要開始使用警示擷取，請參閱警示擷取和警示擷取問卷。

> **Note**
>
> 若要變更您的執行手冊、工作負載資訊或 AWS 事件偵測與回應所監控的警示，請參閱 在事件偵測與回應中請求變更已上線的工作負載。

事件偵測與回應上線

AWS 會與您一起在 AWS 事件偵測與回應中將工作負載和警示上線。您可以使用事件偵測與回應客戶命令列介面 (CLI) 工具，或在 事件偵測與回應中的工作負載上線和警示擷取問卷 中，將您要上線的工作負載和警示的重要資訊提供給 AWS。

下圖顯示事件偵測與回應中工作負載上線和警示擷取的流程：

工作負載上線

在工作負載上線期間，AWS 會與您一起了解工作負載，以及如何在事件期間為您提供支援。您可以提供工作負載的重要資訊來協助緩解影響。

重要輸出：

- 一般工作負載資訊
- 架構詳細資訊，包括圖表
- 執行手冊資訊
- 客戶啟動事件

警示擷取

AWS 會與您一起將警示上線。AWS 事件偵測與回應可透過 Amazon EventBridge，從 Amazon CloudWatch 和第三方應用程式效能監控 (APM) 工具擷取警示。將警示上線可讓您主動偵測事件並自動參與。如需詳細資訊，請參閱從與 Amazon EventBridge 直接整合的 APM 擷取警示。

重要輸出：

- 警示矩陣

下表列出在 AWS 事件偵測與回應中將工作負載上線所需的步驟。此資料表顯示每一項任務的範例持續時間。每一項任務的實際日期是根據您的團隊和排程的可用狀況來定義。

事件偵測與回應中的工作負載上線和警示擷取問卷

此頁面提供在 AWS 事件偵測與回應中將工作負載上線，以及設定警示以擷取至服務中時，需要填寫的問卷。工作負載上線問卷涵蓋有關工作負載、其架構詳細資訊和事件回應聯絡人的一般資訊。在警示擷取問卷中，您可以指定應在事件偵測與回應中針對您的工作負載觸發建立事件的關鍵警示，以及有關應聯絡哪些人員和應採取哪些動作的執行手冊資訊。正確完成這些問卷是為您的 AWS 工作負載設定監控和事件回應程序的關鍵步驟。

下載工作負載上線問卷。

下載警示擷取問卷。

工作負載上線問卷 - 一般問題

一般問題

問題	回應範例
企業名稱	Amazon Inc.
此工作負載的名稱 (包括任何縮寫)	Amazon Retail Operations (ARO)
此工作負載的主要最終使用者和功能。	此工作負載是電子商務應用程式，可讓最終使用者購買各種商品。此工作負載是我們業務的主要營收來源。
此工作負載適用的合規和/或監管要求，以及事件發生後 AWS 需採取的任何行動。	工作負載會處理病患的病歷記錄，其內容必須保持安全和機密。

工作負載上線問卷 - 架構問題

架構問題

問題	回應範例
用於定義屬於此工作負載之資源的 AWS 資源標籤清單。AWS 會使用這些標籤來識別此工作負載的資源，以在事件期間加速提供支援。	appName：Optimax environment：生產

問題	回應範例
Note 標籤會區分大小寫。如果您提供多個標籤，此工作負載使用的所有資源都必須具有相同的標籤。	
此工作負載所使用的 AWS 服務清單，以及這些服務所在的 AWS 帳戶和區域。 Note 為每一項服務建立新的一列。	Route 53：將網際網路流量路由到 ALB。 帳戶：123456789101 區域：US-EAST-1、US-WEST-2
此工作負載所使用的 AWS 服務清單，以及這些服務所在的 AWS 帳戶和區域。 Note 為每一項服務建立新的一列。	ALB：將傳入流量路由到 ECS 容器的目標群組。 帳戶：123456789101 區域：不適用
此工作負載所使用的 AWS 服務清單，以及這些服務所在的 AWS 帳戶和區域。 Note 為每一項服務建立新的一列。	ECS：主要商業邏輯機群的運算基礎結構。負責處理傳入的使用者請求並查詢持續性層。 帳戶：123456789101 區域：US-EAST-1
此工作負載所使用的 AWS 服務清單，以及這些服務所在的 AWS 帳戶和區域。 Note 為每一項服務建立新的一列。	RDS：Amazon Aurora 叢集會儲存 ECS 商業邏輯層存取的使用者資料。 帳戶：123456789101 區域：US-EAST-1

問題	回應範例
此工作負載所使用的 AWS 服務清單，以及這些服務所在的 AWS 帳戶和區域。 Note 為每一項服務建立新的一列。	S3：儲存網站靜態資產。 帳戶：123456789101 區域：不適用
詳細說明任何未上線的上游/下游元件，如遇到中斷情形，這些元件可能會影響此工作負載。	身分驗證微型服務：將防止使用者載入其病歷記錄，因為不會驗證使用者的身分。
此工作負載是否有任何內部部署或非 AWS 元件？ 如果有，這些元件是什麼？其功能為何？	所有傳入/傳出 AWS 的網際網路流量都會透過我們的內部部署代理服務進行路由。
在可用區域和區域層級提供任何手動或自動容錯移轉/災難復原計畫的詳細資訊。	暖待命。在成功率持續下降期間自動容錯移轉至 US-WEST-2。

警示擷取問卷

執行手冊問題

問題	回應範例
AWS 將透過 支援 案例與工作負載聯絡人互動。當此工作負載的警示觸發時，誰是主要聯絡人？ 指定您偏好的會議應用程式，AWS 將會在事件期間請求這些詳細資訊。 Note 如果未提供偏好的會議應用程式，則 AWS 將在事件期間與您聯絡，並提供 Chime 橋接器供您加入。	應用程式團隊 app@example.com +61 2 3456 7890

問題	回應範例
如果在事件期間無法聯繫主要聯絡人，請依偏好的通訊順序提供呈報聯絡人和時間表。	1. 10 分鐘後，如果主要聯絡人沒有回應，則聯絡： John Smith - 應用程式主管 john.smith@example.com +61 2 3456 7890 2. 10 分鐘後，如果 John Smith 沒有回應，則聯絡： Jane Smith - 營運經理 jane.smith@example.com +61 2 3456 7890
AWS 會在整個事件過程中，定期透過支援案例傳達更新。是否還有其他聯絡人應收到這些更新？	john.smith@example.com、jane.smith@example.com

警示矩陣

提供以下資訊以識別將與 AWS 事件偵測與回應互動的一組警示，以代表您的工作負載建立事件。來自 AWS 事件偵測與回應的工程師檢閱您的警示後，就會提供其他上線步驟。

AWS 事件偵測與回應關鍵警示條件：

- AWS 事件偵測與回應警示只有在對監控的工作負載有重大業務影響 (收入損失/客戶體驗降級) 且需要操作員立即注意時，才應進入「警示」狀態。
- AWS 事件偵測與回應警示也必須同時或在互動之前，與工作負載的解決人員互動。AWS事件管理者會在緩解過程中與您的解決人員合作，而且不會作為一線回應者，再呈報給您。
- AWS 事件偵測與回應警示閾值必須設定為適當的閾值和持續時間，以便只要警示觸發，就必須進行調查。如果警示在「警示」和「正常」狀態之間切換，這樣的影響就足以保證操作員回應和注意。

違反條件的 AWS 事件偵測與回應政策：

只有在事件發生時，才會依個別案例評估這些條件。事件管理團隊與您的技術客戶經理 (TAM) 合作調整警示，在極少數情況下才會停用監控，例如懷疑客戶警示未遵循此條件，以及定期與事件管理團隊進行不必要的互動等。

> **Important**
>
> 在提供聯絡地址時提供群組分佈電子郵件地址，讓您可以控制收件人新增和刪除，而不需進行執行手冊更新。
> 如果您希望 AWS 事件偵測與回應團隊在傳送初始參與電子郵件之後致電網站可靠性工程 (SRE) 團隊，請提供該團隊的聯絡電話號碼。

警示矩陣表

指標名稱/ARN/閾值	Description	備註	請求的動作
工作負載量/ *CW ## ARN*/ 5 分鐘內 5 個資料點的 CallCount < 100000，將遺失的資料視為遺失	此指標代表傳入工作負載的請求數量，於 Application Load Balancer 層級衡量。 此警示很重要，因為傳入請求大幅下降可能表示上游網路連線發生問題，或我們的 DNS 實作發生問題，導致使用者無法存取工作負載。	警示在上週進入「警示」狀態 10 次。此警示有誤報的風險。已規劃閾值檢閱。 有問題？「否」或「是」(若否，保留空白)：此警示在某一批特定任務執行期間頻繁切換。 解決人員：網站可靠性工程師	傳送電子郵件至 *SRE@example.com* 以通知網站可靠性工程團隊參與 針對 ELB 和 Amazon Route 53 服務建立 AWS 支援 案例。 如果需要「立即」行動：檢查 EC2 可用記憶體/磁碟空間，並透過電子郵件通知 *##* 團隊重新啟動執行個體，或執行日誌排清。(若不需要立即行動，則保留空白)
工作負載請求延遲/ *CW ## ARN*/	此指標代表工作負載履行的 HTTP 請求的 p90 延遲。	警示在上週進入「警示」狀態 0 次。 有問題？「否」或「是」(若否，保留空	傳送電子郵件至 *SRE@example.com* 以通知網站可靠性工程團隊參與

指標名稱/ARN/閾值	Description	備註	請求的動作
5 分鐘內 5 個資料點的 p90 延遲 > 100 毫秒，將遺失的資料視為遺失	此警示代表延遲 (網站客戶體驗的重要量值)。	白)：此警示在某一批特定任務執行期間頻繁切換。 解決人員：網站可靠性工程師	針對 ECW 和 RDS 服務建立 AWS 支援 案例。 如果需要「立即」行動：檢查 EC2 可用記憶體/磁碟空間，並透過電子郵件通知##團隊重新啟動執行個體，或執行日誌排清。(若不需要立即行動，則保留空白)
工作負載請求可用性/ *CW ## ARN*/ 5 分鐘內 5 個資料點的可用性 < 95%，將遺失的資料視為遺失。	此指標代表工作負載履行的 HTTP 請求的可用性 (每個期間的 HTTP 數量 200/請求數量)。 此警示代表工作負載的可用性。	警示在上週進入「警示」狀態 0 次。 有問題？「否」或「是」(若否，保留空白)：此警示在某一批特定任務執行期間頻繁切換。 解決人員：網站可靠性工程師	傳送電子郵件至 *SRE@example.com* 以通知網站可靠性工程團隊參與 針對 ELB 和 Amazon Route 53 服務建立 AWS 支援 案例。 如果需要「立即」行動：檢查 EC2 可用記憶體/磁碟空間，並透過電子郵件通知##團隊重新啟動執行個體，或執行日誌排清。(若不需要立即行動，則保留空白)
New Relic 警示範例			

指標名稱/ARN/閾值	Description	備註	請求的動作
端對端整合測試/ *CW ## ARN*/ 3 分鐘內 1 分鐘指標的失敗率 3%，將遺失的資料視為遺失 工作負載識別碼：端對端測試工作流程，AWS 區域：US-EAST-1，AWS 帳戶 ID：012345678910	此指標會測試請求是否可周遊工作負載的每一層。如果此測試失敗，則表示處理商業交易發生嚴重失敗。 此警示代表處理工作負載商業交易的能力。	警示在上週進入「警示」狀態 0 次。 有問題？「否」或「是」(若否，保留空白)：此警示在某一批特定任務執行期間頻繁切換。 解決人員：網站可靠性工程師	傳送電子郵件至 *SRE@example.com* 以通知網站可靠性工程團隊參與 針對 Amazon Elastic Container Service 和 Amazon DynamoDB 服務建立 AWS 支援案例。 如果需要「立即」行動：檢查 EC2 可用記憶體/磁碟空間，並透過電子郵件通知##團隊重新啟動執行個體，或執行日誌排清。(若不需要立即行動，則保留空白)

事件偵測與回應中的工作負載探索

AWS 會與您合作，盡可能了解您工作負載的相關內容。AWS 事件偵測與回應會使用此資訊來建立執行手冊，以在事件期間為您提供支援。必要的資訊會在 事件偵測與回應中的工作負載上線和警示擷取問卷 中擷取。最好在 AppRegistry 上註冊工作負載。如需詳細資訊，請參閱《AppRegistry 使用者指南》。

重要輸出：

- 工作負載資訊，例如工作負載的說明、架構圖表、聯絡人和呈報詳細資訊。
- 工作負載如何在每個 AWS 區域中採用 AWS 服務的詳細資訊。
- 團隊用來偵測關鍵工作負載影響的警示。

讓工作負載訂閱事件偵測與回應

為您要訂閱 AWS 事件偵測與回應的每個工作負載建立支援案例。

- 對於單一帳戶工作負載：從工作負載的帳戶或您的付款人帳戶提交。
- 對於多帳戶工作負載：從您的付款人帳戶提交並列出所有帳戶 ID。

> **Important**
>
> 若從錯誤的帳戶提交支援案例來讓工作負載訂閱事件偵測與回應，則可能會導致延遲並需要其他資訊。

若要訂閱工作負載，請完成以下步驟：

1. 開啟 AWS 支援 中心，然後選取建立案例。您只能從已註冊 Enterprise Support 的帳戶訂閱工作負載。下列範例顯示支援中心主控台。

2. 輸入下列資訊以完成填寫支援案例表單：

   - 選取技術支援。
   - 針對服務，選擇事件偵測與回應。
   - 針對類別，選擇將新工作負載上線。
   - 針對嚴重性，選擇一般指引。

3. 輸入此變更的主旨。例如，您可以輸入 [上線] AWS 事件偵測與回應 - *workload_name*。
4. 輸入此變更的說明。例如，您可以輸入這是關於在 AWS 事件偵測與回應中將工作負載上線的請求。

   請求中務必包含下列資訊：

   - 工作負載名稱：您的工作負載名稱
   - 帳戶 ID：ID1、ID2、ID3 (以此類推)。這些是您要在 AWS 事件偵測與回應中上線的帳戶
   - 語言：如需事件偵測與回應支援的語言清單，請參閱 事件偵測與回應的區域可用性。
5. 在其他聯絡人 - 選用區段中，輸入您要接收有關此請求之通信的任何電子郵件 ID。

   以下是其他聯絡人 - 選用區段的範例。

> **Important**
>
> 如果未在其他聯絡人 - 選用區段中新增電子郵件 ID，可能會使 AWS 事件偵測與回應上線程序延遲。

6. 選擇提交。

   提交請求後，您可以新增您組織的其他電子郵件。若要新增電子郵件，請回覆案例，然後在其他聯絡人 - 選用區段中新增電子郵件 ID。

   以下是回覆按鈕和其他聯絡人 - 選用區段的範例。

建立訂閱請求的支援案例後，備妥下列兩份文件，以繼續進行工作負載上線程序：

- AWS 工作負載架構圖。
- 事件偵測與回應中的工作負載上線和警示擷取問卷：完成填寫問卷中與您要上線之工作負載相關的所有資訊。如果您要將多個工作負載上線，請為每個工作負載建立新的上線問卷。如有關於填寫上線問卷的任何疑問，請聯絡您的技術客戶經理 (TAM)。

> **Note**
>
> 請勿使用附加檔案選項將這兩份文件附加至案例。AWS 事件偵測與回應團隊將回覆案例並提供 Amazon Simple Storage Service 上傳工具連結，供您上傳文件。

如需如何在 AWS 事件偵測與回應中建立案例，以請求變更現有的已上線工作負載的資訊，請參閱 在事件偵測與回應中請求變更已上線的工作負載。如需如何將工作負載離線的資訊，請參閱 讓工作負載從事件偵測與回應離線。

在事件偵測與回應中定義和設定警示

AWS 會與您一起定義指標和警示，讓您能夠檢視應用程式及其基礎 AWS 基礎結構的效能。我們要求遵循下列準則來定義和設定警示的閾值：

- 警示只會在對監控的工作負載有重大影響 (收入損失或客戶體驗降級導致效能大幅降低) 且需要操作員立即注意時，才會進入「警示」狀態。
- 警示也必須在與事件管理團隊互動的同時或之前，讓指定的工作負載解決人員參與。事件管理工程師會在緩解過程中與您指定的解決人員合作，而且不會作為一線回應者，再呈報給您。
- 警示閾值必須設定為適當的閾值和持續時間，以便只要警示觸發，就必須進行調查。如果警示在「警示」和「正常」狀態之間轉換，這樣的影響就足以保證操作員回應和注意。

警示類型：

- 描述業務影響層級並傳遞相關資訊以進行簡單的故障偵測的警示。
- Amazon CloudWatch Canary。如需詳細資訊，請參閱 Canary 和 X-Ray 追蹤及 X-Ray。
- 彙總警示 (監控相依性)

下表提供範例警示，這些全都是使用 CloudWatch 監控系統。

指標名稱/警示閾值	警示 ARN 或資源 ID	如果此警示觸發	若已參與，則截止這些服務的付費支援案例
API 錯誤/ 10 個資料點的錯誤數 >= 10	arn:aws:cloudwatch:us-west-2:000000000000:alarm:E2MPmimLambda-Errors	票證分給資料庫管理員 (DBA) 團隊	Lambda、API Gateway
ServiceUnavailable (Http 狀態碼 503) 5 分鐘內 10 個資料點 (不同用戶端) 的錯誤數 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	票證分給服務團隊	Lambda、API Gateway
ThrottlingException (Http 狀態碼 400)	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	票證分給服務團隊	EC2、Amazon Aurora

指標名稱/警示閾值	警示 ARN 或資源 ID	如果此警示觸發	若已參與，則截止這些服務的付費支援案例
5 分鐘內 10 個資料點 (不同用戶端) 的錯誤數 >=3			

如需詳細資訊，請參閱AWS 事件偵測與回應監控與可觀測性。

如果您偏好使用自動化工具來將警示上線，事件偵測與回應命令列介面 (CLI) 可協助您部署並將警示上線。如需詳細資訊，請參閱AWS 事件偵測與回應 CLI。

重要輸出：

- 工作負載上警示的定義和組態。
- 完成填寫上線問卷中的警示詳細資訊。

主題

- 在事件偵測與回應中建立符合您業務需求的 CloudWatch 警示
- 使用 CloudFormation 範本在事件偵測與回應中建置 CloudWatch 警示
- 事件偵測與回應中 CloudWatch 警示的範例使用案例

在事件偵測與回應中建立符合您業務需求的 CloudWatch 警示

當您建立 Amazon CloudWatch 警示時，您可以採取幾個步驟來確保您的警示最合乎您的業務需求。

> **Note**
>
> 如需讓 AWS 服務 在事件偵測與回應上線的建議 CloudWatch 警示範例，請參閱 AWS re:Post 上的事件偵測與回應警示最佳實務。

檢閱您提議的 CloudWatch 警示

檢閱您提議的警示，確保這些警示只會在對監控的工作負載有重大影響 (收入損失或客戶體驗降級導致效能大幅降低) 且需要操作員立即注意時，才會進入「警示」狀態。例如，您是否認為這是重大警示，因此當它進入「警示」狀態時，您必須立即回應？

以下是可能代表重大業務影響的建議指標，例如影響最終使用者使用應用程式的體驗：

- CloudFront：如需詳細資訊，請參閱檢視 CloudFront 和邊緣函數指標。
- Application Load Balancer：盡可能為 Application Load Balancer 建立下列警示，這是最佳實務：
  - HTTPCode_ELB_5XX_Count
  - HTTPCode_Target_5XX_Count

  上述警示可讓您監控來自 Application Load Balancer 後方或其他資源後方之目標的回應。如此更方便您識別 5XX 錯誤的來源。如需詳細資訊，請參閱 Application Load Balancer 的 CloudWatch 指標。
- Amazon API Gateway：如果您在 Elastic Beanstalk 中使用 WebSocket API，請考慮使用下列指標：
  - 整合錯誤率 (篩選出 5XX 錯誤)
  - 整合延遲
  - 執行錯誤

  如需詳細資訊，請參閱使用 CloudWatch 指標來監控 WebSocket API 執行。
- Amazon Route 53：監控 EndPointUnhealthyENICount 指標。此指標是處於自動復原狀態的彈性網路介面數量。此狀態表示，解決人員嘗試復原與端點相關聯的一或多個 Amazon Virtual Private Cloud 網路介面 (以 EndpointId 指定)。在復原過程中，端點會以有限的容量運作。在完全復原之前，端點無法處理 DNS 查詢。如需詳細資訊，請參閱透過 Amazon CloudWatch 監控 Amazon Route 53 Resolver 端點。

驗證您的警示組態

在您確認提議的警示符合您的業務需求後，請驗證警示的組態和歷史記錄：

- 對照指標的圖形趨勢，驗證指標進入「警示」狀態的閾值。
- 驗證用於輪詢資料點的期間。每 60 秒輪詢一次資料點，有助於及早偵測到事件。
- 驗證 DatapointToAlarm 組態。在大多數情況下，最佳實務是將此項設定為 3 之 3 或 5 之 5。發生事件時，警示會在設定為 [60 second metrics with 3 out of 3 DatapointToAlarm] 時經過 3 分鐘後觸

發，或設定為 [60 second metrics with 5 out of 5 DatapointToAlarm] 時經過 5 分鐘後觸發。使用此組合可消除雜訊警示。

> **Note**
>
> 上述建議可能因您使用服務的方式而有所不同。每項 AWS 服務在工作負載內的運作方式有所不同。而且相同服務在多個位置使用時，運作方式也可能不同。您必須確實了解工作負載如何利用饋送警示的資源，以及上游和下游的作用。

驗證警示處理遺失資料的情形

有些指標來源不會定期傳送資料至 CloudWatch。對於這些指標，最佳實務是將遺失的資料視為 notBreaching。如需詳細資訊，請參閱設定 CloudWatch 警示如何處理遺失資料和避免過早轉換到警示狀態。

例如，如果指標監控錯誤率，但沒有錯誤，則指標會回報無資料 (nil) 資料點。如果您將警示設定為將遺失資料視為遺失，則單一違規資料點後面接著兩個無資料 (nil) 資料點會導致指標進入「警示」狀態 (3 個資料點中的 3 個)。這是因為遺失資料組態會評估在評估期間的最後已知資料點。

在指標監控錯誤率的情況下，若未發生服務降級，您可以假設無資料是良好情況。最佳實務是將遺失的資料視為 notBreaching，以便將遺失的資料視為「正常」，且指標不會在單一資料點上進入「警示」狀態。

檢閱每個警示的歷史記錄

如果警示的歷史記錄顯示其經常進入「警示」狀態後快速復原，則該警示可能會對您造成問題。務必調整警示，以防止雜訊或誤報。

驗證基礎資源的指標

確定您的指標查看有效的基礎資源，並使用正確的統計資料。如果警示設定為檢閱無效的資源名稱，則警示可能無法追蹤基礎資料。這可能會導致警示進入「警示」狀態。

建立複合警示

如果您對事件偵測與回應操作提供大量上線警示，則可能需要建立複合警示。複合警示可減少需上線的警示總數。

使用 CloudFormation 範本在事件偵測與回應中建置 CloudWatch 警示

為了加速在 AWS 事件偵測與回應中上線，並減少建置警示所需的工作量，AWS 為您提供了 CloudFormation 範本。這些範本包括常用上線服務的最佳化警示設定，例如 Application Load Balancer、Network Load Balancer 和 Amazon CloudFront。

使用 CloudFormation 範本建置 CloudWatch 警示

1. 使用提供的連結下載範本：

NameSpac	指標	Compariso nOperator (閾值)	Period	Datapoint sToAlarm	TreatMiss ingData	統計數字	範本連結
Applicati on Elastic Load Balancer	(m1+m2)/ (m1+m2+m m4)*100 m1=HTTP(de_Target _2XX_Cou t m2=HTTP(de_Target _3XX_Cou t m3=HTTP(de_Target _4XX_Cou t m4=HTTP(de_Target _5XX_Cou t	LessThanT hreshold(95)	60	3 之 3	missing	總和	範本

NameSpac	指標	Compariso nOperator (閾值)	Period	Datapoint sToAlarm	TreatMiss ingData	統計數字	範本連結
Amazon CloudFron t	TotalErro rRate	GreaterTh anThresho ld(5)	60	3 之 3	notBreach ing	平均數	範本
Applicati on Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3 之 3	notBreach ing	上限	範本
Network Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3 之 3	notBreach ing	上限	範本

2. 檢閱下載的 JSON 檔案，確保其符合您組織的營運和安全程序。
3. 建立 CloudFormation 堆疊：

> **Note**
>
> 以下步驟使用標準 CloudFormation 堆疊建立程序。如需詳細步驟，請參閱在 CloudFormation 主控台上建立堆疊。

a. 在以下網址開啟 AWS CloudFormation 主控台：https://console.aws.amazon.com/cloudformation。

b. 選擇 Create Stack (建立堆疊)。

c. 選擇範本已準備就緒，然後從本機資料夾上傳範本檔案。

以下是建立堆疊畫面的範例。

d. 選擇下一步。

e. 輸入下列必填資訊：

- AlarmNameConfig 和 AlarmDescriptionConfig：輸入警示的名稱和說明。
- ThresholdConfig：修訂閾值以符合應用程式的需求。
- DistributionIDConfig：確定分佈 ID 指向您建立 CloudFormation 堆疊所在帳戶中的正確資源。

f. 選擇下一步。

g. 檢閱 PeriodConfig、EvalutionPeriodConfig 和 DatapointsToAlarmConfig 欄位中的預設值。最佳實務是使用這些欄位的預設值。您可以視需要進行調整，以符合應用程式的需求。

h. 視需要選擇性地輸入標籤和 SNS 通知資訊。最佳實務是開啟終止保護，防止意外刪除警示。若要開啟終止保護，請選取已啟用選項按鈕，如下列範例所示：

i. 選擇下一步。

j. 檢閱您的堆疊設定，然後選擇建立堆疊。

k. 建立堆疊後，您會看到 Amazon CloudWatch 警示清單中列出警示，如下列範例所示：

4. 您在正確的帳戶和 AWS 區域中建立所有警示之後，請通知您的技術客戶經理 (TAM)。AWS 事件偵測與回應團隊會檢閱新警示的狀態，然後繼續上線。

事件偵測與回應中 CloudWatch 警示的範例使用案例

下列使用案例提供如何在事件偵測與回應中使用 Amazon CloudWatch 警示的範例。這些範例示範如何設定 CloudWatch 警示以監控各種 AWS 服務的關鍵指標和閾值，讓您能夠識別和回應可能影響應用程式和工作負載可用性與效能的潛在問題。

範例使用案例 A：Application Load Balancer

您可以建立下列 CloudWatch 警示，以指出潛在的工作負載影響。若要這樣做，您可以建立指標數學，在成功連線低於特定閾值時發出警示。若要了解可用的 CloudWatch 指標，請參閱 Application Load Balancer 的 CloudWatch 指標

指標：`HTTPCode_Target_3XX_Count;HTTPCode_Target_4XX_Count;HTTPCode_Target_5XX_Count`

```
(m1+m2)/(m1+m2+m3+m4)*100 m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 = HTTP Code 4xx || m4 = HTTP Code 5xx
```

NameSpace：AWS/ApplicationELB

ComparisonOperator(Threshold)：小於 x (x = 客戶的閾值)。

Period：60 秒

DatapointsToAlarm：3 之 3

遺失資料處理：將遺失資料視為違反。

統計資料：總和

下圖顯示使用案例 A 的流程：

範例使用案例 B：Amazon API Gateway

您可以建立下列 CloudWatch 警示，以指出潛在的工作負載影響。若要這樣做，您可以建立複合指標，在 API Gateway 中出現高延遲或高平均 4XX 錯誤數時發出警示。如需可用的指標，請參閱 Amazon API Gateway 維度和指標

指標：`compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))`

NameSpace：AWS/API Gateway

ComparisonOperator(Threshold)：大於 (x 或 y 客戶的閾值)

Period：60 秒

DatapointsToAlarm：1 之 1

遺失資料處理：將遺失資料視為未違反。

統計資料：

下圖顯示使用案例 B 的流程：

範例使用案例 C：Amazon Route 53

您可以透過建立 Route 53 運作狀態檢查，以使用 CloudWatch 收集原始資料並將其處理成為可讀取、近乎即時的指標，藉此監控資源。您可以建立下列 CloudWatch 警示，以指出潛在的工作負載影響。您可以使用 CloudWatch 指標來建立警示，並在違反建立的閾值時觸發警示。如需可用的 CloudWatch 指標，請參閱 Route 53 運作狀態檢查的 CloudWatch 指標

指標：R53-HC-Success

NameSpace：AWS/Route 53

Threshold HealthCheckStatus：3 分鐘內 3 個資料點的 HealthCheckStatus < x (x 為客戶的閾值)

Period：1 分鐘

DatapointsToAlarm：3 之 3

遺失資料處理：將遺失資料視為違反。

統計資料：最小值

下圖顯示使用案例 C 的流程：

範例使用案例 D：使用自訂應用程式監控工作負載

請務必花些時間在此案例中定義適當的運作狀態檢查。如果您只驗證應用程式的連接埠是否開啟，則尚未驗證應用程式是否正常運作。此外，呼叫應用程式的首頁不一定是判斷應用程式是否正常運作的正確方式。例如，如果應用程式同時依賴資料庫和 Amazon Simple Storage Service (Amazon S3)，則運作狀態檢查必須驗證所有元素。其中一種方法是建立監控網頁，例如 /monitor。監控網頁會呼叫資料庫，確認其可以連線並取得資料。監控網頁也會呼叫 Amazon S3。接著您將負載平衡器上的運作狀態檢查指向 /monitor 頁面。

下圖顯示使用案例 D 的流程：

將警示擷取至 AWS 事件偵測與回應

AWS 事件偵測與回應支援透過 Amazon EventBridge 擷取警示。本節說明如何將 AWS 事件偵測與回應與不同的應用程式效能監控 (APM) 工具整合，包括 Amazon CloudWatch、與 Amazon EventBridge 直接整合的 APM (例如 Datadog 和 New Relic)，以及未與 Amazon EventBridge 直接整合的 APM。如需與 Amazon EventBridge 直接整合的完整 APM 清單，請參閱 Amazon EventBridge 整合。

若要進一步了解如何使用事件偵測與回應命令列介面 (CLI) 來協助自動執行這些步驟，請參閱 AWS 事件偵測與回應 CLI。

主題

- 佈建存取以將警示擷取至事件偵測與回應

- 將事件偵測與回應與 Amazon CloudWatch 整合
- 從與 Amazon EventBridge 直接整合的 APM 擷取警示
- 範例：整合來自 Datadog 和 Splunk 的通知
- 使用 Webhook 從未與 Amazon EventBridge 直接整合的 APM 擷取警示。

佈建存取以將警示擷取至事件偵測與回應

若要允許 AWS 事件偵測與回應從您的帳戶擷取警示，請安裝 `AWSServiceRoleForHealth_EventProcessor` 服務連結角色 (SLR)。AWS 會擔任 SLR 來建立 Amazon EventBridge 受管規則。受管規則會將您帳戶發出的通知傳送至 AWS 事件偵測與回應。如需此 SLR 的相關資訊，包括相關聯的 AWS 受管政策，請參閱《AWS Health 使用者指南》中的使用服務連結角色。

您可以依照《AWS Identity and Access Management 使用者指南》中的建立服務連結角色的指示，在您的帳戶中安裝此服務連結角色。或者，您可以使用下列 AWS Command Line Interface (AWS CLI) 命令：

```
aws iam create-service-linked-role --aws-service-name event-
processor.health.amazonaws.com
```

重要輸出

- 在您的帳戶中成功安裝服務連結角色。

相關資訊

如需詳細資訊，請參閱下列主題：

- 使用 AWS Health 的服務連結角色
- 建立服務連結角色 ()
- AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy

將事件偵測與回應與 Amazon CloudWatch 整合

AWS 事件偵測與回應會使用您在佈建存取期間開啟的服務連結角色 (SLR)，在您的 AWS 帳戶中建立名為 `AWSHealthEventProcessor-DO-NOT-DELETE` 的 Amazon EventBridge 受管規則。事

件偵測與回應會使用此規則從您的帳戶擷取 Amazon CloudWatch 警示。您不需執行其他步驟來從 CloudWatch 擷取警示。

從與 Amazon EventBridge 直接整合的 APM 擷取警示

下圖顯示從 Datadog 和 Splunk 等與 Amazon EventBridge 直接整合的應用程式效能監控 (APM) 工具，傳送通知至 AWS 事件偵測與回應的程序。如需與 EventBridge 直接整合的完整 APM 清單，請參閱 Amazon EventBridge 整合。

若要進一步了解如何使用事件偵測與回應命令列介面 (CLI) 來協助自動執行這些步驟，請參閱 AWS 事件偵測與回應 CLI。

使用下列步驟來設定與 AWS 事件偵測與回應的整合。在執行這些步驟之前，請先確認您的帳戶中已安裝 AWS 服務連結角色 (SLR) `AWSServiceRoleForHealth_EventProcessor`。

設定與 AWS 事件偵測與回應的整合

您必須為針對每個 AWS 帳戶和 AWS 區域完成以下步驟。警示必須來自應用程式資源所在的 AWS 帳戶和 AWS 區域。

1. 將每個 APM 設定為 Amazon EventBridge 合作夥伴事件來源 (例如 `aws.partner/my_apm/integrationName`)。如需將 APM 設定為事件來源的指引，請參閱透過 Amazon EventBridge 從 SaaS 合作夥伴接收事件。這會在您的帳戶中建立合作夥伴事件匯流排。
2. 執行以下任意一項：
   - (建議的方法) 建立自訂 EventBridge 事件匯流排。AWS 事件偵測與回應會透過 `AWSServiceRoleForHealth_EventProcessor` SLR 安裝受管規則 (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) 匯流排。規則來源是自訂事件匯流排。規則目的地是 AWS 事件偵測與回應。此規則會比對擷取第三方 APM 事件的模式。
   - (替代方法) 使用預設事件匯流排，而不使用自訂事件匯流排。預設事件匯流排會要求受管規則將 APM 警示傳送至 AWS 事件偵測與回應。
3. 建立 AWS Lambda 函式 (例如 `My_APM-AWSIncidentDetectionResponse-LambdaFunction`) 來轉換合作夥伴事件匯流排事件。轉換後的事件符合受管規則 `AWSHealthEventProcessorEventSource-DO-NOT-DELETE`。
   a. 轉換後的事件包含唯一的 AWS 事件偵測與回應識別碼，並且會將事件的來源和詳細資訊類型設定為所需的值。模式符合受管規則。

b. 將 Lambda 函式的目標設定為步驟 2 中建立的自訂事件匯流排 (建議的方法)，或設定為預設事件匯流排。

4. 建立 EventBridge 規則，並定義比對您要推送至 AWS 事件偵測與回應之事件清單的事件模式。規則的來源是您在步驟 1 中定義的合作夥伴事件匯流排 (例如 aws.partner/my_apm/integrationName)。規則的目標是您在步驟 3 中定義的 Lambda 函式 (例如 `My_APM-AWSIncidentDetectionResponse-LambdaFunction`)。如需定義 EventBridge 規則的指引，請參閱 Amazon EventBridge 規則。

如需如何設定合作夥伴事件匯流排整合以搭配 AWS 事件偵測與回應使用的範例，請參閱 範例：整合來自 Datadog 和 Splunk 的通知。

範例：整合來自 Datadog 和 Splunk 的通知

此範例提供將來自 Datadog 和 Splunk 的通知整合到 AWS 事件偵測與回應的詳細步驟。

主題

步驟 1：在 Amazon EventBridge 中將 APM 設定為事件來源

在您的 AWS 帳戶中，將每個 APM 設定為 Amazon EventBridge 中的事件來源。如需將 APM 設定為事件來源的指示，請參閱 Amazon EventBridge 合作夥伴中工具的事件來源設定指示。

透過將 APM 設定為事件來源，您就可以從 APM 將通知擷取至 AWS 帳戶中的事件匯流排。設定完成後，AWS 事件偵測與回應就可以在事件匯流排收到事件時，啟動事件管理程序。此程序會將 Amazon EventBridge 新增為 APM 中的目的地。

步驟 2：建立自訂事件匯流排

最佳實務是使用自訂事件匯流排。AWS 事件偵測與回應使用自訂事件匯流排來擷取轉換的事件。AWS Lambda 函式會轉換合作夥伴事件匯流排事件，並將其傳送至自訂事件匯流排。AWS 事件偵測與回應會安裝受管規則，以從自訂事件匯流排擷取事件。

您可以使用預設事件匯流排，而不使用自訂事件匯流排。AWS 事件偵測與回應會通知受管規則從預設事件匯流排擷取事件，而非從自訂事件匯流排。

在 AWS 帳戶中建立自訂事件匯流排：

1. 前往 https://console.aws.amazon.com/events 開啟 Amazon EventBridge 主控台
2. 選擇匯流排、事件匯流排。
3. 在自訂事件匯流排下，選擇建立。
4. 在名稱下提供事件匯流排的名稱。建議的格式為 APMName-AWSIncidentDetectionResponse-EventBus。

   例如，如果您使用 Datadog 或 Splunk，請使用下列其中一項：

   - Datadog：Datadog-AWSIncidentDetectionResponse-EventBus
   - Splunk：Splunk-AWSIncidentDetectionResponse-EventBus

步驟 3：建立 AWS Lambda 函式來進行轉換

Lambda 函式會在步驟 1 的合作夥伴事件匯流排與步驟 2 的自訂 (或預設) 事件匯流排之間轉換事件。Lambda 函式轉換符合 AWS 事件偵測與回應受管規則。

在您的 AWS 帳戶中建立 AWS Lambda 函式

1. 開啟 AWS Lambda 主控台的 Functions (函數) 頁面。
2. 選擇建立函數。
3. 選擇從頭開始撰寫索引標籤。
4. 在函式名稱中，使用 `APMName-AWSIncidentDetectionResponse-LambdaFunction` 格式輸入名稱。

   以下是 Datadog 和 Splunk 的範例：

   - Datadog：Datadog-AWSIncidentDetectionResponse-LambdaFunction
   - Splunk：Splunk-AWSIncidentDetectionResponse-LambdaFunction
5. 在執行時期中，輸入 Python 3.10。
6. 其餘欄位保留預設值。選擇建立函數。
7. 在程式碼編輯頁面上，將預設 Lambda 函式內容取代為下列程式碼範例中的函式。

   請注意下列程式碼範例中以 # 開頭的註解。這些註解指出要變更哪些值。

   Datadog 轉換程式碼範本：

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example 'Datadog-AWSIncidentDetectionResponse-EventBus'
EventBusName = "Datadog-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # Replace the dictionary path, event["detail"]["meta"]["monitor"]["name"], with
 the path to your alert name based on your APM payload.
    # This example is for finding the alert name for Datadog.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["meta"]["monitor"]["name"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
     Entries=[
              {
               'Detail': json.dumps(event["detail"], indent=2),
               'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
               'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
               'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
             }
     ]
    )
    print(response['Entries'])
```

Splunk 轉換程式碼範本：

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example Splunk-AWSIncidentDetectionResponse-EventBus
EventBusName = "Splunk-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # replace the dictionary path event["detail"]["ruleName"] with the path to your
 alert name based on your APM payload.
    # This example is for finding the alert name in Splunk.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["ruleName"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
    Entries=[
             {
              'Detail': json.dumps(event["detail"], indent=2),
              'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
              'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
              'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
            }
        ]
    )
    print(response['Entries'])
```

8. 選擇部署。
9. 將 PutEvents 許可新增至您要傳送轉換資料的目標事件匯流排的 Lambda 執行角色：

a. 開啟 AWS Lambda 主控台的 Functions (函數) 頁面。

b. 選取函式，然後在組態索引標籤上選擇許可。

c. 在執行角色下選取角色名稱，以在 AWS Identity and Access Management 主控台中開啟執行角色。

d. 在許可政策下，選取現有的政策名稱以開啟政策。

e. 在此政策中定義的許可下，選擇編輯。

f. 在政策編輯器頁面上，選取新增陳述式：

g. 政策編輯器會新增類似下方新的空白陳述式

h. 將自動產生的新陳述式取代為下列內容：

```
{
  "Sid": "AWSIncidentDetectionResponseEventBus0",
  "Effect": "Allow",
  "Action": "events:PutEvents",
  "Resource": "arn:aws:events:{region}:{accountId}:event-bus/{custom-eventbus-
name}"
}
```

i. 如果您在 Lambda 程式碼中使用預設事件匯流排，則資源是您在 步驟 2：建立自訂事件匯流排 中建立的自訂事件匯流排的 ARN，或是預設事件匯流排的 ARN。

10. 檢閱並確認已將所需許可新增至角色。

11. 選擇將此新版本設定為預設值，然後選擇儲存變更。

承載轉換需要什麼？

AWS 事件偵測與回應擷取的事件匯流排事件需要下列 JSON 金鑰:值對。

```
{
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent"
    "detail" : {
        "incident-detection-response-identifier": "Your alarm name from your APM",
    }
}
```

下列範例顯示合作夥伴事件匯流排中轉換前和轉換後的事件。


```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "alert_type": "error",
      "event_type": "query_alert_monitor",
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
          "metadata": {
            "monitor_id": 222222,
            "metric": "aws.applicationelb.un_healthy_host_count"
          }
        },
        "transition": {
          "trans_name": "Triggered",
```

```
          "trans_type": "alert"
        },
        "states": {
          "source_state": "OK",
          "dest_state": "Alert"
        },
        "duration": 0
      },
      "priority": "normal",
      "source_type_name": "Monitor Alert",
      "tags": [
        "aws_account:123456789012",
        "monitor"
      ]
    }
}
```

請注意，在事件轉換之前，`detail-type` 會指出警示來自哪個 APM、來源來自合作夥伴 APM，而且 `incident-detection-response-identifier` 索引鍵不存在。

Lambda 函式會轉換上述事件，並將其放入目標自訂或預設事件匯流排。轉換後的承載現在包含必要的鍵:值對。

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "incident-detection-response-identifier": "UnHealthyHostCount",
      "alert_type": "error",
      "event_type": "query_alert_monitor",
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
```

```
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
          "metadata": {
            "monitor_id": 222222,
            "metric": "aws.applicationelb.un_healthy_host_count"
          }
        },
        "transition": {
          "trans_name": "Triggered",
          "trans_type": "alert"
        },
        "states": {
          "source_state": "OK",
          "dest_state": "Alert"
        },
        "duration": 0
      },
      "priority": "normal",
      "source_type_name": "Monitor Alert",
      "tags": [
        "aws_account:123456789012",
        "monitor"
      ]
    }
}
```


請注意，detail-type 現在是 ams.monitoring/generic-apm，來源現在是 GenericAPMEvent，而詳細資訊下有新的鍵:值對：incident-detection-response-identifier。

在上述範例中，`incident-detection-response-identifier` 值採用路徑 `$.detail.meta.monitor.name` 下的警示名稱。APM 彼此之間的 APM 警示名稱路徑不同。您必須修改 Lambda 函式，以便從正確的合作夥伴事件 JSON 路徑取得警示名稱，並將用其作為 `incident-detection-response-identifier` 值。

在 `incident-detection-response-identifier` 上設定的每個唯一名稱都會在上線期間提供給 AWS 事件偵測與回應團隊。若事件的 `incident-detection-response-identifier` 名稱不明，則不會處理。

步驟 4：建立自訂 Amazon EventBridge 規則

在步驟 1 中建立的合作夥伴事件匯流排需要您建立的 EventBridge 規則。此規則會將所需的事件從合作夥伴事件匯流排傳送至步驟 3 中建立的 Lambda 函式。

如需定義 EventBridge 規則的指引，請參閱 Amazon EventBridge 規則。

1. 前往 https://console.aws.amazon.com/events 開啟 Amazon EventBridge 主控台
2. 選擇規則，然後選取與您的 APM 相關聯的合作夥伴事件匯流排。以下是合作夥伴事件匯流排的範例：
   - Datadog：aws.partner/datadog.com/eventbus-name
   - Splunk：aws.partner/signalfx.com/RandomString
3. 選擇建立規則，以建立新的 EventBridge 規則。
4. 針對規則名稱，以下列格式 `APMName-AWS Incident Detection and Response-EventBridgeRule` 輸入名稱，然後選擇下一步。範例名稱如下：
   - Datadog：Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk：Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. 針對事件來源，選取 AWS 事件或 EventBridge 合作夥伴事件。
6. 範例事件和建立方法保留預設值。
7. 針對事件模式，選擇如下：
   a. 事件來源：EventBridge 合作夥伴。
   b. 合作夥伴：選取您的 APM 合作夥伴。
   c. 事件類型：所有事件。

   以下是範例事件模式：

範例 Datadog 事件模式

範例 Splunk 事件模式

8. 針對目標，選擇如下：
   a. 目標類型：AWS 服務
   b. 選取目標：選擇 Lambda 函式。
   c. 函式：您在步驟 2 中建立的 Lambda 函式名稱。
9. 選擇下一步、儲存規則。

使用 Webhook 從未與 Amazon EventBridge 直接整合的 APM 擷取警示。

AWS 事件偵測與回應支援使用 Webhook 從未與 Amazon EventBridge 直接整合的第三方 APM 擷取警示。若要進一步了解如何使用事件偵測與回應命令列介面 (CLI) 來協助自動執行這些步驟，請參閱 AWS 事件偵測與回應 CLI。

如需與 Amazon EventBridge 直接整合的 APM 清單，請參閱 Amazon EventBridge 整合。

使用下列步驟來設定與 AWS 事件偵測與回應的整合。在執行這些步驟之前，請確認您的帳戶中已安裝 AWS 受管規則 AWSHealthEventProcessorEventSource-DO-NOT-DELETE

使用 Webhook 擷取事件

1. 定義 Amazon API Gateway 以接受來自 APM 的承載。
2. 定義 AWS Lambda 函式以使用身分驗證權杖進行授權，如上圖所示。
3. 定義第二個 Lambda 函式來轉換 AWS 事件偵測與回應識別碼，並將其附加至您的承載。您也可以使用此函式來篩選出您要傳送至 AWS 事件偵測與回應的事件。
4. 設定您的 APM，以將通知傳送至從 API Gateway 產生的 URL。

AWS 事件偵測與回應 CLI

AWS 事件偵測與回應客戶命令列介面 (CLI) 是一種命令列介面工具，可簡化您在 AWS 事件偵測與回應上線的方式。

事件偵測與回應 CLI 會在 AWS CloudShell 中執行，以收集上線資訊、透過資源群組標記 API 收集 AWS 資源資料，以及管理支援案例。CLI 可以建立新的 Amazon CloudWatch 警示或擷取現有警示，也可以透過 AWS CloudFormation 部署和測試基礎結構，以允許第三方工具將警示傳送至事件偵測與回應。您可以在互動式模式下執行 CLI，以引導您完成上線步驟，或在離線模式下執行，以處理大量或 DevOps 使用案例。

如需如何使用 CLI 的詳細資訊，包括安裝、先決條件和完整範例，請參閱 AWS 事件偵測與回應 CLI。

在事件偵測與回應中管理工作負載

有效事件管理的重點在於，制定正確的流程和程序，以上線、測試和維護受監控的工作負載。本節涵蓋基本步驟，包括開發完整的執行手冊和回應計畫，以引導您的團隊完成事件、上線前徹底測試和驗證新工作負載、請求變更以更新工作負載監控，以及在需要時正確將工作負載離線的程序。

主題

開發執行手冊和回應計畫，以在事件偵測與回應中回應事件

事件偵測與回應使用從上線問卷中取得的資訊來開發執行手冊和回應計畫，以管理影響工作負載的事件。執行手冊中記載事件管理者在回應事件時所採取的步驟。回應計畫會對應到至少一個工作負載。事件管理團隊會根據您在工作負載探索期間提供的資訊建立這些範本。回應計畫是用來觸發事件的 AWS Systems Manager (SSM) 文件範本。若要進一步了解 SSM 文件，請參閱 AWS Systems Manager 文件。若要進一步了解事件管理者，請參閱什麼是 AWS Systems Manager Incident Manager？

重要輸出：

- 完成 AWS 事件偵測與回應上的工作負載定義。
- 完成 AWS 事件偵測與回應上的警示、執行手冊和回應計畫定義。

您也可以下載 AWS 事件偵測與回應執行手冊範例：aws-idr-runbook-example.zip。

範例執行手冊：

```
Runbook template for AWS Incident Detection and Response
# Description
This document is intended for [CustomerName] [WorkloadName].

[Insert short description of what the workload is intended for].

## Step: Priority
```

```
**Priority actions**
1. When a case is created with Incident Detection and Response, lock the case to
 yourself, verify the Customer Stakeholders in the Case from *Engagement Plans -
 Initial Engagement*.
2. Send the first correspondence on the support case to the customer as below. If
 there is no support case or if it is not possible to use the support case then backup
 communication details are listed in the steps that follow.

```
Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has
 triggered for your workload <<application name>>. I am currently investigating and
 will update you in a few minutes after I have finished initial investigation.

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
```

Compliance and regulatory requirements for the workload
<<e.g. The workload deals with patient health records which must be kept secured and
 confidential. Information not to be shared with any third parties.>>

Actions required from Incident Detection and Response in complying
<<e.g Incident Management Engineers must not shared data with third parties.>>

Step: Information
Review of common information

* This section provides a space for defining common information which may be needed
 through the life of the incident.
* The target user of this information is the Incident Management Engineer and
 Operations Engineer.
* The following steps may reference this information to complete an action (for
 example, execute the "Initial Engagement" plan).

Engagement plans

Describe the engagement plans applicable to this runbook. This section contains
 only contact details. Engagement plans will be referenced in the step by step
 Communication Plans.

* **Initial engagement**
```

```
AWS Incident Detection and Response Team will add customer stakeholder addresses below
 to the Support Case. AWS Stakeholders are for additional stakeholders that may need to
 be made aware of any issues.
When updating customer stakeholders details in this plan also update the Backup Mailto
 links.
  * ***Customer Stakeholders***:  customeremail1; customeremail2; etc
  * ***AWS Stakeholders***: aws-idr-oncall@amazon.com; tam-team-email; etc.
  * ***One Time Only Contacts***: [These are email contacts that are included on only
 the first communication. Remove these contacts after the first communication has gone
 out. These could be customer paging email addresses such as pager-duty that must not
 be paged for every correspondence]
  * ***Backup Mailto Impact Template***: <*Insert Impact Template Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.
  * ***Backup Mailto No Impact Template***: <*Insert No Impact Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.



* **Engagement Escalation**

AWS Incident Detection and Response will reach out to the following contacts when the
 contacts from the **Initial engagement** plan do not respond to incidents.
For each Escalation Contact indicate if they must be added to the support case, phoned
 or both.
  * ***First Escalation Contact***: [escalationEmailAddress#1] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * ***Second Escalation Contact***: [escalationEmailAddress#2] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * Etc;
---
**Communication plans**

Describe how Incident Management Engineer communicates with designated stakeholders
 outside the incident call and communication channels.

* **Impact Communication plan**
This plan is initiated when Incident Detection and Response have determined from step
 **Triage** that an alert indicates potential impact to a customer.
Incident Detection and Response will request the customer to join the predetermined
 bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated
 in **Engagement plans - Incident call setup**.
All backup email templates for use when cases can't be used are in **Engagement plans -
 Initial engagement**.
```

```
 * 1 - Before sending the impact notification, verify then remove and/or add customer
contacts from the Support Case CC based on the contacts listed in the **Initial
engagement** Engagement plan.
 * 2 - Send the engagement notification to the customer based the following Template:

   (choose one and remove the rest)
   ***Impact Template - Chime Bridge***
   ```
   The following alarm has engaged AWS Incident Detection and Response to an Incident
bridge:
       Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
       Alarm State Change Reason - <insert state change reason>
       Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
   Please join the Chime Bridge below so we can start the steps outlined in your
Runbook:
       <insert Chime Meeting ID>
       <insert Link to Chime Bridge>
       International dial-in numbers: https://chime.aws/dialinnumbers/
   ```


   ***Impact Template - Customer Provided Bridge***
   ```
   The following alarm has engaged AWS Incident Detection and Response:
       Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
       Alarm State Change Reason - <insert state change reason>
       Alarm Start Time - <Example: 1 January 2023 3:30 PM UTC>
   Please respond with your internal bridge details so we can join and start the steps
outlined in your Runbook.
   ```
   ***Impact Template - Customer Static Bridge***
   ```
   The following alarm has engaged AWS Incident Detection and Response to an Incident
bridge:
       Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
       Alarm State Change Reason - <insert state change reason>
       Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
   Please join the Bridge below so we can start the steps outlined in your Runbook:
       Conference Number: <insert conference number>
       Conference URL : <insert bridgeURL>
   ```
 * 3 - Set the Case to Pending Customer Action
 * 4 - Follow **Engagement Escalation** plan as mentioned above.
 * 5 - If the customer does not respond within 30 minutes, disengage and continue to
monitor until the alarm recovers.
```

```
* **No Impact Communication plan**
This plan is initiated when an alarm recovers before Incident Detection and Response
 have completed initial **Triage**.
  * 1 - Before sending the no impact notification, verify then remove and/or add
 customer contacts from the Support Case CC based on the contacts listed in the
 **Engagement plans - Initial engagement** Engagement plan.
  * 2 - Send a no engagement notification to the customer based on the below template:

  ***No Impact Template***
  ```
  AWS Incident Detection and Response received an alarm that has recovered for your
 workload.
       Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
       Alarm State Change Reason - <insert state change reason>
       Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
       Alarm End Time - <Example: 1 January 2023, 3:35 PM UTC>
  This may indicate a brief customer impact that is currently not ongoing.
  If there is an ongoing impact to your workload, please let us know and we will engage
 to assist.
  ```
  * 3 - Put the case in to Pending Customer Action.
  * 4 - If the customer does not respond within 30 minutes Resolve the case.

* **Updates**
If AWS Incident Detection and Response is expected to provide regular updates to
 customer stakeholders, list those stakeholders here. Updates must be sent via the same
 support case.
Remove this section if not needed.
  * Update Cadence: Every XX minutes
  * External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc
  * Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

---
**Application architecture overview**

This section provides an overview of the application/workload architecture for Incident
 Management Engineer and Operations Engineer awareness.

* **AWS Accounts and Regions with key services** - list of AWS accounts with regions
 supporting this application. Assists Engineers in assessing underlying infrastructure
 supporting the application.
    * 123456789012
      * US-EAST-1 - brief desc as appropriate
```

```
        * EC2 - brief desc as appropriate
        * DynamoDB - brief desc as appropriate
        * etc.
      * US-WEST-1 - brief desc as appropriate
      * etc.
    * another-account-etc.

* **Resource identification** - describe how engineers determine resource association
 with application
    * Resource groups: etc.
    * Tag key/value: AppId=123456

* **CloudWatch Dashboards** - list dashboards relevant to key metrics and services
  * 123456789012
    * us-east-1
      * some-dashboard-name
      * etc.
  * some-other-dashboard-name-in-current-acct

## Step: Triage
**Evaluate incident and impact**
This section provides instructions for triaging of the incident to determine correct
 impact, description, and overall correct runbook being executed.

* **Evaluation of initial incident information**
  * 1 - Review Incident Alarm, noting time of first detected impact as well as the
 alarm start time.
  * 2 - Identify which service(s) in the customer application is seeing impact.
  * 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions
 with key services**.
  * 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

---
* **Impact**
Impact is determined when either the customer's metrics do not recover, appear to be
 trending worse or if there is indication of AWS Service Impact.
  * 1 - Start **Communication plans - Impact Communication plan**
  * 2 - Start **Engagement plans - Engagement Escalation** if no response is received
 from the **Initial Engagement** contacts.
  * 3 - Start **Communication plans - Updates** if specified in **Communication plans**

* **No Impact**
```

```
No Impact is determined when the customer's alarm recovers before Triage is complete
 and there are no indications of AWS service impact or sustained impact on the
 customer's CloudWatch Dashboards.
  * 1 - Start **Communication plans - No Impact Communication plan**

## Step: Investigate
**Investigation**

  This section describes performing investigation of known and unknown symptoms.

**Known issue**
  * *List all known issues with the application and their standard actions here*

**Unknown issues**
  * Investigate with the customer and AWS Premium Support.
  * Escalate internally as required.

## Step: Mitigation
**Collaborate**
* Communicate any changes or important information from the **Investigate** step to the
 members of the incident call.

**Implement mitigation**
* ***List customer failover plans / Disaster Recovery plans / etc here for implementing
 mitigation.

## Step: Recovery
**Monitor customer impact**
* Review metrics to confirm recovery.
* Ensure recovery is across all Availability Zones / Regions / Services
* Get confirmation from the customer that impact is over and the application has
 recovered.

**Identify action items**
* Record key decisions and actions taken, including temporary mitigation that might
 have been implemented.
* Ensure outstanding action items have assigned owners.
* Close out any Communication plans that were opened during the incident with a final
 confirmation of recovery notification.
```

在事件偵測與回應中測試上線的工作負載

> **Note**
>
> 您用於警示測試的 AWS Identity and Access Management 使用者或角色必須具有 `cloudwatch:SetAlarmState` 許可。

上線程序的最後一個步驟是為您的新工作負載執行 Gameday。警示擷取完成後，AWS 事件偵測與回應會確認您選擇開始 Gameday 的日期和時間。

您的 Gameday 有兩個主要目的：

- 功能驗證：確認 AWS 事件偵測與回應可以正確接收您的警示事件。此外，功能驗證會確認您的警示事件觸發適當的執行手冊和任何其他必要的動作，例如，自動建立案例 (若您在警示擷取期間選取)。
- 模擬：Gameday 會完整模擬真實事件期間可能發生的狀況。AWS 事件偵測與回應會依照您制定的執行手冊步驟，讓您深入了解實際事件可能發生的情形。Gameday 是您提出問題或精進指示，以改善參與度的機會。

在警示測試期間，AWS 事件偵測與回應會與您一起修復發現的任何問題。

CloudWatch 警示

AWS 事件偵測與回應透過監控警示的狀態變更來測試 Amazon CloudWatch 警示。若要這樣做，請使用 AWS Command Line Interface 手動將警示變更為警示狀態。您也可以從 AWS CloudShell 存取 AWS CLI。AWS 事件偵測與回應提供 AWS CLI 命令清單，可讓您在測試期間使用。

設定警示狀態的範例 AWS CLI 命令：

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-
reason "Testing AWS Incident Detection and Response" --region us-east-1
```

若要進一步了解手動變更 CloudWatch 警示的狀態，請參閱 SetAlarmState。

若要進一步了解 CloudWatch API 操作所需的許可，請參閱 Amazon CloudWatch 許可參考。

第三方 APM 警示

使用 Datadog、Splunk、New Relic 或 Dynatrace 這類第三方應用程式效能監控 (APM) 工具的工作負載，需要不同的指示來模擬警示。在 Gameday 開始時，AWS 事件偵測與回應會要求您暫時變更警示閾值或比較運算子，以強制警示進入 ALARM 狀態。此狀態會觸發 AWS 事件偵測與回應的承載。

重要輸出

重要輸出：

- 警示擷取成功，且您的警示組態正確。
- AWS 事件偵測與回應成功建立和接收警示。
- 此時會建立支援案例讓您參與，您指定的聯絡人也會收到通知。
- AWS 事件偵測與回應可以透過您指定的會議方式與您互動。
- Gameday 過程中產生的所有警示和支援案例都會獲得解決。
- 此時會傳送 Go-Live 電子郵件，確認您的工作負載現在受到 AWS 事件偵測與回應的監控。

在事件偵測與回應中請求變更已上線的工作負載

若要請求變更已上線的工作負載，請完成下列步驟，以使用 AWS 事件偵測與回應建立支援案例。

1. 前往 AWS 支援 中心，然後選取建立案例，如下列範例所示：

2. 選擇技術。
3. 針對服務，選擇事件偵測與回應。
4. 針對類別，選擇工作負載變更請求。
5. 針對嚴重性，選擇一般指引。
6. 輸入此變更的主旨。例如：

   AWS 事件偵測與回應 - *workload_name*
7. 輸入此變更的說明。例如，輸入「這是關於變更 AWS 事件偵測與回應中已上線的現有工作負載的請求」。請求中務必包含下列資訊：

   - 工作負載名稱：您的工作負載名稱。
   - 帳戶 ID：ID1、ID2、ID3 (以此類推)。
   - 變更詳細資訊：輸入所請求變更的詳細資訊。

8. 在其他聯絡人 - 選用區段中，輸入您要接收有關此變更之通信的任何電子郵件 ID。

   以下是其他聯絡人 - 選用區段的範例。

> **Important**
>
> 如果未在其他聯絡人 - 選用區段中新增電子郵件 ID，可能會使變更程序延遲。

9. 選擇提交。

   提交變更請求後，您可以新增您組織的其他電子郵件。若要新增電子郵件，請在案例詳細資訊中選擇回覆，如下列範例所示：

   然後在其他聯絡人 - 選用區段中，新增電子郵件 ID。

   以下是回覆頁面的範例，其中顯示您可以輸入其他電子郵件的位置。

隱藏警示使其無法和事件偵測與回應互動

藉由暫時或依排程隱藏警示的方式，指定哪些已上線的工作負載警示要與 AWS 事件偵測與回應監控互動。例如，您可能會在預定的維護期間暫時隱藏工作負載警示，防止警示與事件偵測與回應互動。或者，如果您有每日重新啟動活動，則可能會依排程隱藏警示。您可以在警示來源 (例如 Amazon CloudWatch) 隱藏警示，也可以提交工作負載變更請求。

主題

在警示來源隱藏警示

藉由在警示來源隱藏警示的方式，指定哪些警示與事件偵測與回應互動，以及何時進行互動。

主題

- 使用指標數學函數來隱藏 CloudWatch 警示
- 移除指標數學函數以取消隱藏 CloudWatch 警示
- 指標數學函數範例和相關聯的使用案例
- 隱藏來自第三方 APM 的警示

使用指標數學函數來隱藏 CloudWatch 警示

若要抑制 Amazon CloudWatch 警示的事件偵測與回應監控，請使用指標數學函數來停止 CloudWatch 警示在指定時段進入 ALARM 狀態。

> **Note**
>
> 停用 CloudWatch 警示的警示動作並不會抑制事件偵測與回應監控您的警示。警示狀態變更會透過 Amazon EventBridge 擷取，而不是透過 CloudWatch 警示動作擷取。

若要使用指標數學函數來隱藏 CloudWatch 警示，請完成下列步驟：

1. 登入 AWS 管理主控台，並在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇警示，然後尋找您要新增指標數學函數的警示。
3. 依序選擇動作和編輯以變更警示。
4. 選擇編輯指標以修改警示的指標。
5. 選擇新增數學、以空白運算式開始。
6. 輸入您的數學運算式，然後選擇套用。
7. 取消選取警示監控的現有指標。
8. 選取您剛才建立的運算式，然後選擇選取指標。
9. 選擇跳至預覽並建立。
10. 檢閱您的變更，以確保依預期套用您的指標數學函數，然後選擇更新警示。

如需使用指標數學函數隱藏 CloudWatch 警示的逐步範例，請參閱 教學課程：使用指標數學函數來隱藏警示。

如需語法和可用函數的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的指標數學語法和函數。

移除指標數學函數以取消隱藏 CloudWatch 警示

透過移除指標數學函數來取消隱藏 CloudWatch 警示。若要移除警示的指標數學函數，請完成下列步驟：

1. 登入 AWS 管理主控台，並在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇警示，然後尋找您要移除其指標數學運算式的警示。
3. 在指標數學區段中，選擇編輯。
4. 若要移除警示的指標，請選擇指標上的編輯，然後選擇指標數學運算式旁的 x 按鈕。
5. 選取原始指標，然後選擇選取指標。
6. 選擇跳至預覽並建立。
7. 檢閱您的變更，以確保依預期套用您的指標數學函數，然後選擇更新警示。

指標數學函數範例和相關聯的使用案例

下表包含指標數學函數範例，以及相關聯的使用案例和每個指標元件的說明。

指標數學函數	使用案例	說明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	在每星期二 1:00 到 3:00 AM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 0。	• DAY(m1) == 2：確認是星期二 (星期一 = 1、星期日 = 7)。 • HOUR(m1) >= 1 && HOUR(m1) > 3：指定時間範圍從 1 AM 到 3 AM UTC。 • IF(condition, value_if_true, value_if_false)：如果條件為 true，則將指標值取代為 0。否則傳回原始值 (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	在每天 11:00 PM 到 4:00 AM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 0。	• HOUR(m1) >= 23：擷取時間從 23:00 UTC 開始。 • HOUR(m1) < 4：擷取時間至 (但不包括) 04:00 UTC 結束。

指標數學函數	使用案例	說明
		• ||：邏輯 OR 確保條件在兩個範圍之間套用，也就是夜間到凌晨時段。 • IF(condition, value_if_true, value_if_false)：在指定的時間範圍內傳回 0。在該範圍之外保留原始指標值 m1。
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	在每天 11:00 AM 到 1:00 PM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 0。	• HOUR(m1) >= 11 && HOUR(m1) < 13：擷取時間範圍從 11:00 到 13:00 UTC。 • IF(condition, value_if_true, value_if_false)：如果條件為 true (例如時間介於 11:00 和 13:00 UTC 之間)，則傳回 0，如果條件為 false，則保留原始指標值 (m1)。
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	在每星期二 1:00 到 3:00 AM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 99。	• DAY(m1) == 2：確認是星期二 (星期一 = 1、星期日 = 7)。 • HOUR(m1) >= 1 && HOUR(m1) < 3：指定時間範圍從 1 AM 到 3 AM UTC。 • IF(condition, value_if_true, value_if_false)：如果條件為 true，則將指標值取代為 99。否則傳回原始值 (m1)。

指標數學函數	使用案例	說明
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	在每天 11:00 PM 到 4:00 AM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 100。	• HOUR(m1) >= 23：擷取時間從 23:00 UTC 開始。 • HOUR(m1) < 4：擷取時間至 (但不包括) 04:00 UTC 結束。 • ||：邏輯 OR 確保條件在兩個範圍之間套用，也就是夜間到凌晨時段。 • IF(condition, value_if_true, value_if_false)：在指定的時間範圍內傳回 100。在該範圍之外保留原始指標值 m1。
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	在每天 11:00 AM 到 1:00 PM UTC 之間隱藏警示，方法是在此時段將實際資料點取代為 99。	• HOUR(m1) >= 11 && HOUR(m1) < 13：擷取時間範圍從 11:00 到 13:00 UTC。 • IF(condition, value_if_true, value_if_false)：如果條件為 true (例如時間介於 11:00 和 13:00 UTC 之間)，則傳回 99。如果條件為 false，則保留原始指標值 (m1)。

隱藏來自第三方 APM 的警示

請參閱第三方 APM 廠商的文件，以取得如何隱藏警示的指示。第三方 APM 廠商的範例包括 New Relic、Splunk、Dynatrace、Datadog 和 SumoLogic。

提交工作負載變更請求以隱藏警示

如果您無法依上一節所述在來源隱藏警示，則可提交工作負載變更請求來指示事件偵測與回應，以手動隱藏部分或全部工作負載警示的監控。

如需如何建立工作負載變更請求的詳細指示，請參閱在事件偵測與回應中請求變更已上線的工作負載。提出工作負載變更請求以請求隱藏警示時，務必提供下列必要資訊

- 工作負載名稱：您的工作負載名稱。
- 帳戶 ID：ID1、ID2、ID3 (以此類推)。
- 變更詳細資訊：警示隱藏
- 隱藏開始時間：日期、時間和時區。
- 隱藏結束時間：日期、時間和時區。
- 要隱藏的警示：要隱藏的 CloudWatch 警示 ARN 或第三方 APM 事件識別碼清單。

建立警示隱藏工作負載變更請求之後，您會收到來自事件偵測與回應的下列通知：

- 工作負載變更請求確認。
- 警示隱藏時的通知。
- 重新啟用警示以進行監控時的通知。

教學課程：使用指標數學函數來隱藏警示

下列教學課程會逐步解說如何使用指標數學來隱藏 CloudWatch 警示。

範例藍本

在即將到來的星期二 1:00 到 3:00 AM UTC 之間要進行一場規劃的活動。您想要建立 CloudWatch 指標數學函數，將這段時間的實際資料點取代為 0 (低於設定閾值的資料點)。

1. 評估導致警示觸發的條件。下方螢幕擷取畫面提供警示條件的範例：

   上方螢幕擷取畫面中顯示的警示會監控 Application Load Balancer 目標群組的 `UnHealthyHostCount` 指標。當 `UnHealthyHostCount` 指標大於或等於 5 之 5 個資料點的 3 個時，此警示就會進入 `ALARM` 狀態。警示會將遺失的資料視為錯誤 (違反設定的閾值)。

2. 建立指標數學函數。

   在此範例中，在即將到來的星期二 1:00 到 3:00 AM UTC 之間要進行一場規劃的活動。因此，建立 CloudWatch 指標數學函數，將這段時間的實際資料點取代為 0 (低於設定閾值的資料點)。

請注意，您必須設定的取代資料點會因警示組態而有所不同。例如，如果您的警示監控 HTTP 成功率，且閾值小於 98，則在規劃的活動期間將實際資料點取代為高於設定的閾值 100。以下是此案例的範例指標數學函數。

```
IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
```

上述指標數學函數包含下列元素：

- DAY(m1) == 2：確認是星期二 (星期一 = 1、星期日 = 7)。
- HOUR(m1) >= 1 && HOUR(m1) < 3：指定時間範圍從 1 AM 到 3 AM UTC。
- IF(condition, value_if_true, value_if_false)：如果條件為 true，則函數會將指標值取代為 0。否則會傳回原始值 (m1)。

如需有關語法和可用函數的其他資訊，請參閱《Amazon CloudWatch 使用者指南》中的指標數學語法和函數

3. 登入 AWS 管理主控台，並在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
4. 選擇警示，然後尋找您要新增指標數學函數的警示。
5. 在指標數學區段中，選擇編輯。
6. 選擇新增數學、以空白運算式開始。
7. 輸入您的數學運算式，然後選擇套用。

   警示監控的現有指標會自動變成 m1，而您的數學運算式為 e1，如下列範例所示：

8. (選用) 編輯指標數學運算式的標籤，以協助其他人了解其功能及其建立原因，如下列範例所示：

9. 取消選取 m1、選取 e1，然後選擇選取指標。這樣就會將警示設定為監控數學運算式，而非直接監控基礎指標。
10. 選擇跳至預覽並建立。
11. 驗證警示的設定如預期，然後選擇更新警示以儲存變更。

在上述範例中，若未套用指標數學函數，則可能會在規劃的活動期間回報實際 UnHealthyHostCount 指標。這會導致 CloudWatch 警示進入 ALARM 狀態並且和事件偵測與回應互動，如下列範例所示：

有了指標數學函數後，就會在活動期間將實際資料點取代為 0，且警示會保持 OK 狀態，藉此抑制事件偵測與回應參與。

教學課程：移除指標數學函數以取消隱藏警示

如果您針對一次性活動隱藏 CloudWatch 警示，可在活動完成後移除警示的指標數學函數，以繼續定期監控警示。若要定期隱藏警示，例如，您已排程每週例行修補作業，使得執行個體每週在相同日期和時間重新啟動，則保留指標數學函數。

下列教學課程會逐步解說如何移除指標數學函數來取消隱藏 CloudWatch 警示

1. 登入 AWS 管理主控台，並在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇警示，然後尋找您要新增指標數學函數的警示。
3. 在指標數學區段中，選擇編輯。
4. 若要取消隱藏警示，請選取指標數學運算式旁的 x 按鈕。

5. 選取指標以繼續監控實際指標。然後選擇選取指標。

6. 選擇跳至預覽並建立。
7. 驗證警示的設定如預期，然後選擇更新警示以儲存變更。

讓工作負載從事件偵測與回應離線

若要讓工作負載從 AWS 事件偵測與回應離線，請為每個工作負載建立新的支援案例。當您建立支援案例時，請記住下列事項：

- 若要讓單一 AWS 帳戶中的工作負載離線，請從工作負載的帳戶或您的付款人帳戶建立支援案例。
- 若要讓跨多個 AWS 帳戶的工作負載離線，請從您的付款人帳戶建立支援案例。在支援案例的內文中，列出所有要離線的帳戶 ID。

> **Important**
>
> 如果您從錯誤的帳戶建立支援案例讓工作負載離線，則在工作負載離線之前，您可能會遇到延遲和請求您提供其他資訊的情形。

請求將工作負載離線

1. 前往 AWS 支援 中心，然後選取建立案例。
2. 選擇技術。
3. 針對服務，選擇事件偵測與回應。
4. 針對類別，選擇工作負載離線。
5. 針對嚴重性，選擇一般指引。
6. 輸入此變更的主旨。例如：

   [離線] AWS 事件偵測與回應 - *workload_name*
7. 輸入此變更的說明。例如，輸入「這是關於將 AWS 事件偵測與回應中已上線的現有工作負載離線的請求」。請求中務必包含下列資訊：

   - 工作負載名稱：您的工作負載名稱。
   - 帳戶 ID：ID1、ID2、ID3 (以此類推)。
   - 離線原因：提供讓工作負載離線的原因。
8. 在其他聯絡人 - 選用區段中，輸入您要接收有關此離線請求之通信的任何電子郵件 ID。
9. 選擇提交。

AWS 事件偵測與回應監控與可觀測性

AWS 事件偵測與回應為您提供專家指引，協助您從應用程式層到基礎結構，定義工作負載之間的可觀測性。監控會通知您發生錯誤。可觀測性使用資料集合來通知您發生什麼錯誤，以及發生的原因。

事件偵測與回應系統利用 Amazon CloudWatch 和 Amazon EventBridge 等原生 AWS 服務來偵測可能影響工作負載的事件，以監控 AWS 工作負載是否有故障和效能降級的情形。監控會通知您即將發生、持續發生、下降或潛在故障或效能降級的情形。當您在事件偵測與回應中將帳戶上線時，您會選取要由事件偵測與回應監控系統監控帳戶中的哪些警示，並將這些警示與應用程式和事件管理期間使用的執行手冊建立關聯。

事件偵測與回應使用 Amazon CloudWatch 和其他 AWS 服務 來建置您的可觀測性解決方案。AWS 事件偵測與回應透過兩種方式協助您實現可觀測性：

- 業務成果指標：AWS 事件偵測與回應的可觀測性是從定義關鍵指標來監控工作負載或最終使用者體驗的成果開始。AWS 專家會與您合作，以了解工作負載的目標、重要輸出或可能影響使用者體驗的因素，並定義擷取這些關鍵指標中任何降級情形的指標和警示。例如，行動通話應用程式的關鍵業務指標是通話設定成功率 (監控使用者嘗試通話的成功率)，而網站的關鍵指標是頁面速度。事件參與是根據業務成果指標觸發。
- 基礎結構層級指標：在此階段，我們會識別支援您應用程式的基礎 AWS 服務 和基礎結構，並定義指標和警示來追蹤這些基礎結構服務的效能。這些指標可能包括 Application Load Balancer 執行個體的 `ApplicationLoadBalancerErrorCount`。這會在工作負載上線且監控設定完成後開始。

在 AWS 事件偵測與回應上實作可觀測性

由於可觀測性是一個持續的過程，無法在一次實務或一個時段內完成，因此 AWS 事件偵測與回應會分成兩個階段來實作可觀測性：

- 上線階段：上線期間的可觀測性著重於偵測應用程式的業務成果何時受損。為達成此目的，上線階段期間的可觀測性著重於定義應用程式層的關鍵業務成果指標，以通知 AWS 工作負載發生中斷。如此一來，AWS 就可以快速回應這些中斷情形，並協助您復原。若要進一步了解如何使用事件偵測與回應命令列介面 (CLI) 來協助自動執行這些步驟，請參閱 AWS 事件偵測與回應 CLI。
- 上線後階段：AWS 事件偵測與回應根據客戶的成熟度，提供適用於可觀測性的許多主動式服務，包括定義基礎結構層級指標、調校指標，以及設定追蹤和日誌。這些服務的實作可能跨越數個月，並涉及多個團隊。AWS 事件偵測與回應提供設定可觀測性的指引，客戶必須在其工作負載環境中實作必要的變更。如需實際實作可觀測性功能的協助，請向技術客戶經理 (TAM) 提出請求。

使用事件偵測與回應進行事件管理

AWS 事件偵測與回應提供全年無休的主動監控，以及由指定的事件管理者團隊提供的事件管理。下圖概述應用程式警示觸發事件時的標準事件管理程序，包括警示產生、AWS Incident Manager 參與、事件解決和事件後檢討。

1. 警示產生：工作負載上觸發的警示會透過 Amazon EventBridge 推送至 AWS 事件偵測與回應。AWS 事件偵測與回應會自動叫出與您的警示相關聯的執行手冊，並通知事件管理者。如果您的工作負載發生重大事件，而 AWS 事件偵測與回應所監控的警示未偵測到該事件，則您可以建立支援案例來請求事件回應。如需請求事件回應的詳細資訊，請參閱 請求事件回應。
2. AWS Incident Manager 參與：Incident Manager 會回應警示，並讓您參與電話會議，或依照執行手冊中的指示進行。事件管理員會驗證 AWS 服務 的運作狀態，以判斷警示是否與工作負載所使用 AWS 服務 的問題有關，並建議基礎服務的狀態。如有需要，事件管理者會代表您建立案例，並請適當的 AWS 專家提供支援。由於 AWS 事件偵測與回應專門監控您應用程式的 AWS 服務，因此 AWS 事件偵測與回應可能會在 AWS 服務 事件宣告之前就判斷出事件是否與 AWS 服務 問題相關。在此案例中，事件管理者會告知您 AWS 服務 的狀態、觸發 AWS 服務 事件事件管理工作流程，並跟進服務團隊後續解決的狀況。提供的資訊可讓您及早實施復原計畫或解決措施，以緩解 AWS 服務 事件的影響。
3. 解決事件：事件管理者會在必要的 AWS 團隊之間協調事件，並確保您持續與適當的 AWS 專家互動，直到事件獲得緩解或解決為止。
4. 事件後檢討 (若有請求)：在事件之後，AWS 事件偵測與回應可依您請求執行事件後檢討，並產生事件後報告。事件後報告包含問題的說明、影響、參與的團隊，以及採取了哪些解決措施或行動來緩解或解決事件。事件後報告可能包含一些資訊，可用於降低事件再次發生的可能性，或改善未來類似事件發生時的管理。事件後報告不是根本原因分析 (RCA)。除了事件後報告之外，您還可以請求 RCA。下一節將提供事件後報告的範例。

> **Important**
>
> 下列報告範本僅為範例。

```
Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS ## case ID(s): 0000000000
```

Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-impaired-useast1-P95

Problem Statement:
Outlines impact to end users and operational infrastructure impact.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage of their workload that lasted one hour and two minutes and spanning across all Availability Zones where the application is deployed. During impact, end users were unable to connect to the workload's Application Load Balancers (ALBs) which service inbound communications to the application.

Incident Summary:

Summary of the incident in chronological order and steps taken by AWS Incident Managers to direct the incident to a path to mitigation.
At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical incident for the workload. AWS Incident Detection and Response Managers responded to the alarm, checking AWS service health and steps outlined in the workload’s runbook.
At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the Incident Management team sent the engagement email to the customer’s Site Reliability Team (SRE) team, created a troubleshooting bridge, and an ## support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and ## Engineering joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to services the workload depends on. The investigation shifted to the specific resources in the customer account.
At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase in traffic volume was causing a drop in connections. The customer confirmed this ALB was newly provisioned to handle an increase in workload traffic for an on-going promotional event.
At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The Incident Manager worked with the Cloud Support Engineer to raise an escalation a higher support level to quickly scale the ALB per the runbook.
At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The back-off/retry logic yields mild recovery but timeouts are still being seen for some clients.
By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to pre-incident levels. Connection timeouts subside.
At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

```
Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
  Back-off and retries yielded mild recovery. Full mitigation happened after escalation
 to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer to the
 time of impact.
Work with AWS ## and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

主題

為應用程式團隊佈建 AWS Support Center Console 的存取權

AWS 事件偵測與回應會在事件生命週期內透過 支援 案例與您溝通。若要與事件管理者通信，您的團隊必須能夠存取 支援 中心。

如需佈建存取權的詳細資訊，請參閱《支援 使用者指南》中的管理 支援 中心的存取權。

請求事件回應

如果您的工作負載發生重大事件，而 AWS 事件偵測與回應所監控的警示未偵測到該事件，您可以建立支援案例來請求事件回應。您可以使用 AWS Support Center Console、AWS 支援 API 或 AWS Support App in Slack，針對訂閱 AWS 事件偵測與回應的任何工作負載請求事件回應，包括上線過程中的工作負載。

下圖說明 AWS 客戶向事件偵測與回應團隊請求事件協助的完整工作流程，當中詳細說明從初始請求到調查、緩解和解決的步驟。

若要針對正在影響工作負載的事件請求事件回應，請建立 支援 案例。提出支援案例後，AWS 事件偵測與回應會請您與 AWS 專家一起參加電話會議，以便加速復原工作負載。

使用 AWS Support Center Console 請求事件回應

1. 開啟 AWS Support Center Console，然後選擇建立案例。
2. 選擇技術。
3. 針對服務，選擇事件偵測與回應。
4. 針對類別，選擇作用中事件。
5. 針對嚴重性，選擇業務關鍵系統關閉。
6. 輸入此事件的主旨。例如：

   AWS 事件偵測與回應 - 作用中事件 - workload_name
7. 輸入此事件的問題說明。新增下列詳細資訊：
   - 技術資訊：

     工作負載名稱

     受影響的 AWS 資源 ARN
   - 業務資訊：

     說明對業務的影響

     [選用] 客戶橋接詳細資訊
8. 為了協助我們更快與 AWS 專家互動，請提供下列詳細資訊：
   - 受影響的 AWS 服務
   - 其他服務/其他受影響
   - 受影響的 AWS 區域
9. 在其他聯絡人區段中，輸入您要接收有關此事件之通信的任何電子郵件地址。

   下圖顯示主控台畫面，其中反白顯示其他聯絡人欄位。

10選擇提交。

   提交事件回應請求後，您可以新增組織的其他電子郵件地址。若要新增其他地址，請回覆案例，然後在其他聯絡人區段中新增電子郵件地址。

   下圖顯示案例詳細資訊畫面，其中反白顯示回覆按鈕。

下圖顯示案例回覆，其中反白顯示其他聯絡人欄位和提交按鈕。

11AWS 事件偵測與回應會在五分鐘內確認您的案例，並請您與適當的 AWS 專家一起參加電話會議。

使用 AWS 支援 API 請求事件回應

您可以使用 AWS 支援 API，以程式設計方式建立支援案例。如需詳細資訊，請參閱《AWS 支援 使用者指南》中的關於 AWS 支援 API。

使用 AWS Support App in Slack 請求事件回應

若要使用 AWS Support App in Slack 請求事件回應，請完成下列步驟：

1. 開啟您在其中設定 Slack 頻道的 AWS Support App in Slack。
2. 輸入以下命令：

```
/awssupport create
```

3. 輸入此事件的主旨。例如，輸入 AWS 事件偵測與回應 - 作用中事件 - workload_name。
4. 輸入此事件的問題說明。新增下列詳細資訊：

   技術資訊：

   受影響的服務：

   受影響的資源：

   受影響的區域：

   工作負載名稱：

   業務資訊：

   說明對業務的影響：

   [選用] 客戶橋接詳細資訊：
5. 選擇下一步。

6. 針對問題類型，選擇技術支援。
7. 針對服務，選擇事件偵測與回應。
8. 針對類別，選擇作用中事件。
9. 針對嚴重性，選擇業務關鍵系統關閉。
10. 或者，在要通知的其他聯絡人欄位中輸入最多 10 個其他聯絡人，並以逗號分隔。這些其他聯絡人會收到有關此事件的電子郵件通信副本。
11. 選擇檢閱。
12. Slack 頻道中會顯示只有您可看見的新訊息。檢閱案例詳細資訊，然後選擇建立案例。
13. 您的案例 ID 會在 AWS Support App in Slack 發出的新訊息中提供。
14. 事件偵測與回應會在 5 分鐘內確認您的案例，並請您與適當的 AWS 專家一起參加會議橋。
15. 來自事件偵測與回應的通信會在案例討論串中更新。

使用 AWS Support App in Slack 管理事件偵測與回應支援案例

您可以使用 AWS Support App in Slack 在 Slack 中管理您的 支援 案例、接收 AWS 事件偵測與回應工作負載上有關新警示啟動事件的通知，以及建立事件回應請求。

若要設定 AWS Support App in Slack，請依照《支援 使用者指南》中提供的指示進行。

> **Important**
>
> - 若要在 Slack 中接收工作負載上所有警示啟動事件的通知，您必須為已在 AWS 事件偵測與回應中上線的所有工作負載帳戶設定 AWS Support App in Slack。支援案例是在產生工作負載警示所在的帳戶中建立。
> - 在事件期間可以代表您開啟多個高嚴重性支援案例，以便與 支援 解決人員互動。您會在 Slack 中收到在事件期間開啟且與 Slack 頻道通知組態相符的所有支援案例的通知。
> - 您透過 AWS Support App in Slack 收到的通知不會取代 AWS 事件偵測與回應在事件期間，透過電子郵件或電話聯繫的工作負載初始和呈報聯絡人。

主題

Slack 中的警示啟動事件通知

您在 Slack 頻道中設定 AWS Support App in Slack 之後，就會收到 AWS 事件偵測與回應監控的工作負載上警示啟動事件的通知。

下列範例顯示警示啟動事件的通知在 Slack 中的顯示方式。

範例通知

當 AWS 事件偵測與回應確認您的警示啟動事件時，Slack 中就會產生類似以下的通知：

若要檢視 AWS 事件偵測與回應新增的完整通信，請選擇查看詳細資訊。

AWS 事件偵測與回應的進一步更新會在案例的討論串中顯示。

選擇查看詳細資訊，以檢視 AWS 事件偵測與回應新增的完整通信。

在 Slack 中建立事件回應請求

如需如何透過 AWS Support App in Slack 建立事件回應請求的說明，請參閱 請求事件回應。

事件偵測與回應中的報告

AWS 事件偵測與回應提供營運和效能資料，協助您了解服務的設定方式、事件歷史記錄，以及事件偵測與回應服務的效能。此頁面涵蓋可用的資料類型，包括組態資料、事件資料和效能資料。

組態資料

- 所有已上線的帳戶
- 所有應用程式的名稱
- 與每個應用程式相關聯的警示、執行手冊和支援設定檔

事件資料

- 每個應用程式的事件日期、數量和持續時間
- 與特定警示相關聯的事件日期、數量和持續時間
- 事件後報告

效能資料

- 服務水準目標 (SLO) 效能

請聯絡技術客戶經理，以取得您可能需要的營運和效能資料。

事件偵測與回應安全和彈性

AWS 共同責任模式適用於 支援 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。此內容包括您所使用 AWS 服務 的安全組態和管理任務。

如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。

如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和 GDPR 部落格文章。

為了保護資料，我們建議您保護 AWS 帳戶登入資料，並使用 AWS Identity and Access Management (IAM) 來設定個別使用者帳戶。如此一來，每個使用者都只會獲得授予完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用安全通訊端層/傳輸層安全性 (SSL/TLS) 憑證與 AWS 資源通訊。建議使用 TLS 1.2 或更新版本。如需相關資訊，請參閱什麼是 SSL/TLS 憑證？。
- 使用 AWS CloudTrail 設定 API 和使用者活動日誌記錄。如需相關資訊，請參閱。AWS CloudTrail
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Simple Storage Service (Amazon Simple Storage Service (Amazon S3)) 的個人資料。如需 Amazon Macie 的詳細資訊，請參閱 Amazon Macie。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關可用 FIPS 端點的資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的欄位中，例如名稱欄位。這包括當您使用 支援，或是使用主控台、API、AWS CLI 或 AWS SDK 的其他 AWS 服務 時。您在標籤或自由格式欄位中輸入的任何資料都可能用於計費或診斷記錄。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

AWS 事件偵測與回應對您帳戶的存取

AWS Identity and Access Management (IAM) 是一種 Web 服務，讓您能夠安全地控制對 AWS 資源的存取。您可以使用 IAM 來控制能通過身分驗證 (登入) 和授權使用資源的 (具有許可) 的人員。

AWS 事件偵測與回應和您的警示資料

根據預設，事件偵測與回應會接收您帳戶中每個 CloudWatch 警示的 Amazon Resource Name (ARN) 和狀態，然後在已上線的警示變更為 ALARM 狀態時啟動事件偵測與回應程序。如果您想要自訂事件偵測與回應可從您的帳戶接收哪些警示相關資訊，請聯絡您的技術客戶經理。

文件歷史記錄

下表說明自上次發行 IDR 指南之後，文件內的重要變更。

變更	描述	Date
「使用指標數學函數來隱藏 CloudWatch 警示」區段中的更新步驟	「使用指標數學函數來隱藏 CloudWatch 警示」區段中的更新步驟。 如需更多詳細資訊，請參閱 在警示來源隱藏警示。	2026 年 2 月 3 日
新增了韓文作為支援語言	新增了韓文作為支援語言。 如需更多詳細資訊，請參閱 事件偵測與回應的區域可用性。	2026 年 1 月 22 日
新增了中文作為支援語言	新增了中文作為支援語言。 如需更多詳細資訊，請參閱 事件偵測與回應的區域可用性。	2026 年 1 月 13 日
新增章節：事件偵測與回應客戶命令列介面 (CLI)	新增了事件偵測與回應客戶命令列介面 (CLI) 一節，並更新了入門一章，以加入有關事件偵測與回應客戶命令列介面 (CLI) 的資訊。 如需更多詳細資訊，請參閱 AWS 事件偵測與回應 CLI。	2025 年 12 月 8 日
更新了多個章節：事件偵測與回應中的工作負載上線和警示擷取問卷及開始使用事件偵測與回應	AWS 服務 事件處理程序不再是 AWS 事件偵測與回應的一部分。本使用者指南的章節更新後，移除了此程序的參考。您將繼續透過 AWS 服務運作狀態儀表板接收服務事件通知。AWS 事件偵測與回應客戶可以在服務事件期間，視需要使用事件回應請求獲得協助。如需更多詳細資訊，請參閱 請求事件回應。	2025 年 10 月 14 日
刪除了此節：服務事件的事件管理	AWS 服務 事件處理程序不再是 AWS 事件偵測與回應的一部分。使用者指南的本節已移除，以	2025 年 10 月 14 日

變更	描述	Date
	反映此變更。您將繼續透過 AWS 服務運作狀態儀表板接收服務事件通知。AWS 事件偵測與回應客戶可以在服務事件期間，視需要使用事件回應請求獲得協助。如需更多詳細資訊，請參閱請求事件回應。	
更新了此節：事件偵測與回應的區域可用性	AWS 事件偵測與回應現在於 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 中提供。如需詳細資訊，請參閱事件偵測與回應的區域可用性	2025 年 10 月 05 日
更新了此節：事件偵測與回應中的工作負載上線和警示擷取問卷	更新了警示矩陣表的範例電子郵件地址。如需詳細資訊，請參閱事件偵測與回應中的工作負載上線和警示擷取問卷	2025 年 8 月 26 日
更新了此節：讓工作負載訂閱 AWS 事件偵測與回應	移除了對建立案例視窗的說明區段中訂閱開始日期欄位的參考。 更新了此節：讓工作負載訂閱事件偵測與回應	2025 年 8 月 4 日
新功能：隱藏警示使其無法和事件偵測與回應互動	新增了新章節至受管工作負載，提供如何暫時或依排程隱藏警示的資訊 新章節：隱藏警示使其無法和事件偵測與回應互動	2025 年 4 月 9 日
更新了使用 AWS Support Center Console 請求事件回應的指示	新增了有關在問題說明欄位中輸入哪些資訊的詳細資訊。 更新了此節：請求事件回應	2025 年 2 月 6 日
新增了額外的 AWS 區域	事件偵測與回應可用性一節中新增了額外的 AWS 區域。 更新了此節：事件偵測與回應的區域可用性	2024 年 11 月 1 日

變更	描述	Date
更新使用 AWS Support App in Slack 管理事件偵測與回應支援案例頁面	移動了事件管理下的頁面、修訂了文字並取代了螢幕擷取畫面。 更新了此節：使用 AWS Support App in Slack 管理事件偵測與回應支援案例	2024 年 10 月 10 日
新增了一個新頁面 AWS Support App in Slack 更新了使用 AWS 事件偵測與回應進行事件管理	AWS Support App in Slack 新增了一個新頁面 更新了使用 AWS 事件偵測與回應進行事件管理，以加入新的一節「使用 AWS Support App in Slack 請求事件回應」。	2024 年 9 月 10 日
更新了帳戶訂閱	更新了帳戶訂閱一節，以納入當您請求訂閱帳戶時，在何處開啟支援案例的詳細資訊。 更新了此節：讓工作負載訂閱事件偵測與回應	2024 年 6 月 12 日
新增了新的一節：將工作負載離線	在入門中新增了將工作負載離線一節，以納入有關將工作負載離線的資訊 如需更多詳細資訊，請參閱 讓工作負載從事件偵測與回應離線。	2024 年 3 月 28 日
更新了帳戶訂閱	更新了帳戶訂閱一節，以納入有關將工作負載離線的資訊 如需詳細資訊，請參閱帳戶訂閱	2024 年 3 月 28 日
更新了測試	更新了測試一節，在上線程序的最後一個步驟中加入有關 Gameday 測試的資訊。 更新了此節：在事件偵測與回應中測試上線的工作負載	2024 年 2 月 29 日
更新了什麼是 AWS 事件偵測與回應	更新了什麼是 AWS 事件偵測與回應一節。 更新了此節：什麼是 AWS 事件偵測與回應？	2024 年 2 月 19 日

變更	描述	Date
更新了問卷一節	更新了工作負載上線問卷，並新增了警示擷取問卷。上線問卷一節已重新命名為工作負載上線和警示擷取問卷。 更新了此節：事件偵測與回應中的工作負載上線和警示擷取問卷	2024 年 2 月 2 日
更新了 AWS 服務事件和上線資訊	更新了數節以加入有關上線的新資訊。 更新了這些章節： • 事件偵測與回應中的工作負載探索 • 事件偵測與回應上線 • 讓工作負載訂閱事件偵測與回應 新章節 • 為應用程式團隊佈建 AWS Support Center Console 的存取權	2024 年 1 月 31 日
新增了相關資訊一節	存取佈建中新增了相關資訊一節。 更新了此節：佈建存取以將警示擷取至事件偵測與回應	2024 年 1 月 17 日
更新了範例步驟	更新了範例：整合來自 Datadog 和 Splunk 的通知中步驟 2、3 和 4 的程序。 更新了此節：範例：整合來自 Datadog 和 Splunk 的通知	2023 年 12 月 21 日
更新了簡介圖形和文字	更新了從與 Amazon EventBridge 直接整合的 APM 擷取警示中的圖形。 更新了此節：開發執行手冊和回應計畫，以在事件偵測與回應中回應事件	2023 年 12 月 21 日

變更	描述	Date
更新了執行手冊範本	更新了開發 AWS 事件偵測與回應的執行手冊中的執行手冊範本。 更新了此節：開發執行手冊和回應計畫，以在事件偵測與回應中回應事件	2023 年 12 月 4 日
更新了警示組態	更新了警示組態，加入有關 CloudWatch 警示組態的詳細資訊。 新章節：在事件偵測與回應中建立符合您業務需求的 CloudWatch 警示 新章節：使用 CloudFormation 範本在事件偵測與回應中建置 CloudWatch 警示 新章節：事件偵測與回應中 CloudWatch 警示的範例使用案例	2023 年 9 月 28 日
更新了入門	更新了入門，加入有關工作負載變更請求的資訊。 新章節：在事件偵測與回應中請求變更已上線的工作負載 更新了此節：讓工作負載訂閱事件偵測與回應	2023 年 9 月 05 日
入門中的新章節	新增了將警示擷取至 AWS 事件偵測與回應將警示擷取至 AWS 事件偵測與回應中。	2023 年 6 月 30 日
原始文件	AWS 事件偵測與回應首次發佈	2023 年 3 月 15 日