AWS事故偵測與回應的概念與程序

AWS事件偵測與回應使用者指南

版本 July 3, 2024

AWS事件偵測與回應使用者指南: AWS事故偵測與回應的概念與程序

Table of Contents

什麼是 AWS 事件偵測與回應？

AWS 事件偵測與回應提供符合資格的 AWS Enterprise Support 客戶主動事件互動，以減少故障的可能性，並加速從中斷回復關鍵工作負載。事件偵測與回應可促進您的協同合作， AWS 開發針對每個已登入工作負載量身打造的手冊和回應計畫。事件管理工程師 (IME) 團隊全年無休地監控您已登入的工作負載，並在發生嚴重警示後的 5 分鐘內為您提供呼叫橋接。

事件偵測與回應提供下列主要功能：

- 改善可觀察性： AWS 專家提供指引，協助您定義工作負載的應用程式和基礎架構層之間的指標和警示，並建立關聯，以及早偵測中斷情況。
- 5 分鐘回應時間：IME 全天候監控已登入的工作負載，以偵測重大事件。IME 會在警報觸發後的 5 分鐘內做出回應，或回應您向事件偵測與回應提出的關鍵業務 Support 案例。
- 解決速度更快：IME 使用專為工作負載開發的預先定義和自訂 Runbook，在 5 分鐘內回應、代表您建立 Support 案例，以及管理工作負載的事件。IME 為事件提供單執行緒擁有權，並讓您與合適的 AWS 專家保持聯繫，直到事件解決為止。
- 事件的事件管理：由於 AWS 我們瞭解重要工作負載的內容 (例如客戶、服務和執行個體)，因此我們可以偵測並主動通知您在 AWS 服務事件期間可能對工作負載造成的影響。如有要求，IME 會在 AWS 服務活動期間與您聯繫，並提供有關活動的最新消息。雖然事件偵測與回應無法排定您在服務事件期間進行復原的優先順序，但事件偵測與回應確實提供 Support 指引，協助您實作緩解計畫。
- 降低失敗的可能性：解決後，IME 會根據要求提供您事件後審查。而且， AWS 專家會與您合作，運用學到的經驗教訓，以改善事件回應計畫和手冊。您還可以利 AWS Resilience Hub 用工作負載的持續恢復追蹤。

事件偵測與回應產品術語

- AWS 事件偵測與回應適用於直接和合作夥伴轉售的企業 Support 帳戶。
- AWS 事件偵測和回應不適用於合作夥伴主導 Support 的帳戶。
- 在事件偵測與回應服務期間，您必須隨時維持 AWS 企業 Support。如需相關資訊，請參閱企業 Support。終止企業 Support 會同時從 AWS 事件偵測與回應服務中移除。
- 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架程序。
- 訂閱 AWS 事件偵測和回應帳戶的最短持續時間為九十 (90) 天。所有取消請求必須在預定取消生效日期前三十（30）天提交。
- AWS 按照AWS 隱私聲明中所述處理您的信息。

> **Note**
>
> 如需事件偵測與回應帳單相關問題，請參閱取得 AWS 帳單相關說明。

事件偵測與回應可用性

AWS 事件偵測與回應目前提供以下任何一種語言的企業 Support 帳戶使用英文版本 AWS 區域：

名稱	AWS 區域
us-east-1	美國東部 (維吉尼亞)
us-east-2	美國東部 (俄亥俄)
us-west-1	美國西部 (加利佛尼亞北部)
us-west-2	美國西部 (奧勒岡)
ca-central-1	加拿大 (中部)
sa-east-1	南美洲 (聖保羅)
eu-central-1	歐洲 (法蘭克福)
eu-west-1	歐洲 (愛爾蘭)
eu-west-2	歐洲 (倫敦)
eu-west-3	Europe (Paris)
eu-north-1	歐洲 (斯德哥爾摩)
ap-south-1	亞太區域 (孟買)
ap-northeast-1	亞太區域 (東京)
ap-northeast-2	亞太區域 (首爾)
ap-southeast-1	亞太區域 (新加坡)

名稱	AWS 區域
ap-southeast-2	亞太區域 (悉尼)

AWS 事件偵測與回應 RACI

下表顯示 AWS 事件偵測和回應負責、負責、諮詢和知情或 RACI。

活動	顧客	事件偵測與回應
資料收集		
客戶與工作負載簡介	C	R
架構	R	A
作業	R	A
確定要配置的 CloudWatch 警報	R	A
定義事件回應計劃	R	A
填寫入職問卷	R	A
作業準備檢討		
對工作負載進行架構良好的審查（WAR）	C	R
驗證事件回應	C	R
驗證警報矩陣	C	R
識別工作負載正在使用的關鍵 AWS 服務	A	R
帳戶配置		
在客戶帳戶中建立 IAM 角色	R	I
使用建立的角色安裝受管 EventBridge 規則	I	R

活動	顧客	事件偵測與回應
測試 CloudWatch 警報	R	A
驗證客戶警報是否涉及事件偵測和回應	I	R
更新鬧鐘	R	C
更新工作手冊	C	R
事件管理		
主動通知事件偵測與回應偵測到的事件	I	R
提供事件回應	I	R
提供事故解決/基礎結構還原	R	C
事件後審查		
請求事件後審查	R	I
提供事件後審查	I	R

AWS 事件偵測與回應架構

AWS 事件偵測與回應與您現有的環境整合，如下圖所示。該架構包括以下服務：

- Amazon EventBridge：Amazon EventBridge 是您工作負載與 AWS 事件偵測與回應之間的唯一整合點。使用由 AWS管理的預先定義規則，透過 Amazon CloudWatch 從您的監控工具 (例如 EventBridge Amazon) 擷取警示。若要允許事件偵測與回應建置及管理 EventBridge 規則，請安裝服務連結角色。要了解有關這些服務的更多信息，請參閱什麼是 Amazon EventBridge 和 Amazon EventBridge 規則，什麼是 Amazon CloudWatch 和使用服務鏈接角色。 AWS Health
- AWS Health：持續 AWS Health 提供您的資源效能以及您和帳戶的可用性的可用性 AWS 服務 的可見性。事件偵測與回應會用 AWS Health 來追蹤工作負載使 AWS 服務 用的事件，並在收到工作負載的警示時通知您。若要深入瞭解 AWS Health，請參閱「什麼是 AWS Health」。
- AWS Systems Manager：Systems Manager 提供統一的使用者介面，可在您的 AWS 資源中進行自動化和工作管理。AWS 事件偵測與回應會在文件中託管工作負載的相關資訊，包括工作負載架構圖、警示詳細資料及其對應的事 AWS Systems Manager 件管理手冊 (如需詳細資訊，請參閱AWS Systems Manager 文件)。若要深入瞭解 AWS Systems Manager，請參閱「什麼是 AWS Systems Manager」。
- 您的特定手冊：事件管理手冊定義 AWS 事件偵測和回應在事件管理期間執行的動作。您的特定手冊會告訴 AWS 事件偵測和回應應聯絡人員、如何聯絡他們，以及要分享哪些資訊。

開始使用AWS事件偵測與回應

您可以使用事件偵測與回應，選取特定工作負載進行監控和關鍵AWS事件管理。工作負載是資源和程式碼的集合，可共同運作以提供商業價值。工作負載可能是構成您銀行支付門戶或客戶關係管理（CRM）系統的所有資源和代碼。您可以在一個單一的方式託管工作負載 AWS 帳戶或多個 AWS 帳戶。

例如，您可能在單一帳戶中託管一個整合式應用程式 (例如，Fig.1 中的員工績效應用程式)。或者，您可能有一個應用程式 (例如，圖 1 中的 Storefront Webapp) 分解為橫跨不同帳戶的微型服務。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)，如圖 1 所示。

> **Note**
>
> 若要變更您的 Runbook、工作負載資訊或AWS事件偵測與回應上監視的警示，請建立要求變更已登入的工作負載.

入職

AWS 與您合作，將您的工作負載和警報加入AWS事件偵測與回應。您提供關鍵資訊 AWS ，位於 工作負載上線和警示擷取問卷。最佳做法是在上註冊工作負載 AppRegistry。若要取得更多資訊，請參閱AppRegistry 使用者指南。

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 與您合作，瞭解您的工作負載，以及在事件發生時如何為您提供支援，AWS 服務事件。您可以提供有關工作負載的重要資訊，以協助緩解影響。

按鍵輸出：

- 一般工作量資訊
- 架構細節，包括圖表
- 手冊資訊

- 客戶發起的事件
- AWS 服務事件

警報攝入

AWS 與您一起使用您的鬧鐘。AWS事件偵測和回應可透過 Amazon 擷取 Amazon CloudWatch 和第三方應用程式效能監控 (APM) 工具的警示。 EventBridge入職警報可讓您主動偵測事件並自動化參與。如需詳細資訊，請參閱擷取與 Amazon EventBridge 直接整合的警示。APMs

按鍵輸出：

- 報警矩陣

下表列出將工作負載上線至AWS事件偵測與回應所需的步驟。該表顯示了每個任務的實例持續時間。每個任務的實際日期都是根據團隊的可用性和時間表來定義的。

帳戶訂閱

若要將工作負載訂閱「AWS事件偵測與回應」，請為每個工作負載建立新的支援案例。建立支援案例時，請記住下列事項：

- 將單一工作負載上線 AWS 帳戶中，從工作負載的帳戶或付款人帳戶建立支援案例。
- 將跨越多個工作負載的上線 AWS 帳戶，從付款人帳戶建立支援案例。在支援案例正文中，列出IDs要上載的所有帳戶。

> **Important**
>
> 如果您建立支援案例以從錯誤的帳戶訂閱工作負載至事件偵測與回應，則在訂閱工作負載之前，您可能會遇到延遲並要求其他資訊。

若要訂閱工作負載

1. 前往 AWS Support 置中，然後選取 [建立案例]，如下列範例所示。您只能從已註冊企業 Support 的帳戶訂閱工作負載。

2. 填寫支援案例表格：

   - 選取 [技術支援]。
   - 針對「服務」，選擇「事件偵測與回應」。
   - 在類別中，選擇內建新工作負載。
   - 針對嚴重性，選擇一般指引。

3. 輸入此變更的「主旨」。例如：

   [板載] AWS 事件偵測與回應- *workload_name*

4. 輸入此變更的「摘要」。例如，輸入「此要求將工作負載上線至AWS事件偵測與回應」。請務必在要求中包含下列資訊：

   - 工作負載名稱：工作負載名稱。
   - 帳戶 ID：ID1、ID2ID3、等等。這些是您想要加入AWS事件偵測與回應的帳戶。
   - 訂閱開始日期：您要開始「AWS事件偵測與回應」訂閱的日期。

5. 在 [其他聯絡人-選擇性] 區段中，輸入您要接收有關此要求之通訊的任何電子郵件IDs。

   以下是「其他聯絡人-選用」區段的範例：

   > **Important**
   >
   > 若未IDs在 [其他聯絡人-選用] 區段中新增電子郵件，可能會延遲AWS事件偵測與回應上線程序。

6. 選擇提交。

   提交請求後，您可以從組織新增其他電子郵件。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IDs中新增電子郵件。

   以下是「其他聯絡人-選用」區段的範例：

建立訂閱要求的支援案例後，請保留下列兩份文件，以便繼續進行工作負載上線程序：

- AWS 工作負載架構圖。

- 工作負載上線和警示擷取問卷：完成問卷中與您正在上線的工作負載相關的所有資訊。如果您要加入多個工作負載，請為每個工作負載建立新的入職問卷。如果您對填寫入職問卷有任何疑問，請聯絡您的技術客戶經理 (TAM)。

> **Note**
>
> 請使用「NOT附加檔案」選項，將這兩份文件附加到案例中。AWS事件偵測與回應團隊會透過 Amazon 簡易儲存服務上傳連結回覆個案，讓您上傳文件。

如需如何使用AWS事件偵測與回應建立案例，以要求變更現有已登入工作負載的資訊，請參閱。要求變更已登入的工作負載如需有關如何離開工作負載的資訊，請參閱離開工作負載。

工作量探查

AWS 與您合作，盡可能了解有關工作負載的內容。AWS事件偵測與回應會使用此資訊建立 Runbook，以便在事件發生時為您提供支援， AWS 服務事件。必要的資訊會在中擷取工作負載上線和警示擷取問卷。在上註冊您的工作負載是最佳做法 AppRegistry。若要取得更多資訊，請參閱AppRegistry 使用者指南。

按鍵輸出：

- 工作負載資訊，例如工作負載的說明、架構圖表、連絡人和呈報詳細資料。
- 工作負載如何採用的詳細資料 AWS 每個服務 AWS 區域。
- 有關如何的具體信息 AWS 在服務事件期間為您提供支援。
- 您的團隊用來偵測重大工作負載影響的警示。

警報配置

AWS 與您合作定義指標和警示，以提供您應用程式及其基礎效能的可見性 AWS 基礎設施。我們要求警示在定義和設定閾值時遵守下列準則：

- 警示只會在受監控的工作負載造成嚴重影響時 (收入損失或大幅降低效能的客戶體驗降低) 造成嚴重影響時，才會進入「警示」狀態，而且需要操作員立即注意。
- 警示也必須與您指定的工作負載解析器互動，同時或在事件管理團隊之前使用。事件管理工程師應該在緩解過程中與您指定的解析器進行協作，而不是作為第一線響應者，然後升級給您。

- 必須將警示閾值設定為適當的閾值和持續時間，以便在警示觸發調查時，任何時候都必須發生。如果警報在「警報」和「正常」狀態之間跳動，則會產生足夠的影響以保證操作員的反應和注意力。

警報類型：

- 描繪業務影響程度的警報，並傳遞相關資訊以進行簡單的故障偵測。
- Amazon CloudWatch 金絲雀。如需詳細資訊，請參閱加那利群島和 X-Ray 追蹤和 X-Ray 追蹤。
- 聚合警報（監視依賴關係）

示例報警，全部使用 CloudWatch 監控系統

度量名稱/警報值值	警示ARN或資源 ID	如果此警報觸發	如果參與，請剪下這些服務的進階 Support 案例
API錯誤/ 對於 10 個資料點，大於等於 10 個的錯誤數量	警報：AW：雲觀察：美國西部-2：000000000000：警報：E2-錯誤 MPmimLambda	票證削減到數據庫管理員（DBA）團隊	API閘道器，Lambda
ServiceUnavailable（HTTP 狀態碼 503） 在 5 分鐘窗口中 10 個數據點（不同的客戶端）的錯誤數 > = 3	警報:awn: 雲監視:美國西部-2: XXXXX: 警報:	門票削減給服務團隊	API閘道器，Lambda
ThrottlingException（HTTP 狀態碼 400） 在 5 分鐘窗口中 10 個數據點（不同的客戶端）的錯誤數 > = 3	警報:AWN: 雲監視:我們-西部-2: XXXXX: 警報:	門票削減給服務團隊	EC2，Amazon Aurora

如需詳細資訊，請參閱AWS 事件偵測與回應監控與觀察能力。

按鍵輸出：

- 工作負載警示的定義和組態。
- 完成入職問卷上的警示詳細資訊。

在事件偵測與回應中建立符合您業務需求的 CloudWatch 警報

建立 Amazon CloudWatch 警示時，您可以採取幾個步驟來確保鬧鐘最符合您的業務需求。

查看您建議的 CloudWatch 鬧鐘

檢閱您提議的警示，確保警示只有在受監控的工作負載產生重大影響時 (收入損失或降低客戶體驗會大幅降低效能)，才會進入「警示」狀態。例如，您認為此警報是否足夠重要，以至於進入「警報」狀態時必須立即做出反應？

以下是可能代表重要業務影響的建議度量，例如影響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 Edge 函數量度量。
- 應用程式負載平衡器：如果可能，最佳做法是為應用程式負載平衡器建立下列警示：
  - HTTPCode計ELB數
  - HTTPCode目標計數

  上述警示可讓您監視來自應 Application Load Balancer 後方或其他資源之後的目標的回應。這使得更容易識別 5XX 錯誤的來源。如需詳細資訊，請參閱應用程式負載平衡器的CloudWatch 指標。
- Amazon API 閘道：如果您 WebSocket API在 Elastic Beanstalk 中使用，請考慮使用以下指標：
  - 整合錯誤率 (篩選為 5XX 錯誤)
  - 整合延遲
  - 執行錯誤

  如需詳細資訊，請參閱使用測 CloudWatch 量結果監視 WebSocket API執行。
- Amazon 路線 53：監控指EndPointUnhealthyENICount標。此測量結果是處於「自動復原」狀態的彈性網路介面數目。此狀態表示解析程式嘗試復原與端點相關聯的一或多個 Amazon 虛擬私有雲網路界面 (由EndpointId指定)。在復原程序中，端點在容量有限的情況下運作。端點在完全復原之前無法處理DNS查詢。如需詳細資訊，請參閱使用 Amazon 監控 Route 53 解析器端點。 CloudWatch

驗證您的警報配置

確認提議的警報符合您的業務需求後，請驗證警示的組態和歷史記錄：

- 驗證測量結果的「臨界值」，以根據量度的圖形趨勢進入「警示」狀態。
- 驗證用於輪詢資料點的「期間」。60 秒的輪詢資料點有助於早期事件偵測。
- 驗證組DatapointToAlarm態。在大多數情況下，最好將其設置為 3 或 5 中的 5 個。在事件中，設定為 [60 秒量度 (共 3 個) DatapointToAlarm] 時，警示會在 3 分鐘後觸發，或設為 [60 秒量度，共 5 個量度中有 5 個 DatapointToAlarm] 時 5 分鐘後觸發警示。使用此組合可消除嘈雜的警報。

> **Note**
>
> 上述建議可能會因您使用服務的方式而有所不同。每個AWS服務在工作負載內的運作方式不同而且，在多個地方使用相同的服務可能會有所不同。您必須確定您瞭解工作負載如何利用提供警示的資源，以及上游和下游的影響。

驗證警示如何處理遺失資料

某些量度來源不會定期將資料傳送 CloudWatch 至。對於這些指標，最佳做法是將遺失的資料視為notBreaching。如需詳細資訊，請參閱設定 CloudWatch 警示如何處理遺失的資料和避免過早轉換為警示狀態。

例如，如果測量結果監控錯誤率且沒有錯誤，則量度不會報告任何資料 (nil) 資料點。如果您將警示設定為將遺失的資料視為「遺失」，則單一違規資料點後接兩個無資料 (nil) 資料點會導致量度進入「警示」狀態 (針對 3 個資料點中的 3 個)。這是因為缺少的資料組態會評估評估期間中最後一個已知的資料點。

在指標監視錯誤率的情況下，在沒有服務降級的情況下，您可以假設沒有數據是好事。最佳做法是將遺失的資料視為「正notBreaching常」，而且量度不會在單一資料點上進入「警示」狀態，將遺失的資料視為「正常」。

查看每個警報的歷史記錄

如果警報的歷史記錄顯示它經常進入「鬧鐘」狀態，然後快速恢復，則警報可能會成為您的問題。確保調整警報以防止噪音或誤報。

驗證基礎資源的指標

請確定您的指標會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。這可能會導致警報進入「鬧鐘」狀態。

建立複合警報

如果您提供事件偵測與回應作業，其中包含大量警示以供上線，系統可能會要求您建立複合警示。複合警報可減少需要登入的警報總數。

使用 AWS CloudFormation 在事件偵測與回應中建立 CloudWatch 警示的範本

為了加速AWS事件偵測與回應的上線速度，並減少建立警示所需的工作量， AWS 為您提供 AWS CloudFormation 範本。這些範本包括常用服務的最佳化警示設定，例如 Application Load Balancer、Network Load Balancer 和 Amazon。 CloudFront

使用 CloudFormation 範本建立 CloudWatch 警示

1. 使用提供的鏈接下載模板：

NameSpac	指標	Compariso nOperator (臨界值)	期間	Datapoint sToAlarm	TreatMiss ingData	統計數字	樣板連結
應用 Elastic Load Balancer	（立方米 + 平方米）/（立方米 + 平方米 + 平方米 4）* 100 立方米 = _ 目標 _ 計數 m2 = 目標 _ 目標 _ 計數 M3	LessThanT hreshold 九十五	60	3 出來的 3	丟失	總和	Template (範本)

NameSpac	指標	Compariso nOperator (臨界值)	期間	Datapoint sToAlarm	TreatMiss ingData	統計數字	樣板連結
	= _ 目標 _ 目標 _4xx_ 計數 M4= 目標 _5XX_ 計數 HTTPCode HTTPCode HTTPCode HTTPCode						
Amazon CloudFron t	TotalErro rRate	GreaterTh anThresho ld(五)	60	3 出來的 3	notBreach ing	平均數	Template (範本)
應用 Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(二)	60	3 出來的 3	notBreach ing	最大	Template (範本)
網路 Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(二)	60	3 出來的 3	notBreach ing	最大	Template (範本)

2. 檢閱下載的JSON檔案，確定其符合您組織的作業和安全性程序。
3. 創建一個 CloudFormation 堆棧：

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

a. 打開 AWS CloudFormation 控制台在 https://console.aws.amazon.com/雲形成。

b. 選擇建立堆疊。

c. 選擇 [範本已準備就緒]，然後從本機資料夾上載範本檔案。

以下是「建立堆疊」畫面的範例。

d. 選擇 Next (下一步)。

e. 輸入下列必要資訊：

- AlarmNameConfig和 AlarmDescriptionConfig：輸入鬧鐘的名稱和說明。
- ThresholdConfig：修改閾值以符合應用程序的要求。
- D istributionIDConfig：確保分發 ID 指向您正在創建的帳戶中的正確資源 AWS CloudFormation 堆疊。

f. 選擇 Next (下一步)。

g. 檢閱、和欄位PeriodConfig中EvalutionPeriodConfig的預設DatapointsToAlarmConfig值。最佳做法是針對這些欄位使用預設值。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與SNS通知資訊。最佳作法是開啟終止保護，以防止意外刪除警示。若要開啟終止保護，請選取 [已啟動] 選項按鈕，如下列範例所示：

i. 選擇 Next (下一步)。

j. 檢閱堆疊設定，然後選擇 [建立堆疊]。

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

4. 在正確的帳戶中創建所有鬧鐘後 AWS 請通知您的技術客戶經理 (TAM)。AWS事件偵測與回應團隊會審核新警報的狀態，然後繼續您的上線作業。

事件偵測與回應中的 CloudWatch 警示使用案例範例

請參閱下列使用案例，瞭解如何在事件偵測和回應中使用 Amazon CloudWatch 警示。

範例使用案例 A：Application Load Balancer

建立以下 CloudWatch 警示，以表示潛在的工作負載影響。您可以建立度量數學運算，在成功連線低於特定臨界值時發出警示。如需可用的 CloudWatch 指標，請參閱 Ap plication Load Balancer 的 CloudWatch 指標

公制: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/應用程式 ELB

ComparisonOperator(臨界值)：小於 x (x = 客戶的門檻)。

使用時間：60 秒

DatapointsToAlarm: 3 出來的 3

遺失資料處理：將遺失的資料視為違規。

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 閘道

建立以下 CloudWatch 警示，以表示潛在的工作負載影響。您可以建立一個複合量度，以便在閘道中出現高通道或平均 4XX 錯誤數量過高時發出警示。API如需可用指標，請參閱 Amazon API 閘道維度和指標

公制:compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))

NameSpace: AWS/API閘道

ComparisonOperator(臨界值)：大於 (x 或 y 客戶的臨界值)

使用時間：60 秒

DatapointsToAlarm: 1 出來的 1

遺失資料處理：將遺失的資料視為不違規。

統計：

下圖顯示使用案例 B 的流程：

示例用例 C：Amazon 路線 53

您可以透過建立 Route 53 運作狀態檢查來監控資源，這些檢查用 CloudWatch 來收集原始資料並將其處理為可讀且接近即時的指標。您可以建立下列 CloudWatch 警示，以表示潛在的工作負載影響。您可以使用指 CloudWatch 標來創建警報，該警報在超出建立的閾值時觸發。如需可用的 CloudWatch 量度，請參閱 Route 53 運作狀態檢查的CloudWatch 指標

公制:R53-HC-Success

NameSpace: AWS/53號公路線

臨界值 HealthCheckStatus：3 分鐘內 3 個資料點 HealthCheckStatus < x (即 x 客戶的閾值)

時間：1 分鐘

DatapointsToAlarm: 3 出來的 3

遺失資料處理：將遺失的資料視為違規。

統計資料：最小值

下圖顯示了用例 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

在此案例中，您必須花點時間定義適當的健康狀態檢查。如果您只驗證應用程式的連接埠已開啟，則表示您尚未驗證應用程式是否正常運作。此外，調用應用程序的首頁不一定是確定應用程序是否正常工作的正確方法。例如，如果應用程式依賴於資料庫 AND Amazon 簡單儲存服務，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視網頁，例如 /monitor。監控網頁會呼叫資料庫，以確保它可以連線並取得資料。而且，監控網頁會呼叫 Amazon S3。然後，您可以將負載平衡器上的健康狀態檢查指向 /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事件偵測和回應與不同的應用程式效能監控 (APM) 工具 (包括 Amazon) 整合 CloudWatch， DataDog 並直接APMs與 Amazon 整合 EventBridge (例如 New Relic)，APMs而且無需與 Amazon EventBridge 直接整合。有關直接集成到 Amazon APMs 的完整列表 EventBridge，請參閱 Amazon EventBridge 集成。

主題

- 針對事件偵測與回應提供警示擷取的存取權
- 將事件偵測和回應與 Amazon 整合 CloudWatch
- 擷取與 Amazon 直APMs接整合的警示 EventBridge
- 範例：整合來自資料多和 Splunk 的通知
- 使用 Webhook 在不與 Amazon 直接集成的APMs情況下導入警報 EventBridge

針對事件偵測與回應提供警示擷取的存取權

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 假設SLR建立 Amazon 受 EventBridge管規則。受管規則會將通知從您的帳戶傳送至「AWS事件偵測與回應」。有關此信息SLR，包括相關的 AWS 受管理策略，請參閱在 AWS Health 用戶指南。

您可以依照建立服務連結角色中的指示，在您的帳戶中安裝此服務連結角色 AWS Identity and Access Management 用戶指南。或者，您可以使用下列AWS指令行介面 (AWSCLI) 指令：

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

按鍵輸出

- 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：

- 對 AWS Health 使用服務連結角色

- 建立服務連結角色
- AWS受管理的策略： AWSHealth_EventProcessorServiceRolePolicy

將事件偵測和回應與 Amazon 整合 CloudWatch

AWS事件偵測和回應會使用您在存取佈建期間開啟的服務連結角色 (SLR)，在您的 EventBridge AWS 名為的帳號`AWSHealthEventProcessor-DO-NOT-DELETE`。事件偵測與回應會使用此規則從您的帳戶擷取 Amazon CloudWatch 警示。擷取鬧鐘不需要其他步驟。 CloudWatch

擷取與 Amazon 直APMs接整合的警示 EventBridge

下圖顯示透過與 Amazon EventBridge (例如 Datadog 和 Splunk) 直接整合的應用程式效能監控 (APM) 工具傳送通知至AWS事件偵測和回應的程序。如需直接整合APMs的完整清單 EventBridge，請參閱 Amazon EventBridge 整合

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

設定與AWS事件偵測與回應的整合

您必須為每個步驟完成以下步驟 AWS 帳戶和 AWS 區域。警報必須來自 AWS 帳戶和 AWS 應用程式資源所在的區域。

1. 設定您的每個作APMs為 Amazon EventBridge 合作夥伴事件來源 (例如`aws.partner/my_apm/integrationName`)。如需設定APM為事件來源的指導方針，請參閱透過 Amazon 從 SaaS 合作夥伴接收事件 EventBridge。這會在您的帳戶中建立合作夥伴活動匯流排。
2. 執行以下任意一項：
   - (建議方法) 建立自訂 EventBridge 事件匯流排。AWS事件偵測與回應會透過安裝受管規則 (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) 匯流排`AWSServiceRoleForHealth_EventProcessor`SLR。規則來源是自訂事件匯流排。規則目的地為「AWS事件偵測與回應」。該規則與攝取第三方APM事件的模式相匹配。
   - (替代方法) 使用預設事件匯流排，而非自訂事件匯流排。預設事件匯流排要求受管規則將APM警示傳送至「AWS事件偵測與回應」。
3. 建立 AWS Lambda函數（例如，`My_APM-AWSIncidentDetectionResponse-LambdaFunction`）轉換您的合作夥伴事件總線事件。轉換後的事件符合受管規則`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`。

a. 轉換後的事件包括唯一的AWS事件偵測與回應識別碼，並將事件的來源和詳細資料類型設定為必要的值。此模式符合受管規則。

b. 將 Lambda 函數的目標設定為在步驟 2 (建議方法) 中建立的自訂事件匯流排或預設事件匯流排。

4. 建立 EventBridge 規則，並定義符合您要推送至「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.合作夥伴 integrationName /my_apm/)。規則的目標是您在步驟 3 中定義的 Lambda 函數 (例如`My_APM-AWSIncidentDetectionResponse-LambdaFunction`)。有關定義規則的指南，請參閱 Amazon EventBridge EventBridge 規則。

如需如何設定合作夥伴事件匯流排整合以與AWS事件偵測與回應搭配使用的範例，請參閱範例：整合來自資料多和 Splunk 的通知。

範例：整合來自資料多和 Splunk 的通知

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

1. 在您的AWS帳戶中將您設置APM為 Amazon EventBridge 中的事件來源。
2. 建立自訂事件匯流排。
3. 創建一個 AWS Lambda 用於轉換的函數。
4. 建立您的自訂 EventBridge 規則。

第 1 步：在 Amazon 中將您的事件源設置APM為事件源 EventBridge

在您的AWS帳戶中APMs將您的每個設置為 Amazon EventBridge 中的事件來源。如需將您的事件來源設定APM為事件來源的說明，請參閱 Amazon EventBridge 合作夥伴中工具的事件來源設定說明。

透過APM將您的事件來源設定APM為事件來源，您可以將通知導入AWS帳戶中的事件匯流排。設定完成後，AWS事件偵測與回應可在事件匯流排收到事件時啟動事件管理程序。這個過程將 Amazon EventBridge 作為您的目的地APM.

步驟 2：建立自訂事件匯流排

使用自訂事件匯流排是最佳作法。AWS事件偵測與回應使用自訂事件匯流排來擷取轉換後的事件。同時 AWS Lambda 函數轉換合作夥伴事件總線事件，並將其發送到自定義事件總線。AWS事件偵測與回應會安裝受管規則，以便從自訂事件匯流排擷取事件。

您可以使用預設事件匯流排，而非自訂事件匯流排。AWS事件偵測與回應會將受管理規則修改為從預設事件匯流排 (而非自訂事件匯流排) 內嵌。

在您的系統中建立自訂活動匯流排 AWS 帳戶：

1. 打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/
2. 選擇巴士，活動巴士。
3. 在「自訂事件匯流排」下，選擇「建立
4. 在「名稱」下提供活動匯流排的名稱。建議的格式為 APMName-AWSIncidentDetectionResponse-EventBus。

   例如，如果您使用資料多或 Splunk，請使用下列其中一項：

   - 達塔多格：數據多--AWSIncidentDetectionResponse EventBus
   - 潑濺：潑濺--AWSIncidentDetectionResponse EventBus

步驟 3：創建一個 AWS Lambda 轉換函數

Lambda 函數會在步驟 1 中的合作夥伴事件匯流排和步驟 2 中的自訂 (或預設) 事件匯流排之間轉換事件。Lambda 函數轉換符合AWS事件偵測與回應管理規則。

創建一個 AWS Lambda 在你的功能 AWS 帳戶

1. 開啟 [函數] 頁面 AWS Lambda 控制台。
2. 選擇建立函數。
3. 選擇「從頭開始作者」標籤。
4. 在函數名稱中，使用格式輸入名稱`APMName-AWSIncidentDetectionResponse-LambdaFunction`。

   以下是資料多和潑濺的範例：

   - 達塔多格：數據多--AWSIncidentDetectionResponse LambdaFunction
   - 潑濺：潑濺--AWSIncidentDetectionResponse LambdaFunction
5. 在「執行階段」中，輸入 Python 3.10。
6. 將其餘欄位保留為預設值。選擇建立函數。
7. 在程式碼編輯頁面上，以下列程式碼範例中的函數取代預設 Lambda 函數內容。

   請注意下列程式碼範例中以 # 開頭的註解。這些註解會指出要變更的值。

數據多轉換代碼模板：

```
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'])
```

潑濺轉換代碼模板：

```
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. 為您要將轉換後的資料傳送至的事件匯流排新增 Lambda 執行角色的PutEvents權限：

   a. 開啟 [函數] 頁面 AWS Lambda 控制台。
   b. 選取函數，然後在 [組態] 索引標籤上選擇 [權限]。
   c. 在 [執行角色] 底下，選取要開啟執行角色的角色名稱 AWS Identity and Access Management 控制台。
   d. 在 [權限原則] 下，選取現有的原則名稱以開啟原則。
   e. 在此原則中定義的權限下，選擇 [編輯]。
   f. 在 [原則編輯器] 頁面上，選取 [新增陳述式]：
   g. 原則編輯器會新增類似下列內容的新空白陳述式

   h. 將新自動產生的陳述式取代為下列項目：

```
{
  "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，則資源是您在其中建立的自訂事件匯流排步驟 2：建立自訂事件匯流排或預設事件匯流排的。ARN ARN

10. 檢閱並確認必要的權限已新增至角色。
11. 選擇 [將此新版本設定為預設值]，然後選擇 [儲存變更]。

有效負載轉換需要什麼？

在AWS事件偵測與回應所擷取的事件匯流排事件中，需要下列 JSON key: value 配對。

```
{
    "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在轉換前後的事件。


```
{
    "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指出警示來源、來源來自夥伴APM，且incident-detection-response-identifier金鑰不存在。APM

Lambda 函數會轉換上述事件，並將其置於目標自訂或預設事件匯流排。轉換後的裝載現在包含必要的索引鍵:value 配對。

```
{
    "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ams.monitoring/generic-apm，現在detail-type是 sourceGenericAPMEvent，並且在詳細信息下有新的鍵：值對：。incident-detection-response-identifier

在上述範例中，incident-detection-response-identifier值取自路徑下的警示名稱$.detail.meta.monitor.name。APM警示名稱路徑不同。APM必須修改 Lambda 函數，才能從正確的合作夥伴事件JSON路徑取得警示名稱，並將其用於incident-detection-response-identifier值。

上設定的每個唯一名稱都會incident-detection-response-identifier在上線期間提供給AWS事件偵測與回應小組。不會處理具有未知名稱的incident-detection-response-identifier事件。

步驟 4：創建自定義 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 函數。

如需定義規 EventBridge 則的指導方針，請參閱 Amazon EventBridge 規則。

1. 打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/
2. 選擇 [規則]，然後選取與您相關聯的合作夥伴活動匯流排APM。以下是合作夥伴活動總線的範例：
   - 資料處理器：aws.合作夥伴/資料流網/事件總線名稱
   - 分享:aws.合作夥伴/信號fx/ RandomString
3. 選擇 [建立規則] 以建立新 EventBridge 規則。
4. 針對規則名稱，輸入下列格式的名稱APMName-AWS Incident Detection and Response-EventBridgeRule，然後選擇下一步。以下是範例名稱：
   - 達塔多格：數據多--AWSIncidentDetectionResponse EventBridgeRule
   - 潑濺：潑濺--AWSIncidentDetectionResponse EventBridgeRule
5. 對於事件來源，請選取AWS事件或 EventBridge 合作夥伴事件。
6. 將 [範例] 事件和 [建立方法] 保留為預設值。
7. 對於事件模式，請選擇下列項目：
   a. 事件來源： EventBridge 合作夥伴。
   b. 合作夥伴：選擇APM合作夥伴。
   c. 事件類型：所有事件。

   以下是事件模式範例：

示例數據多事件模式

溢出事件模式範例

8. 針對「目標」，選擇下列項目：
   a. 目標類型： AWS 服務
   b. 選取目標：選擇 Lambda 函數。
   c. 函數：您在步驟 2 中建立的 Lambda 函數的名稱。
9. 選擇下一步，儲存規則。

使用 Webhook 在不與 Amazon 直接集成的APMs情況下導入警報 EventBridge

AWS事件偵測和回應支援使用 Webhook 從沒有直接與 Amazon 整合APMs的第三方擷取警示。EventBridge

有關APMs與 Amazon 直接集成的列表 EventBridge，請參閱 Amazon EventBridge 集成。

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

使用網路掛接擷取事件

1. 定義 Amazon API 閘道以接受您的APM.
2. 定義一個 AWS Lambda 使用驗證 Token 進行授權的功能，如前圖所示。
3. 定義第二個 Lambda 函數，以轉換AWS事件偵測和回應識別碼，並將其附加至您的承載。您也可以使用此功能來篩選要傳送至「AWS事件偵測與回應」的事件。
4. 設定您的APM將通知傳送至API閘道URL產生的通知。

開發AWS事件偵測與回應的手冊

您可以下載範例事件偵測與回應手冊：aws-idr-runbook-example. zip。

事件偵測與回應會使用從您的入職問卷調查中擷取的資訊，為影響工作負載的事件管理開發手冊和回應計畫。Runbook 文件事件管理員在回應事件時採取的步驟。回應計劃會對應至少一個工作負載。事件管理團隊會根據您在工作負載探查期間提供的資訊建立這些範本，如前所述。響應計劃是 AWS Systems Manager (SSM) 用來觸發事件的文件範本。若要進一步瞭解SSM文件，請參閱 AWS Systems Manager 文件，若要深入了解事件管理員，請參閱什麼是 AWS Systems Manager Incident Manager?

按鍵輸出：

- 完成「AWS事件偵測與回應」上的工作負載定義。
- 完成關於AWS事件偵測與回應的警報、手冊和回應計畫定義。

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

示例手冊：

```
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.
```

測試已登入的工作負載

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

入職過程的最後一步是為您的新工作負載執行遊戲日。警報擷取完成後，AWS事件偵測與回應會確認您選擇開始遊戲日的日期和時間。

您的遊戲日有兩個主要目的：

- 功能驗證：確認AWS事件偵測與回應能正確接收警示事件。而且，功能驗證會確認您的警示事件會觸發適當的 Runbook 和任何其他所需動作，例如 auto 動建立案例 (如果您在警報擷取期間選取)。
- 模擬：遊戲日是對真實事件中可能發生的事情的端對端模擬。AWS事件檢測和響應遵循您規定的 runbook 步驟，讓您深入了解如何真正的事件可能會展開. 遊戲日是您提出問題或完善說明以提高參與度的機會。

在警報測試期間，AWS事件偵測與回應會與您合作，協助您修正任何已識別的問題。

CloudWatch 警報

AWS事件偵測和回應會監控 CloudWatch 警示的狀態變更，以測試 Amazon 警示。若要執行此操作，請使用 AWS Command Line Interface。 您也可以存取 AWS CLI from AWS CloudShell。 AWS事件偵測與回應為您提供下列清單： AWS CLI 指令供您在測試期間使用。

範例 AWS CLI 設置警報狀態的命令：

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

若要深入瞭解如何手動變更 CloudWatch 警示狀態，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 許可參考資料。

第三方APM警報

使用第三方應用程式效能監控 (APM) 工具 (例如 DataDog Splunk 或 Dynatrace) 的工作負載需要不同的指令來模擬警示。 NewRelic在「AWS事件偵測與回應」要求開始時 GameDay，您會暫時變更警示閾值或比較運算子，以強制警示進入ALARM狀態。此狀態會觸發承載至AWS事件偵測與回應。

按鍵輸出

按鍵輸出：

- 警報擷取成功，您的警報設定正確。
- AWS事件偵測與回應已成功建立及接收警示。
- 為您的參與創建一個支持案例，並通知您指定的聯繫人。
- AWS事件檢測和響應可以通過您規定的會議方式與您進行互動。
- 解決了作為 Gameday 一部分產生的所有警報和支持案例。
- 系統會傳送 Go-Live 電子郵件，確認AWS事件偵測與回應正在監控您的工作負載。

工作負載上線和警示擷取問卷

下載工作負載上線問卷。

下載警報擷取問卷。

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 公司
此工作負載的名稱 (包括任何縮寫)	Amazon 零售業務（ARO）
主要使用者和此工作負載的功能。	此工作負載是一個電子商務應用程序，允許最終用戶購買各種物品。這項工作負載是我們業務的主要收入產生器。
適用於此工作負載的合規性和/或法規要求，以及從下列項目 AWS 事件發生後。	工作量涉及病人的健康記錄，必須保持安全和保密。

工作負載入職問卷-架構問題

架構問題

問題	回應範例
一個列表 AWS 用於定義屬於此工作負載之資源的資源標記。 AWS 使用這些標記來識別此工作負載的資源，以便在事件發生時加速支援。 Note 標籤會區分大小寫。如果您提供多個標記，則此工作負載使用的所有資源都必須具有相同的標記。	appName: 最佳 環境：生產
一個列表 AWS 此工作負載所使用的服務及 AWS 他們所在的帳戶和地區。	路線 53：路由互聯網流量到ALB. 帳戶名稱:

問題	回應範例
Note 為每個服務建立新資料列。	地區：美國 EAST -1，美國 WEST -2
一個列表 AWS 此工作負載所使用的服務及 AWS 他們所在的帳戶和地區。 Note 為每個服務建立新資料列。	ALB：將傳入流量路由到目標ECS容器群組。 帳戶： 地區:
一個列表 AWS 此工作負載所使用的服務及 AWS 他們所在的帳戶和地區。 Note 為每個服務建立新資料列。	ECS：主要業務邏輯叢集的計算基礎架構。負責處理傳入的用戶請求並向持久層進行查詢。 帳戶： 地區:美國 EAST -1
一個列表 AWS 此工作負載所使用的服務及 AWS 他們所在的帳戶和地區。 Note 為每個服務建立新資料列。	RDS：Amazon Aurora 叢集會儲存由ECS商業邏輯層存取的使用者資料。 帳戶： 地區:美國 EAST -1
一個列表 AWS 此工作負載所使用的服務及 AWS 他們所在的帳戶和地區。 Note 為每個服務建立新資料列。	S3：存放網站靜態資產。 帳戶： 地區:
詳細說明如果發生中斷，可能會影響此工作負載的任何上游/下游元件。	驗證微服務：將防止用戶加載其健康記錄，因為他們將未經身份驗證。

問題	回應範例
是否有任何內部部署或非AWS 此工作負載的元件？ 如果是這樣，它們是什麼以及執行哪些功能？	所有基於互聯網的流量輸入/輸出 AWS 透過我們的內部部署 Proxy 服務進行路由。
在可用區域和地區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料。	熱待機。在成功率持續下降期間自動容錯移轉至 US WEST -2。

工作負載入職問卷- AWS 服務事件問題

AWS 服務事件問題

問題	回應範例
提供貴公司內部重大事件/IT 危機管理團隊的聯絡資料（姓名/電子郵件/電話）。	重大事故管理團隊 mim@example.com +61 2 3456 7890
提供貴公司所建立之任何靜態事件/危機管理橋樑的詳細資料。如果您使用非靜態橋接器，請指定您喜歡的應用程序和 AWS 將在事件發生期間要求這些詳細資料。 **Note** 如果沒有提供，那麼 AWS 將在事件發生時伸出援手，並提供一個 Chime 橋供您加入。	Amazon Chime https://chime.aws/1234567890

警報擷取問卷

手冊問題

問題	回應範例
AWS 將透過 AWS Support 案例。觸發此工作負載警示時，主要連絡人是誰？ 指定您偏好的會議應用程式， AWS 將在事件發生期間要求這些詳細資料。 Note 如果未提供偏好的會議應用程式，則 AWS 將在事件發生時伸出援手，並提供一個 Chime 橋供您加入。	應用團隊 app@example.com +61 2 3456 7890
如果在事件發生期間無法使用主要聯絡人，請依照偏好的通訊順序提供問題上報連絡人和時間表。	1. 10 分鐘後，如果主要聯絡人沒有回應，請參與： 約翰·史密斯-應用主管 john.smith@example.com +61 2 3456 7890 2. 10 分鐘後，如果約翰·史密斯沒有回應，請聯繫： 簡·史密斯-運營經理 jane.smith@example.com +61 2 3456 7890
AWS 在整個事件中，定期通過支持案例傳達更新。是否有其他聯絡人應該收到這些更新？	john.smith@example.com, jane.smith@example.com

報警矩陣

報警矩陣

提供下列資訊，以識別將參與AWS事件偵測與回應的警示集，以代表您的工作負載建立事件。一旦AWS事件偵測與回應的工程師審核了您的警示，就會提供額外的上線步驟。

AWS事件偵測與回應關鍵警示標準：

- AWS事件偵測和回應警示只有在需要操作員立即注意的受監控工作負載 (收入損失/客戶體驗降級) 產生重大業務影響時，才應進入「警示」狀態。
- AWS事件偵測和回應警示也必須同時或在參與之前使用您的工作負載解析器。 AWS 事件管理員在緩解過程中與您的解析器協作，並且不會擔任隨後升級給您的第一線響應人員。
- AWS事件偵測和回應警示閾值必須設定為適當的臨界值和持續時間，以便在警示觸發調查時，任何時候都必須發生。如果警報在「警報」和「正常」狀態之間移動，則會產生足夠的影響以保證駕駛員的回應和注意力。

AWS違反條件的事件偵測與回應政策：

這些標準只能在事件發生時進行評估。 case-by-case 事件管理團隊會與您的技術客戶經理 (TAMs) 合作調整警示，在極少數情況下，如果懷疑客戶警示不符合此條件，而且正以不必要的速率與事件管理團隊合作，則會停用監控功能。

> **Important**
>
> 提供連絡人地址時，請提供群組分發電子郵件地址，以便您可以控制收件者新增和刪除，而不需要 runbook 更新。
> 如果您希望AWS事件檢測和響應團隊在發送初始參與電子郵件後致電給他們，請提供站點可靠性工程團隊的聯繫電話號碼（SRE）。

報警矩陣表

測量結果名稱/ARN/臨界值	描述	備註	要求的動作
工作量/ *CW Alarm ARN* /	此測量結果代表在「Application Load Balancer 衝器」層次	警報在上週已進入 10 次「警報」狀態。此	傳送電子郵件至網站可靠性工程團隊 *SRE@xyz.com*

測量結果名稱/ARN/臨界值	描述	備註	要求的動作
CallCount 5 分鐘內有 5 個資料點 <100000，將遺失的資料視為遺失	測量到工作負載的內送要求數目。 此警示非常重要，因為傳入要求的大幅下降可能表示上游網路連線有問題，或是DNS導致使用者無法存取工作負載的實作問題。	警報有誤報的風險。臨界值審查計劃。 問題？「否」或「是」(如果是「否」，則保留空白)：此警示會在特定批次工作執行期間頻繁翻轉。 解析器：網站可靠性工程師	為我ELB們和 Route 53 服務建立AWS頂級 Support 案例。 如果需要IMMEDIATE採取行動：檢查EC2釋放內存/磁盤空間並通知 *XYZ* 通過電子郵件團隊重新啟動實例，或運行日誌刷新。（如果不需要立即採取行動，請留空）
工作負載請求延遲/ *CW Alarm ARN* / p90 5 個資料點在 5 分鐘內延遲大於 100 毫秒，將遺失的資料視為遺失	此指標代表工作負載要滿足之HTTP要求的 p90 延遲。 此警報代表延遲（網站客戶體驗的重要衡量標準）。	警報在上週已進入「警報」狀態 0 次。 問題？「否」或「是」(如果是「否」，則保留空白)：此警示會在特定批次工作執行期間頻繁翻轉。 解析器：網站可靠性工程師	傳送電子郵件至網站可靠性工程團隊 *SRE@xyz.com* 為我ECW們和RDS服務建立AWS頂級 Support 案例。 如果需要IMMEDIATE採取行動：檢查EC2釋放內存/磁盤空間並通知 *XYZ* 通過電子郵件團隊重新啟動實例，或運行日誌刷新。（如果不需要立即採取行動，請留空）

測量結果名稱/ARN/臨界值	描述	備註	要求的動作
可用工作負載請求/ *CW Alarm 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。	此測量結果代表工作負載要滿足之HTTP要求的可用性。每個期間 (HTTP200 個/要求數目)。 此警示代表工作負載的可用性。	警報在上週已進入「警報」狀態 0 次。 問題？「否」或「是」(如果是「否」，則保留空白)：此警示會在特定批次工作執行期間頻繁翻轉。 解析器：網站可靠性工程師	傳送電子郵件至網站可靠性工程團隊 *SRE@xyz.com* 為我ELB們和 Route 53 服務建立AWS頂級 Support 案例。 如果需要IMMEDIATE採取行動：檢查EC2釋放內存/磁盤空間並通知 *XYZ* 通過電子郵件團隊重新啟動實例，或運行日誌刷新。（如果不需要立即採取行動，請留空）
新的遺物警報示例			

測量結果名稱/ARN/臨界值	描述	備註	要求的動作
端對端整合測試/ *CW Alarm ARN* / 3 分鐘持續時間內 1 分鐘指標的失敗率為 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:美國 EAST -1，AWS帳戶識別碼：012345678910	此測量結果會測試要求是否可以遍歷工作負載的每一層。如果此測試失敗，則表示處理業務交易的嚴重失敗。 此警示代表處理工作負載之商業交易的能力。	警報在上週已進入「警報」狀態 0 次。 問題？「否」或「是」(如果是「否」，則保留空白)：此警示會在特定批次工作執行期間頻繁翻轉。 解析器：網站可靠性工程師	傳送電子郵件至網站可靠性工程團隊 *SRE@xyz.com* 為我ECS們和 DynamoDB 服務建立AWS頂級 Support 案例。 如果需要IMMEDIATE採取行動：檢查EC2釋放內存/磁盤空間並通知 *XYZ* 通過電子郵件團隊重新啟動實例，或運行日誌刷新。（如果不需要立即採取行動，請留空）

要求變更已登入的工作負載

若要要求變更已登入的工作負載，請完成以下步驟，以建立具有AWS事件偵測與回應的支援案例。

1. 前往 AWS Support 置中，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. 在類別中，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事故偵測與回應- *workload_name*
7. 輸入此變更的「摘要」。例如，輸入「此要求適用於變更已登入AWS事件偵測與回應的現有工作負載」。請務必在要求中包含下列資訊：

- 工作負載名稱：工作負載名稱。
- 帳戶 ID：ID1、ID2ID3、等等。
- 變更詳細資料：輸入要求變更的詳細資訊。

8. 在 [其他連絡人-選擇性] 區段中，輸入任何您想要接收關於此變更通訊的電子郵件IDs。

   以下是「其他連絡人-選項」區段的範例。

   > **Important**
   >
   > 無法在 [其他聯絡人-選用] 區段IDs中新增電子郵件，可能會延遲變更程序。

9. 選擇提交。

   提交變更請求後，您可以從組織新增其他電子郵件。若要新增電子郵件，請在案例詳細資料中選擇「回覆」，如下列範例所示：

   然後，將電子郵件添IDs加到其他聯繫人-可選部分。

   以下是「回覆」頁面的範例，顯示您可以在其中輸入其他電子郵件。

離開工作負載

若要從AWS事件偵測與回應離開工作負載，請為每個工作負載建立新的支援案例。建立支援案例時，請記住下列事項：

- 若要離開單一工作負載 AWS 帳戶中，從工作負載的帳戶或付款人帳戶建立支援案例。
- 離開跨越多個工作負載的步驟 AWS 帳戶，然後從付款人帳戶建立支援案例。在支援案例主體中，列出IDs要離線的所有帳戶。

> **Important**
>
> 如果您建立支援案例以從不正確的帳戶卸載工作負載，則在卸載工作負載之前，您可能會遇到延遲和要求提供其他資訊的情況。

要求離開工作負載

1. 前往 AWS Support 置中，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. 在類別中，選擇工作負載卸載。
5. 針對嚴重性，選擇一般指引。
6. 輸入此變更的「主旨」。例如：

   [離岸] 事AWS故偵測與回應- *workload_name*
7. 輸入此變更的「摘要」。例如，輸入「此要求用於卸載已登入AWS事件偵測與回應的現有工作負載」。請務必在要求中包含下列資訊：

   - 工作負載名稱：工作負載名稱。
   - 帳戶 ID：ID1、ID2ID3、等等。
   - 卸載原因：提供卸載工作負載的原因。
8. 在 [其他聯絡人-選擇性] 區段中，輸入您想要接收有關此登機要求之通訊的任何電子郵件IDs。
9. 選擇提交。

AWS 事件偵測與回應監控與觀察能力

AWS 事件偵測與回應可為您提供專家指導，協助您定義從應用程式層到基礎設施的工作負載的可觀察性。監視會告訴您出現問題。可觀測性使用數據收集來告訴您什麼是錯誤的以及發生的原因。

事件偵測與回應系統會利用 Amazon 和 Amazon 等原生 AWS 服務偵測可能影響工作 AWS 負載的事件，監控您的工作負載是否發生故障 CloudWatch 和效能降低。 EventBridge 監控可為您提供即將發生、持續、後退或潛在故障或效能降低的通知。當您將帳戶登入事件偵測與回應時，您可以選擇事件偵測與回應監控系統應監控帳戶中的哪些警示，並將這些警示與事件管理期間使用的應用程式和 Runbook 建立關聯。

事件偵測與回應使用 Amazon CloudWatch 和其他產品 AWS 服務 來建立您的可觀察性解決方案。AWS 事件偵測與回應可透過兩種方式協助您觀察：

- 業務成果指標：AWS 事件偵測和回應的觀察性從定義監控工作負載或終端使用者體驗結果的關鍵指標開始。 AWS 專家會與您合作，瞭解工作負載的目標、可能影響使用者體驗的關鍵輸出或因素，並定義可擷取這些關鍵指標中任何降級情況的指標和警示。例如，行動通話應用程式的主要商業指標是呼叫設定成功率 (監控使用者呼叫嘗試的成功率)，而網站的關鍵指標就是頁面速度。事件參與是根據業務成果指標觸發的。
- 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架構 AWS 服務 和基礎結構，並定義指標和警示，以追蹤這些基礎架構服務的效能。這些可能包括諸如 Application Load Balancer 執行個體`ApplicationLoadBalancerErrorCount`的指標。這會在已登入工作負載並設定監控之後啟動。

實作 AWS 事件偵測與回應的可觀察性

由於可觀測性是一個連續的程序，可能無法在一個練習或時間範圍內完成，因此 AWS 事件偵測和回應分兩個階段實作可觀察性：

- 入職階段：入職期間的可觀察性專注於偵測應用程式的業務成果何時受損。為此，在入職階段期間的可觀察性專注於在應用程式層定義關鍵業務成果指標，以通知您 AWS 的工作負載中斷。這種方式 AWS 可以及時響應這些中斷，並為您提供幫助恢復。
- 上線後階段：AWS 事件偵測和回應提供許多可觀察性的主動服務，包括定義基礎設施層級指標、指標調整，以及根據客戶的成熟度等級設定追蹤和日誌。這些服務的實施可能會持續數月，並涉及多個團隊。AWS 事件偵測與回應提供可觀察性設定的指導，客戶必須在其工作負載環境中實作必要的變更。如需實作觀察功能的協助，請向您的技術客戶經理 (TAM) 提出要求。

利用事件偵測與回應進行AWS事件管理

AWS事件偵測與回應可由指定的事件管理團隊提供 24 小時全年無休的主動監控與事件管理。

1. 警示產生：在工作負載上觸發的警示會透過 Amazon 推送 EventBridge 至AWS事件偵測與回應。AWS事件偵測與回應會自動提取與警示相關聯的 Runbook，並通知事件管理員。如果您的工作負載發生嚴重事件，而AWS事件偵測與回應所監控的警示未偵測到，您可以建立支援案例來要求事件回應。如需請求事件回應的詳細資訊，請參閱事件回應要求。
2. AWS 事件管理器參與度：事件管理器響應警報，並參與您在電話會議或在 runbook 中指定的其他方式。事件管理員會驗證 AWS 服務 確定警報是否與問題有關 AWS 服務 由工作負載使用，並就基礎服務的狀態提供建議。如果需要，事件管理員然後代表您創建案例並參與權利 AWS 專家的支持。

   因為AWS事件偵測與回應監控 AWS 服務 針對您的應用程式，AWS事件偵測與回應可能會判斷事件與 AWS 服務 甚至在一個問題之前 AWS 服務 事件被聲明。在這個案例中，事件管理員會建議您的狀態 AWS 服務，觸發 AWS 服務事件事件管理流程，並與服務團隊跟進解決方案。所提供的資訊讓您有機會儘早實作復原計畫或因應措施，以減輕復原計畫的影響 AWS 服務事件。如需詳細資訊，請參閱服務事件的事件管理。
3. 事件解決方案：事件管理器協調所需的事件 AWS 團隊，並確保你保持與正確的互動 AWS 專家，直到事件得到緩解或解決為止。
4. 事件後審查（如果要求）：事件發生後，AWS事件偵測和回應可根據您的要求執行事件後審查，並產生事件後報告。事件後報告包括問題的描述、影響、哪些團隊參與，以及緩解或解決事件所採取的因應措施或採取的行動。事件後報告可能包含的資訊可用於減少事件復發的可能性，或改善 future 發生類似事件的管理。事件後報告不是根本原因分析 (RCA)。除了事件後報告RCA之外，您還可以要求。下節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 Support 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 AWS Support support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and AWS Support 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 a 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 an 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 Support and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

為應用程式團隊佈建存取

AWS事件偵測與回應與您溝通 AWS Support 事件生命週期中的案例。若要與事件管理員對應，您的團隊必須擁有 AWS Support 中心。

如需有關佈建存取權的詳細資訊，請參閱管理 AWS Support 中心位於 AWS Support 用戶指南。

服務事件的事件管理

AWS事件偵測與回應會通知您持續發生的服務事件 AWS 區域，無論您的工作負載是否受到影響。在一個期間 AWS 服務事AWS件，事件檢測和響應創建 AWS Support 案例、加入電話會議橋接以接收影響力和情緒的意見反應，並提供在活動期間叫用復原計畫的指引。您也會透過以下方式收到通知 AWS Health 包含事件的詳細信息。不受影響的客戶 AWS 擁有的服務事件 (例如，在不同的操作 AWS 區域，請勿使用 AWS 受損的服務等）繼續得到標準參與的支持。如需關於 AWS Health，請參閱什麼是 AWS Health?.

服務事件後報告（如有要求）：如果服務事件導致事件發生事件，您可以要求「AWS事件偵測與回應」以執行事件後檢閱並產生「事件發生後報告」。服務事件的事件後報告包括以下內容：

- 問題的描述
- 事件的影響
- 共享的信息 AWS Health 儀表板
- 事件期間參與的團隊
- 緩解或解決事件所採取的因應措施和行動

服務事件的「事件後報告」可能包含可用於減少事件再次發生的可能性的資訊，或改善 future 發生類似事件的管理。服務事件的事件後報告不是根本原因分析 (RCA)。您可以針對服務RCA事件另外要求「事件後報告」。

以下是服務事件的事件後報告範例：

> **Note**
>
> 下列報告範本僅為範例。

```
Post Incident Report - LSE000123
Customer: Example Customer
AWS Support Case ID(s): 0000000000
Incident Start: Example: 1 January 2024, 3:30 PM UTC
Incident Resolved: Example: 1 January 2024, 3:30 PM UTC
Incident Duration: 1:02:00
Service(s) Impacted: Lists the impacted services such as EC2, ALB
Region(s): Lists the impacted AWS Regions, such as US-EAST-1
Alarm Identifiers: Lists any customer alarms that triggered during the Service Level
 Event

Problem Statement:
Outlines impact to end users and operational infrastructure impact during the Service
 Level Event.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a service outage...

Impact Summary for Service Level Event:
(This section is limited to approved messaging available on the AWS Health Dashboard)
Outline approved customer messaging as provided on the AWS Health Dashboard.
Between 1:14 PM and 4:33 PM UTC, we experienced increased error rates for the Amazon
 SNS Publish, Subscribe, Unsubscribe, Create Topic, and Delete Topic APIs in the EU-
WEST-1 Region. The issue has been resolved and the service is operating normally.

Incident Summary:
Summary of the incident in chronological order and steps taken by AWS Incident Managers
 during the Service Level Event to direct the incident to a path to mitigation.
At 2024-01-04T01:25:00 UTC, the workload alarm triggered a critical incident...
At 2024-01-04T01:27:00 UTC, customer was notified via case 000000000 about the
 triggered alarm
```

```
At 2024-01-04T01:30:00 UTC, IDR team identified an ongoing service event which was
 related to the customer triggered alarm
At 2024-01-04T01:32:00 UTC, IDR team sent an impact case correspondence requesting for
 the incident bridge details
At 2024-01-04T01:32:00 UTC, customer provided the incident bridge details
At 2024-01-04T01:32:00 UTC, IDR team joined the incident bridge and provided
 information about the ongoing service outage
By 2024-01-04T02:35:00 UTC, customer failed over to the secondary region (EU-WEST-1) to
 mitigate impact...
At 2024-01-04T03:27:00 UTC, customer confirmed recovery, the call was spun down...

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not an Root Cause Analysis
 (RCA).
Back-off and retries yielded mild recovery. Full mitigation happened ...

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 ...
Work with AWS Support and TAM team to ensure ...
```

事件回應要求

如果您的工作負載發生嚴重事件，而AWS事件偵測與回應所監控的警示未偵測到，您可以建立支援案例來要求事件回應。您可以針對已訂閱「事件偵測與回應」的任何工作負載 (包括上線程序中的工作負載) 要求AWS事件回應。

若要針對主動影響您工作負載的事件要求事件回應，請建立 AWS Support 案例。提出支援案例之後，AWS事件偵測和回應會讓您與 AWS 需要專家來加速您的工作負載復原。

使用要求事件回應 AWS Support Center Console

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. 在「類別」中選擇「作用中未預期
5. 在「嚴重性」中，選擇「關鍵業務系統」。

6. 輸入此事件的「主旨」。例如：

   AWS事件偵測與回應-主動式事件

7. 輸入此事件的「問題描述」。新增下列詳細資訊：

   - 技術資訊：

     受影響的服務：

     受影響的資源：

     受影響地區：

     工作負載名稱：

   - 商業資訊：

     對業務的影響說明：

     [選用] 客戶橋接器詳細資料：

8. 在「其他聯絡人」區段中，輸入您要接收與此事件相關通訊的任何電子郵件地址。

   下圖顯示主控台畫面，其中 [其他連絡人] 欄位已反白顯示。

9. 選擇提交。

   提交事件回應要求後，您可以從組織新增其他電子郵件地址。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「案例詳細資料」畫面，其中「回覆」按鈕會反白顯示。

   下圖顯示「其他連絡人」欄位和「提交」按鈕反白的案例「回覆」。

10AWS事件偵測與回應會在五分鐘內確認您的案件，並讓您參與適當的會議橋接 AWS 專家。

使用要求事件回應 AWS Support API

Support 案例可以透過程式設計方式建立 AWS Support API.

請求事件回應 AWS Support App in Slack

1. 打開您配置的 Slack 頻道 AWS Support App in Slack 在。
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「問題描述」。新增下列詳細資訊：

   技術資訊：

   受影響的服務：

   受影響的資源：

   受影響地區：

   工作負載名稱：

   商業資訊：

   對業務的影響說明：

   [選用] 客戶橋接器詳細資料：
5. 選擇 Next (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. 在「類別」中選擇「作用中未預期
9. 在「嚴重性」中，選擇「關鍵業務系統」。

10.在「聯絡方式」中，選擇「電子郵件和 Slack 通知」。

> **Note**
>
> AWS事件偵測與回應不支援 Slack 中的即時聊天功能。如果您選取此選項，您會發現事件回應要求的回應延遲。

11您可以設定您希望收到有關此事件之電子郵件通訊副本的其他聯絡人。

12選擇檢閱。

13只有您可以看到的新訊息會出現在 Slack 頻道中。檢閱案例詳細資料，然後選擇「建立案例」。

14您的案例 ID 會在新訊息中提供 AWS Support App in Slack.

15事件偵測與回應會在五分鐘內確認您的案件，並讓您參與適當的會議橋接 AWS 專家。

16事件偵測與回應的通訊會在案件的討論串中更新。

AWSSlack 中的 Support 應用

AWS 客戶可以使用 AWS Support App in Slack管理他們的 AWS Support 在鬆弛的情況下。

AWS 事件偵測與回應客戶可以使用 AWS Support App in Slack 接收有關其工作負載上新警示起始事件的通知，或建立事件回應要求。

若要設定 AWS Support App in Slack，請按照中提供的說明進行操作 AWS Support 使用者指南。

> **Important**
>
> - 當您更新或建立 Support 案例 AWS 事件偵測與回應 AWS Support App in Slack，您必須選擇電子郵件和 Slack 通知聯繫方式。
>
> AWS 事件偵測與回應僅支援支 Support 案例的電子郵件通訊。不支持實時聊天。
>
> - 若要確保您在 Slack 中收到工作負載上所有警示起始事件的通知，您必須設定 AWS Support App in Slack 針對已登入的所有工作負載帳戶 AWS 事件偵測與回應。Support 案例是在工作負載警示產生所在的帳戶中建立。
> - 在事件發生期間，您可以代表您開立多個高嚴重性 Support 案例以參與 AWS Support 解析器。您會在 Slack 中收到與 Slack 通道通知設定相符的事件期間開啟的所有支援案例的通知。
> - 您透過 AWS Support App in Slack 請勿取代透過電子郵件或電話參與的工作負載初始和上報聯絡人 AWS 事件發生期間的事件偵測與回應。

Slack 中的警報啟動事件通知

在 Slack Channel 中設定 Slack 中的 Sup AWS port 應用程式時，系統會通知您有關事AWS件偵測與回應監控工作負載的警示起始事件。

下列範例顯示警示發起事件的通知如何在 Slack 中顯示。

通知範例

當事件偵測與回應確認您的警報發起的AWS事件時，Slack 中會產生類似下列內容的通知：

若要檢視「AWS事件偵測與回應」新增的完整通訊，請選擇「查看詳細資訊」。

AWS事件偵測與回應的進一步更新會出現在案例的執行緒中。

選擇「查看詳細資訊」以檢視「AWS事件偵測與回應」新增的完整通訊。

Slack 中的事件回應要求

如需如何透過 Slack 中的 Sup AWS port 應用程式建立事件回應要求的指示，請參閱事件回應要求。

AWS 事件偵測與回應報告

事件偵測與回應提供營運與效能資料，協助您瞭解服務的設定方式、事件歷史記錄，以及事件偵測與回應服務的效能。

組態資料

- 已登入的所有帳戶
- 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

- 每宗申請的事故發生的日期、數目及持續時間
- 與特定警示相關聯的事件日期、數目和持續時間
- 事件後報告

效能資料

- 服務等級目標 (SLO) 效能

請聯絡我們的技術客戶經理，以取得您可能需要的營運和績效資料。

事件偵測與回應安全性與復原

AWS 共用責任模型適用於中的資料保護 AWS Support。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。此內容包括您使用的安全性組態和管理工作。 AWS 服務

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。

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶登入資料，並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) 憑證與資源通訊。 AWS 建議使用 TLS 1.2 或更新版本。如需詳細資訊，請參閱什麼是 SSL/TLS 憑證？ 。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。如需相關資訊，請參閱AWS CloudTrail。
- 使用 AWS 加密解決方案，以及 AWS 服務中的所有預設安全性控制。如需詳細資訊，請參閱AWS 密碼編譯服務和工具。
- 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。有關 Amazon Macie 的信息，請參閱 Amazon Mac ie。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需可用 FIPS 端點的相關資訊，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。這包括當您使用主控台、API、 AWS CLI AWS Support 或 AWS SDK 時使用或其他 AWS 服務 使用時。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 事件偵測與回應存取您的帳戶

AWS Identity and Access Management (IAM) 是可協助您安全地控制 AWS 資源存取的 Web 服務。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 事件偵測與回應以及您的警示資料

根據預設，事件偵測和回應會接收您帳戶中每個 CloudWatch 警示的 Amazon 資源名稱 (ARN) 和狀態，然後在登入的警示變更為警示狀態時啟動事件偵測和回應程序。如果您想要自訂事件偵測和回應從您的帳戶收到的警示資訊，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指南以來，文件的重要變更。

- 最新文件更新：2024 年 6 月 12 日

變更	描述	日期
增加了一個新的頁面 AWS Support App in Slack 利用事件偵測與回應的更新 AWS事件管理	增加了一個新的頁面 AWS Support App in Slack 已更新事件管理，包含AWS事件偵測與回應功能，新增「請求事件回應 AWS Support App in Slack".	2024年9月10日
更新帳戶訂閱	已更新「帳戶訂閱」區段，以包含當您要求訂閱帳戶時如何開立支援案例的詳細資訊。 更新部分：帳戶訂閱	2024年6月12日
服務事件的事件後報告現已推出	已更新服務事件的事件管理區段，以包含服務事件之事件發生事件後報告的相關資訊。 更新部分：服務事件的事件管理	2024年5月8日
新增區段：離開工作負載	在入門中新增卸載工作負載區段，以包含有關卸載工作負載的資訊 如需詳細資訊，請參閱離開工作負載。	2024年3月28日
更新帳戶訂閱	更新了帳戶訂閱部分，以包含有關卸載工作負載的資訊 如需詳細資訊，請參閱帳戶訂閱	2024年3月28日
更新的測試	更新了「測試」部分，以包含有關遊戲日測試的信息，這是入職過程的最後一步。 更新部分：測試已登入的工作負載	2024 年 2 月 29 日

變更	描述	日期
更新什麼是AWS事件偵測與回應	更新什麼是AWS事件偵測與回應區段。 更新部分：什麼是 AWS 事件偵測與回應？	2024年2月19日
更新問卷部分	更新了工作負載上線問卷，並新增警報擷取問卷。將「入職問卷」區段重新命名為「工作負載上線」和「警示擷取問卷」。 更新部分：工作負載上線和警示擷取問卷	2024年2月2日
Updated AWS 服務事件和入職資訊	更新了數個章節，其中包含新的入職資訊。 更新的部分： • 服務事件的事件管理 • 工作量探查 • 入職 • 帳戶訂閱 新章節 • 為應用程式團隊佈建存取	2024 年 1 月 31 日
新增相關資訊區段	在存取佈建中新增相關資訊區段。 更新部分：針對事件偵測與回應提供警示擷取的存取權	2024年1月17日
更新的示例步驟	更新範例中步驟 2,3 和 4 的程序：整合來自 Datadog 和 Splunk 的通知。 更新部分：範例：整合來自資料多和 Splunk 的通知	2023 年 12 月 21 日

變更	描述	日期
更新了介紹圖文和文字	在嵌入警報中APMs更新了與 Amazon EventBridge 直接整合的圖形。 更新部分：開發AWS事件偵測與回應的手冊	2023 年 12 月 21 日
更新的手冊模板	更新開發AWS事件偵測與回應的手冊中的 runbook 範本。 更新部分：開發AWS事件偵測與回應的手冊	2023 年 12 月 4 日
更新的警報配置	更新了警報配置，包含 CloudWatch 警報配置的詳細信息。 新區段：在事件偵測與回應中建立符合您業務需求的 CloudWatch 警報 新區段：使用 AWS CloudFormation 在事件偵測與回應中建立 CloudWatch 警示的範本 新區段：事件偵測與回應中的 CloudWatch 警示使用案例範例	2023 年 9 月 28 日
更新開始使用	已使用工作負載變更要求的相關資訊更新入門。 新區段：要求變更已登入的工作負載 更新部分：帳戶訂閱	2023年9月05日
開始使用中的新章節	新增將警將警示擷取至AWS事件偵測與回應示導入AWS事件偵測與回應。	2023 年六月三十日
原始文件	AWS事件偵測與回應首次發佈	2023 年三月十五日

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的AWS 詞彙表。

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。