aws

使用者指南

Incident Manager

Incident Manager: 使用者指南

Table of Contents

什麼是 AWS Systems Manager Incident Manager？

事件管理員是一項功能AWS Systems Manager，可協助您減輕影響託管應用程式的事件，並從中復原AWS。

在的背景下AWS，事件是任何意外中斷或服務質量降低，可能會對業務運營產生重大影響。因此，對於組織而言，建立回應策略以有效減輕事件並從事件中復原，並實作防止 future 發生事件的動作至關重要。

事件管理員透過下列方式協助縮短解決事件的時間：

- 提供自動化計劃，以有效地吸引負責響應事件的人員。
- 提供相關疑難排解資料。
- 使用預先定義的自動化手冊啟用自動回應動作。
- 提供與所有利益相關者合作和溝通的方法。

事件管理員內建的功能和工作流程是以事件回應的最佳實務為基礎，Amazon 自成立以來幾乎一直在開發這些事件回應。事件管理器AWS 服務與 Amazon CloudWatchAWS CloudTrail，AWS Systems Manager和 Amazon 等集成 EventBridge。

主要元件和功能

本節說明事件管理員中用來設定事件回應計劃的功能。

回應計劃

回應計劃可做為範本，定義事件發生時必須到位的項目。它包括以下信息：

- 發生事件時需要誰做出回應。
- 已建立的自動化回應，以減輕事件。
- 回應者必須使用的協同作業工具來溝通及接收有關事件的自動通知。

事件偵測

您可以設定 Amazon CloudWatch 警示和 Amazon EventBridge 事件，以在偵測到影響AWS資源的條件或變更時建立事件。

手冊自動化支持

您可以從事件管理員內部啟動自動化工作流程手冊，以自動化您對事件的重要回應，並向第一線應變人員提供詳細步驟。

參與和升級

參與計劃指定每個人都要通知每個獨特的事件。您可以指定已新增至「事件管理員」的個別連絡人，或指定在「事件管理員」中建立的隨叫排程。參與計劃還指定了升級途徑，以幫助確保利益相關者之間的可見性和在事件響應過程中積極參與。

待命時間表

「事件管理員」中的隨叫排程包含您為排程建立的一或多個旋轉。對於每個旋轉，您最多可以包含 30 個接觸。當新增至升級計劃或回應計劃時，隨時待命排程會定義在發生需要回應者介入的事件發生時，誰會收到通知。隨時待命排程有助於確保您在事件回應所需時獲得全天候、備援的全天候保障。

積極協作

事件應變人員透過與AWS Chatbot客戶整合，積極回應事件。 AWS Chatbot支援為使用 Slack、Microsoft Teams或 Amazon Chime 的事件管理員建立聊天管道。回應者可以直接彼此通訊、接收有關事件的自動通知，以Slack及Microsoft Teams直接執行某些事件管理員命令列介面 (CLI) 作業。

事故診斷

回應者可在事件發生期間，在「事件管理員」主控台中檢視 up-to-date 資訊。根據資訊中的變更，回應者接著可以建立後續項目，並使用自動化工作流程手冊來修復這些項目。

其他服務的發現

若要支援回應事件診斷，您可以啟用「事件管理員」中的「發現項目」功能。發現項目是關於發生事件時發生的AWS CodeDeploy部署和AWS CloudFormation堆疊更新，以及涉及可能與事件相關的一或多個資源的相關資訊。擁有此資訊可減少評估潛在原因所需的時間，從而縮短事件復原 (MTTR) 的平均時間。

事件後分析

事件解決後，您可以使用事件後分析來識別事件回應的改善情況，包括偵測和緩解時間。分析還可以幫助您了解事件的根本原因。事件管理員會建立建議的後續行動項目，讓您用來改善事件回應。

使用事件管理器的好處

瞭解在事件偵測和回應作業中使用事件管理員的好處。

本節說明您的組織在實作「事件管理員」回應計劃時可獲得的優勢。

立即有效率地診斷問題

當您的服務 EventBridge 發生任何意外中斷或降低時，您設定的 Amazon CloudWatch 警示和 Amazon 事件可以自動建立事件。

CloudWatch 警示會偵測並報告量度或運算式的值在數個期間內相對於臨界值的變更時。 EventBridge 事件是由於您在 EventBridge 規則中指定的環境、應用程式或服務發生變更而建立的。當您建立警示或事件時，您可以針對要在事件管理員中建立的事件指定動作，並指定適當的回應計劃，以促進事件的參與、升級和緩解。

事件管理員提供了通過使用指標自動收集和跟踪與事件相關的 CloudWatch 指標的能力。除了透過 CloudWatch 警示建立事件時為事件產生的自動化指標之外，您還可以即時手動新增指標，為事件中的回應者提供額外的內容和資料。

使用「事件管理員」事件時間表，依時間順序顯示興趣點。回應者也可以使用時間軸來新增自訂事件，以說明他們所做的事或發生了什麼事。自動化興趣點包括：

- CloudWatch 警示或 EventBridge 規則會建立事件。
- 事件指標會報告給事件管理員。
- 響應者正在參與。
- 手冊步驟已成功完成。

有效地參與

事件管理器通過使用聯繫人，隨時調度，升級計劃和聊天渠道將事件響應人員聚集在一起。您可以直接在事件管理員中定義個別聯絡人，並指定聯絡人喜好設定（電子郵件、簡訊或語音）。您可以將聯絡人新增至隨叫的排程輪換，以決定在指定期間內處理事件的人員。使用您定義的聯繫人和隨時待命的時間表，您可以創建升級計劃，以在事件發生期間在正確的時間吸引必要的響應者。

即時協同合作

事件期間的溝通是更快解決問題的關鍵。使用設定為使用Slack、Microsoft Teams或 Amazon Chime 的用AWS Chatbot戶端，您可以在他們偏好的連線聊天頻道中將回應者聚集在一起，讓他們直接與事件互動。事件管理員還可以在聊天頻道中顯示事件響應人員的實時操作，為其他人提供背景信息。

自動化服務恢復

事件管理員可讓您的回應人員透過使用自動化手冊，專注於解決事件所需的關鍵工作。在事件管理員中，Runbook 是為了解決事件而採取的一系列預先定義的動作。它們將自動化工作的強大功能與必要時的手動步驟相結合，讓回應者更容易分析和回應影響。

預防 future 的事件

使用事件管理員事件後分析，您的團隊可以制定更健全的回應計劃，並在整個應用程式中影響變更，以防止 future 的事件和停機時間 事件後分析還提供了迭代學習和改進手冊，響應計劃和指標。

相關服務

事件管理員與其他AWS 服務多種第三方服務和工具整合，可協助您偵測並解決事件，並間接與 API 作業互動，以及管理基礎架構。如需相關資訊，請參閱 與事件管理器的產品和服務整合。

存取事件管理員

您可以使用下列任何一種方式存取「事件管理員」：

- 事件管理員主控台
- AWS CLI-如需一般資訊，請參閱《使用指南》中的〈〉AWS CLI中的〈AWS Command Line Interface使用〉。如需事件管理員之 CLI 命令的相關資訊，請參閱《AWS CLI命令參考》ssm-contacts中的ssm-incidents和。
- 事件管理器 API — 如需詳細資訊，請參閱 AWS Systems Manager Incident ManagerAPI 參考資料。
- AWSSDK — 如需詳細資訊，請參閱要建置的工具。AWS

事件管理員區域和配額

系統管理員並不支AWS 區域援所有事件 Systems Manager。

若要檢視事件管理員區域和配額的相AWS Systems Manager Incident Manager關資訊，請參閱 Amazon Web Services 一般參考.

事件管理員的定價

使用事件管理員需要支付費用。如需詳細資訊，請參閱 AWSSystems Manager 定價。

> **Note**
>
> 與本服務相關的其他AWS 服務、AWS內容和第三方內容可能需另外收費，並受其他條款約束。

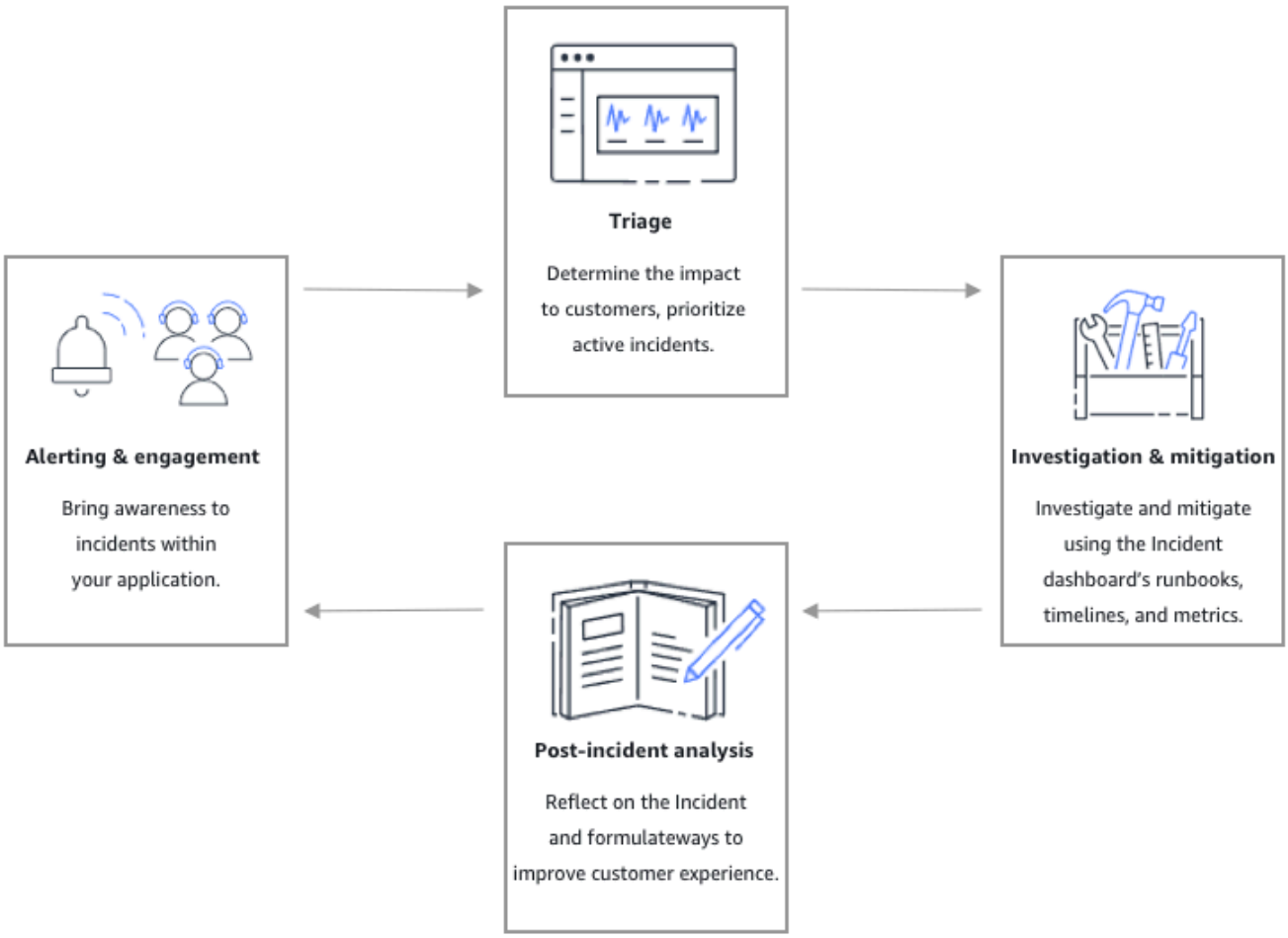
如需協助您最佳化AWS環境成本、安全性和效能的服務概觀，請參閱《AWS Support使用者指南》AWS Trusted Advisor中的。Trusted Advisor

事件管理員中的事件生命週期

AWS Systems Manager Incident Manager提供基於最佳實踐的 step-by-step 框架，以識別事件並對其做出反應，例如服務中斷或安全威脅。事件管理員的主要重點是透過完整的事件生命週期管理解決方案，協助將受影響的服務或應用程式盡快恢復正常狀態。

事件管理員為事件生命週期的每個階段提供工具和最佳實務：

- 警示和參與
- 分類
- 調查和緩解
- 事件後分析



警示和參與

事件生命週期的警示和參與階段著重於提高應用程式和服務中的事件意識。這個階段在偵測到事件之前就開始，需要深入瞭解您的應用程式。您可以使用 Amazon CloudWatch 指標監控應用程式效能的相關資料，或利用 Amazon 彙總 EventBridge來自不同來源、應用程式和服務的提醒。在您為應用程式設定監視之後，您可以開始對超出歷史規範的指標發出警示。若要深入瞭解監視最佳做法，請參閱監控。

若要支援回應事件診斷，您可以啟用「事件管理員」中的「發現項目」功能。發現項目是在事件發生時發生的AWS CodeDeploy部署和AWS CloudFormation堆疊更新的相關資訊。擁有此資訊可減少評估潛在原因所需的時間，從而縮短事件復原 (MTTR) 的平均時間。

現在您正在監控應用程式中的事件，您可以定義事件回應計劃，以便在事件期間使用。若要進一步瞭解如何建立回應計劃，請參閱在事件管理員中使用回應計劃。Amazon EventBridge 事件或 CloudWatch

警報可以使用回應計劃做為範本，自動建立事件。若要深入瞭解事件建立，請參閱在事件管理員中建立事件。

應變計劃推出相關的升級計劃和參與計劃，以將急救人員引入事件中。有關如何設置升級計劃的更多內容，敬請參閱建立升級計劃。同時，使用聊天管道AWS Chatbot通知回應者，將他們導向事件詳細資料頁面。團隊可以使用聊天管道和事件詳細資料來溝通和分類事件。如需在事件管理員中設定聊天頻道的詳細資訊，請參閱任務 2：建立聊天頻道AWS Chatbot。

分類

分類是當第一響應者試圖確定對客戶的影響。事件管理員主控台中的事件詳細資料檢視可為回應者提供時間表和指標，以協助他們評估事件。評估事件的影響也為事件的回應時間、解決方案和溝通奠定了基礎。回應者使用 1 (嚴重) 到 5 (無影響) 的影響等級，排定事件的優先順序。

您的組織可以根據您的選擇定義每個影響評級的確切範圍。下表提供通常如何定義每個影響等級的範例。

影響代碼	影響名稱	範例定義範圍
1	Critical	影響大多數客戶的完整應用程式故障。
2	High	影響客戶子集的完整應用程式失敗。
3	Medium	對客戶造成影響的部分應用程式失敗。
4	Low	對客戶影響有限的間歇性故障。
5	No Impact	客戶目前沒有受到影響，但需要採取緊急行動以避免影響。

調查和緩解

事件詳細資料檢視可為您的團隊提供工作流程、時間表和指標。若要瞭解如何處理事件，請參閱事件詳情。

Runbook 通常會提供調查步驟，並且可以自動提取資料或嘗試常用的解決方案。Runbook 還提供了清晰，可重複的步驟，您的團隊已經發現是有用的緩解事件。runbook 選項卡側重於當前 runbook 步驟，並顯示過去和 future 的步驟。

事件管理器與 Systems Manager 自動化集成以構建手冊。使用工作手冊執行下列任一項作業：

- 管理執行個體和AWS資源
- 自動執行指令碼
- 管理AWS CloudFormation資源

如需有關支援動作類型的詳細資訊，請參閱《AWS Systems Manager使用者指南》中的 Systems Manager 自動化動作參考。

「時間軸」標籤會顯示已採取的動作。時間軸記錄每個時間戳記和自動創建的詳細信息。若要將自訂事件新增至時間表，請參時間表閱本使用手冊之「事件詳細資料」頁面中的章節。

診斷索引標籤會顯示自動填入的量度和手動新增的量度。此檢視可為您的應用程式在事件期間的活動提供有價值的資訊。

「參與」標籤可讓您在事件中新增其他聯絡人，並協助提供參與聯絡人的資源，以便在涉及事件後迅速上手。通過定義的升級計劃或個人參與計劃進行聯繫。

使用聊天管道，您可以直接與您的事件和團隊中的其他回應者互動。使用AWS Chatbot，您可以在中配置聊天頻道。 Slack、Microsoft Teams、和 Amazon Chime 聲。在Slack和Microsoft Teams頻道中，回應者可以使用許多`ssm-incidents`指令直接從聊天頻道與事件互動。如需詳細資訊，請參閱透過聊天頻道進行互動。

事件後分析

事件管理器提供了一個框架，用於反思事件，採取必要的步驟，以防止事件在 future 再次發生，並改善整體事件響應活動。改進可能包括：

- 事件涉及的應用程式的變更。您的團隊可以利用這段時間來改善系統並使其更具容錯能力。
- 事件回應計劃的變更。花時間把學到的經驗教訓.
- 工作手冊的變更。您的團隊可以深入探討解決方案所需的步驟，以及您可以自動執行的步驟。
- 警示的變更。事件發生後，您的團隊可能已經注意到您可以用來提醒團隊有關事件的指標中的關鍵點。

事件管理器通過在事件時間表旁邊使用一組事件後分析問題和行動項目來促進這些潛在的改進。若要進一步瞭解透過分析改善，請參閱在事件管理員中執行事件後分析。

設定 AWS 系統管理員事件管理員

我們建議您在用來管理作業的帳戶中設定 AWS 系統管理員事件管理員。第一次使用「事件管理員」之前，請先完成下列工作：

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

授與程式設計存取權

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參

哪個使用者需要程式設計存取權？	到	By
		考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

事件管理員設定所需的角色

開始之前，您的帳戶必須具有 IAM 許可`iam:CreateServiceLinkedRole`。事件管理員會使用此權限`AWSServiceRoleforIncidentManager`在您的帳戶中建立。如需更多詳細資訊，請參閱 針對事件管理員使用服務連結角色。

開始使用事件管理員

本節逐步說明「事件管理員」主控台中的「準備工作」。您必須先完成「在主控台中做好準備」，才能將其用於事件管理。精靈會逐步引導您設定複製組、至少一位連絡人和一個上報計劃，以及您的第一個回應計劃。以下指南將幫助您了解事件管理器和事件生命週期：

- 什麼是 AWS Systems Manager Incident Manager？
- 事件管理員中的事件生命週期

必要條件

如果您是第一次使用事件管理員，請參閱設定 AWS 系統管理員事件管理員. 我們建議您在用來管理作業的帳戶中設定事件管理員。

我們建議您先完成「Systems Manager」快速設定，然後再開始「事件管理員」準備精靈。使用 Systems Manager 快速設定，以建議的最佳做法來設定常用的AWS服務和功能。事件管理員使用 Systems Manager 功能來管理與您相關的事件，以AWS 帳戶及先設定 Systems Manager 所帶來的好處。

準備精靈

第一次使用事件管理員時，您可以從「事件管理員」服務首頁存取「準備就緒」精靈。若要在第一次完成設定之後存取 [準備好] 精靈，請選擇 [事件] 清單頁面上的 [準備]。

1. 開啟「事件管理員」主控台。
2. 在「事件管理員」服務首頁上，選擇「做好準備」。

一般設定

1. 在 [一般設定] 下，選擇 [設定]。
2. 閱讀條款和條件。如果您同意事件管理員的條款與條件，請選取 [我已閱讀並同意事件管理員條款與條件]，然後選擇 [下一步]。
3. 在 [區域] 區域中，您的目前區域AWS 區域會顯示為複製組中的第一個區域。若要將更多區域新增至您的複製組，請從 [區域] 清單中選擇它們。

我們建議至少包括兩個區域。如果某個「區域」暫時無法使用，則事件相關活動仍可路由至另一個「區域」。

> **Note**
>
> 建立複製組會在您的帳戶中建立AWSServiceRoleforIncidentManager服務連結角色。若要進一步瞭解此角色，請參閱針對事件管理員使用服務連結角色。

4. 若要為複製組設定加密，請執行下列其中一個動作：

> **Note**
>
> 所有事件管理員資源都經過加密。若要進一步瞭解資料加密方式，請參閱事件管理員中的資料保護。如需有關「事件管理員」複製組的詳細資訊，請參閱使用事件管理員複製組。

- 若要使用AWS擁有的金鑰，請選擇 [使用AWS擁有的金鑰]。
- 若要使用您自己的AWS KMS金鑰，請選擇 [選擇現有金鑰] AWS KMS key。針對您在步驟 3 中選取的每個區域，選擇AWS KMS金鑰，或輸入 AWS KMS Amazon 資源名稱 (ARN)。

> **Tip**
>
> 如果您沒有可用的項目AWS KMS key，請選擇 [建立] AWS KMS key。

5. (選擇性) 在「標籤」區域中，將一或多個標籤新增至複製組。標籤包括一個鍵和一個值（可選）。

   標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。如需詳細資訊，請參閱標記事件管理員中的資源。

6. (選擇性) 在「服務存取」區域中，若要啟動「發現項目」功能，請選擇為此帳戶中的發現項目建立服務角色核取方塊。

   發現項目是指在建立事件時發生的程式碼部署或基礎結構變更的相關資訊。發現可以作為事件的潛在原因進行檢查。有關這些潛在原因的資訊會新增至事件的「未預期事件」詳細資訊頁面。有了這些部署和變更的相關資訊，回應者不需要手動搜尋此資訊。

> **Tip**
>
> 若要檢視要建立之角色的相關資訊，請選擇 [檢視權限]。

7. 選擇建立。

   若要深入了解複製組和復原能力，請參閱韌性在 AWS Systems Manager Incident Manager。

聯絡人 (選擇性)

1. 選擇建立聯絡人。

   事件管理員在事件期間與聯繫人互動。如需連絡人的詳細資訊，請參閱在事件管理員中使用連絡人。

2. 在名稱中，輸入連絡人的名稱。
3. 針對唯一別名，輸入識別此連絡人的別名。
4. 在「聯絡管道」區段中，執行下列動作以定義聯絡人在事件期間的參與方式：

   a. 在「類型」中選擇「電子郵件」、「簡訊」或「語音

   b. 在「頻道名稱」中，輸入唯一的名稱以協助您識別頻道。

   c. 在 [詳細資料] 中，輸入連絡人的電子郵件地址或電話號碼。

      電話號碼必須包+含 9—15 個字元，並以國家/地區代碼和訂戶號碼開頭。

   d. 若要建立其他聯絡人管道，請選擇 [新增聯絡人管道]。我們建議為每個接觸至少定義兩個管道。

5. 在 [參與計劃] 區域中，執行下列動作以定義要透過哪些通道通知連絡人，以及等待每個通道接收確認的時間長度。選取事件期間用來與聯絡人互動的聯絡管道。

   > **Note**
   >
   > 我們建議在參與計劃中至少定義兩個裝置。

   a. 在 [連絡人頻道名稱] 中，選擇您在 [連絡人管道] 區域中指定的頻道。

   b. 對於參與時間 (分鐘)，請輸入參與聯絡管道之前要等待的分鐘數。

我們建議您至少選取一個裝置，以便在互動開始時使用，指定 **0** (零) 分鐘等待時間。

c. 若要將更多聯絡人管道新增至參與計劃，請選擇 [新增互動]。

6. (選擇性) 在「標籤」區域中，新增一或多個標籤至連絡人。標籤包括一個鍵和一個值（可選）。

   標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。如需詳細資訊，請參閱標記事件管理員中的資源。

7. 若要建立聯絡人記錄並將啟用碼傳送至定義的聯絡人管道，請選擇「下一步」。

8. (選擇性) 在「聯絡管道啟動」頁面中，輸入傳送至每個管道的啟動碼。

   如果您現在無法輸入驗證碼，您可以稍後產生新的啟動碼。

9. 重複步驟 4，直到您已將所有聯絡人新增至「事件管理員」。

10. 輸入所有連絡人後，選擇 [完成]。

（可選）升級計劃

1. 選擇 [建立升級計劃]。

   升級計劃通過您的聯繫人在事件期間升級，以確保事件管理器在事件期間與正確的響應者互動。有關升級計劃的更多內容，敬請參閱在事件管理員中使用升級計劃。

2. 在 [名稱] 中，輸入提升計劃的唯一名稱。

3. 在別名中，輸入唯一的別名，以協助您識別提升計劃。

4. 在「階段 1」區域中，執行下列動作：

   a. 對於升級渠道，選擇要參與的聯繫渠道。

   b. 如果您希望聯絡人能夠中止提升計劃階段的進度，請選取確認停止計劃進展。

   c. 若要將更多頻道新增至階段，請選擇 [新增上報管道]。

5. 若要在提升計劃中建立新階段，請選擇 [新增階段] 並新增其階段詳細資訊。

6. (選擇性) 在 [標籤] 區域中，將一或多個標籤新增至上報計劃。標籤包括一個鍵和一個值（可選）。

   標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。如需詳細資訊，請參閱標記事件管理員中的資源。

7. 選擇 [建立升級計劃]。

反應計劃

1. 選擇 [建立回應計劃]。使用響應計劃將您創建的聯系人和升級計劃放在一起。在此 [開始使用] 精靈中，下列區段是選擇性的，特別是如果這是您第一次設定回應計劃時：

   - 聊天頻道
   - 手冊
   - 參與
   - 第三方整合

   如需有關將這些元素新增至回應計劃的資訊，請參閱事件管理員中的事件做好準備。
2. 在 [名稱] 中，輸入回應計劃的唯一可識別名稱。此名稱可用來建立回應計劃 ARN 或在沒有顯示名稱的回應計劃中建立。
3. (選擇性) 針對「顯示名稱」，輸入名稱，以協助您在建立事件時識別此回應計劃。
4. 在「標題」中，輸入標題，以協助識別與此回應計劃相關的事件類型。您指定的值會包含在每個事件的標題中。啟動事件的警示或事件也會新增至標題中。
5. 針對「影響」，選取您預期與此回應計劃相關之事件的影響等級，例如**Critical**或**Low**。
6. (選擇性) 在「摘要」中，輸入用來提供未預期事件概觀的簡短說明。事件管理員會在事件期間自動將相關資訊填入摘要中。
7. (選擇性) 在「刪除重複資料」字串中，輸入去除重複資料字串。事件管理員使用此字串來防止相同的根本原因在相同帳戶中建立多個事件。

   重複資料刪除字串是系統用來檢查重複事件的術語或片語。如果您指定重複資料刪除字串，「事件管理員」會在建立事件時，搜尋`dedupeString`欄位中包含相同字串的未決事件。如果偵測到重複的事件，「事件管理員」會將較新的事件刪除到現有的事件中。

   > **Note**
   >
   > 依預設，事件管理員會自動刪除由相同 Amazon CloudWatch 警示或 Amazon 事件所建立的多個 EventBridge 事件重複資料。您不需要輸入自己的重複資料刪除字串，即可防止這些資源類型重複。
8. (選擇性) 在「標籤」區域中，將一或多個標籤新增至回應計劃。標籤包括一個鍵和一個值（可選）。

標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。如需詳細資訊，請參閱標記事件管理員中的資源。

9. 從「參與」下拉式清單中選取要套用至事件的連絡人和升級計劃。
10. 選擇 [建立回應計劃]。

建立回應計劃後，您可以將 Amazon CloudWatch 警示或 Amazon EventBridge 事件與回應計劃建立關聯。這將根據警報或事件自動創建事件。如需詳細資訊，請參閱 在事件管理員中建立事件。

事件管理員中的跨區域和跨帳戶事件管理

您可以設定事件管理員 (的功能)AWS Systems Manager，以處理多個帳戶AWS 區域和帳戶。本節說明跨區域和跨帳戶的最佳做法、設定步驟以及已知的限制。

主題

跨區域事件管理

事件管理器支持自動和手動創建事件的幾個AWS 區域。當您最初使用 [準備就緒] 精靈使用事件管理員上線時，您最多可以AWS 區域為複製組指定三個。對於 Amazon CloudWatch 警示或 Amazon 事件自動建立的 EventBridge 事件，事件管理員會嘗試以事件規則或警示AWS 區域相同的方式建立事件。如果無法在中使用事件管理員AWS 區域， CloudWatch 或 EventBridge 將在複製組中指定的其中一個可用區域中自動建立事件。

> **Important**
>
> 請注意以下重要詳細資訊。
>
> - 我們建議您至少在複製組AWS 區域中指定兩個。如果您沒有指定至少兩個區域，系統將無法在事件管理員無法使用期間建立事件。
> - 跨區域容錯移轉所建立的事件不會叫用回應計畫中指定的 Runbook。

如需使用事件管理員入職及指定其他區域的詳細資訊，請參閱開始使用事件管理員。

跨帳戶事件管理

事件管理員使用 AWS Resource Access Manager (AWS RAM) 在管理和應用程式帳戶之間共用事件管理員資源。本節說明跨帳戶最佳做法、如何為事件管理員設定跨帳戶功能，以及事件管理員中跨帳戶功能的已知限制。

管理帳戶是您從中執行作業管理的帳戶。在組織設定中，管理帳戶擁有回應計劃、連絡人、升級計劃、執行手冊和其他AWS Systems Manager資源。

應用程式帳戶是擁有組成應用程式之資源的帳戶。這些資源可以是 Amazon EC2 執行個體、Amazon DynamoDB 表格，或是您用來在中建立應用程式的任何其他資源。AWS 雲端應用程式帳戶也擁有 Amazon CloudWatch 警示和 Amazon 事件，這些 EventBridge 事件會在事件管理器中建立事件。

AWS RAM使用資源共用率在帳號之間共用資源。您可以在中的帳號之間共用回應計劃和聯絡資源 AWS RAM。透過共用這些資源，應用程式帳戶和管理帳戶可以與互動和事件互動。共用回應計劃會共用使用該回應計劃建立的所有過去和 future 事件。共享聯繫人共享聯繫人或響應計劃的所有過去和 future 參與。

最佳實務

在不同帳戶之間共用事件管理員資源時，請遵循下列最佳做法

- 定期更新回應計畫和聯絡人的資源共用。
- 定期檢閱資源共用主體。
- 在您的管理帳戶中設定事件管理員、手冊和聊天頻道。

設定和設定跨帳戶事件管理

下列步驟說明如何設定和設定事件管理員資源，並將其用於跨帳戶功能。您過去可能已經為跨帳戶功能配置了一些服務和資源。使用跨帳戶資源開始您的第一個事件之前，請使用這些步驟作為需求檢查清單。

1. (選擇性) 使用建立組織和組織單位AWS Organizations。請遵循《使用指南》中〈教學課程：建立和配置組織AWS Organizations〉中的步驟。
2. (選擇性) 使用「Systems Manager 快速設定」功能來設定正確的AWS Identity and Access Management角色，供您在設定跨帳戶手冊時使用。如需詳細資訊，請參閱《使用指南》中的AWS Systems Manager〈快速設定〉。
3. 請依照AWS Systems Manager使用者指南中的多個執行自動化AWS 區域和帳戶中列出的步驟，在 Systems Manager 自動化文件中建立 Runbook。runbook 可以由管理帳戶或您的應用程式帳戶之一執行。根據您的使用案例，您需要為在事件期間建立和檢視 Runbook 所需的角色安裝適當的 AWS CloudFormation範本。
    - 在管理帳戶中執行工作流程簿。管理帳戶必須下載並安裝AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 範本。安裝時AWS-SystemsManager-AutomationReadOnlyRole，請指定所有應用程式帳戶的帳戶 ID。這個角色可讓您的應用程式帳戶從事件詳細資料頁面讀取 runbook 的狀態。應用程式帳戶必須安裝AWS-

SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 範本。事件詳細資料頁面會使用此角色從管理帳戶取得自動化狀態。

- 在應用程式帳戶中執行 Runbook。管理帳戶必須下載並安裝AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 範本。這個角色可讓管理帳戶讀取應用程式帳戶中 runbook 的狀態。應用程式帳戶必須下載並安裝AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 範本。安裝時AWS-SystemsManager-AutomationReadOnlyRole，請指定管理帳戶和其他應用程式帳戶的帳戶 ID。管理帳戶和其他應用程式帳戶會擔任此角色來讀取 runbook 的狀態。

4. (選擇性) 在組織中的每個應用程式帳戶中，下載並安裝AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation 範本。安裝時AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole，請指定管理帳戶的帳號 ID。此角色提供事件管理員存取AWS CodeDeploy部署和AWS CloudFormation堆疊更新相關資訊所需的權限。如果啟用「發現項目」功能，則會將此資訊報告為未預期事件的發現項目。如需詳細資訊，請參閱在事件管理員中使用發現項目。
5. 若要設定和建立聯絡人、升級計畫、聊天頻道和回應計劃，請遵循中詳述的步驟事件管理員中的事件做好準備。
6. 將您的聯絡人和回應計劃資源新增至您現有的資源共用或中的新資源共用AWS RAM。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的 AWS RAM 入門 新增回應計畫，AWS RAM讓應用程式帳戶能夠存取使用回應計劃建立的事件和事件儀表板。應用程式帳戶也可以將 CloudWatch 警示和 EventBridge 事件與回應計劃建立關聯。新增連絡人和升級計畫，AWS RAM讓應用程式帳戶能夠從事件儀表板檢視互動並與聯絡人互動。
7. 將跨帳戶跨區域功能新增至您的 CloudWatch 主控台。有關步驟和資訊，請參閱 Amazon CloudWatch 使用者指南中的跨帳戶跨區域 CloudWatch 主控台。新增此功能可確保您建立的應用程式帳戶和管理帳戶可以從事件和分析儀表板檢視和編輯指標。
8. 創建一個跨帳戶 Amazon EventBridge 事件總線。有關步驟和資訊，請參閱在AWS帳戶之間傳送和接收 Amazon EventBridge 事件。然後，您可以使用此事件匯流排建立事件規則，以偵測應用程式帳戶中的事件，並在管理帳戶中建立事件。

限制

以下是事件管理員跨帳戶功能的已知限制：

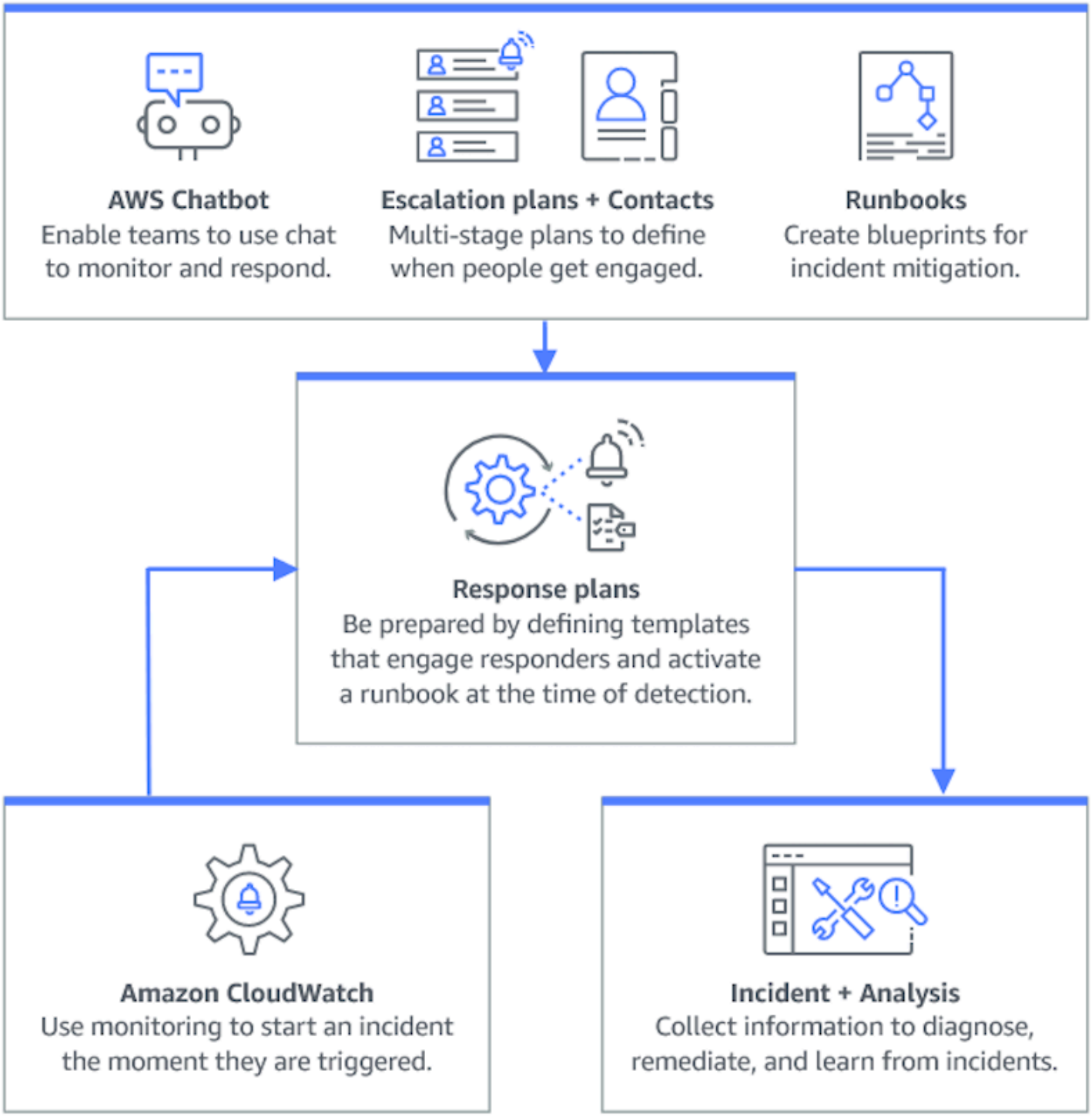
- 建立事件後分析的帳戶是唯一可以檢視和變更它的帳戶。如果您使用應用程式帳戶建立事件後分析，則只有該帳戶的成員可以檢視和變更它。如果您使用管理帳戶建立事件後分析，也是如此。

- 不會為在應用程式帳戶中執行的自動化文件填入時間軸事件。在應用程式帳戶中執行的自動化文件更新會顯示在事件的 Runbook 索引標籤中。

- Amazon 簡易通知服務主題無法跨帳戶使用。Amazon SNS 主題必須在與其使用的回應計劃相同的區域和帳戶中建立。我們建議您使用管理帳戶來建立所有 SNS 主題和回應計劃。
- 升級計劃只能使用同一帳戶中的聯絡人來建立。已與您分享的聯絡人無法新增至您帳戶中的升級計劃。
- 套用至回應計劃、事件記錄和連絡人的標籤只能從資源擁有者帳號檢視和修改。

事件管理員中的事件做好準備

事件的規劃早在事件生命週期之前就開始了。若要為事件做好準備，請在建立回應計劃之前考慮下列各個主題。使用監控、連絡人、升級計畫、聊天頻道和 Runbook 來建立自動化回應的回應計劃。



主題

監控

監控AWS託管應用程式的健康狀態是確保應用程式正常運作時間和效能的關鍵。決定監控解決方案時，請考慮下列事項：

- 功能重要性 — 如果系統故障，對下游使用者的影響會有多嚴重。
- 故障的共通性 — 系統故障的普遍程度；需要頻繁介入的系統應密切監控。
- 延遲時間增加 — 完成任務的時間增加或減少了多少。
- 用戶端與伺服器端度量 — 用戶端和伺服器上的相關指標之間存在差異。
- 依賴性失敗 — 您的團隊可以並且應該準備的失敗。

建立回應計劃後，您可以使用監控解決方案，在事件發生在環境中時自動追蹤事件。如需事件追蹤與建立的詳細資訊，請參閱追蹤事件管理員中的事件。

如需架構安全、高效能、彈性且有效率的基礎架構應用程式和工作負載的詳細資訊，請參閱 AWSWell-Architected 的白皮書。

使用一般設定

完成「事件管理員」上線精靈之後，您可以在「設定」頁面管理某些選項。這些選項包括複製組、套用至複製組的標籤，以及「發現項目」功能。

主題

使用事件管理員複製組

事件管理員複寫組可將您的資料複製AWS 區域到多個資料，以增加跨區域備援、讓事件管理員存取不同區域的資源，並減少使用者的延遲。複製組也可用來使用AWS 受管金鑰或您自己的客戶管理金鑰來加密您的資料。依預設，所有事件管理員資源都會加密。若要深入瞭解資源的加密方式，請參閱事件管理員中的資料保護。若要開始使用事件管理員，請先使用 [準備就緒] 精靈建立複寫組。若要深入了解如何在事件管理員中做好準備，請參閱準備精靈。

編輯複製組

您可以使用「事件管理員設定」頁面編輯複製組。您可以新增區域、刪除區域，以及啟用或停用複製組刪除保護。您無法編輯用於加密資料的金鑰。若要變更金鑰，請刪除並重新建立複製組。

新增區域

1. 開啟「事件管理員」主控台，然後選擇左側導覽窗格中的 [設定]。
2. 選擇「新增區域」。
3. 選取區域。
4. 選擇新增。

刪除區域

1. 開啟「事件管理員」主控台，然後選擇左側導覽窗格中的 [設定]。
2. 選取您要刪除的「區域」。
3. 選擇 刪除。
4. 在文字方塊中輸入刪除，然後選擇 [刪除]。

刪除複製組

刪除複製組中的最後一個區域會刪除整個複製組。刪除最後一個區域之前，請先切換 [設定] 頁面上的 [刪除保護]，以停用刪除保護。刪除複製組之後，您可以使用 [準備就緒] 精靈建立新的複製組。

若要從複製組刪除區域，請在建立區域後等候 24 小時。嘗試在建立後 24 小時內從複製組刪除「區域」會導致刪除失敗。

刪除複製組會刪除所有「事件管理員」資料。

刪除複製組

1. 開啟「事件管理員」主控台，然後選擇左側導覽窗格中的 [設定]。
2. 選取複製組中的最後一個區域。
3. 選擇 刪除。
4. 在文字方塊中輸入刪除，然後選擇 [刪除]。

管理複製組的標籤

標籤是您指派給資源的選用性中繼資料。使用標籤以不同的方式對資源進行分類，例如依目的、擁有者或環境。

管理複製組的標籤

1. 開啟「事件管理員」主控台，然後選擇左側導覽窗格中的 [設定]。
2. 在「標籤」區域中，選擇 「編輯」。
3. 若要新增標籤，請執行以下操作：
   a. 選擇 Add new tag (新增標籤)。
   b. 輸入標籤的索引鍵值和選擇性值。
   c. 選擇儲存。
4. 若要刪除標籤，請執行下列動作：
   a. 在您要刪除的標籤下方，選擇「移除」。
   b. 選擇儲存。

管理發現項目功能

「發現項目」功能可協助組織中的回應者在事件開始後立即識別事件的潛在根本原因。目前，事件管理員會針對AWS CodeDeploy部署和AWS CloudFormation堆疊更新提供發現項目。

對於發現項目的跨帳戶支援，啟用此功能之後，您必須在組織中的每個應用程式帳戶中完成額外的設定步驟。

若要使用此功能，您可以讓事件管理員建立服務角色，其中包含代表您存取資料的必要權限。

啟用「發現項目」功能

1. 開啟「事件管理員」主控台，然後選擇左側導覽窗格中的 [設定]。
2. 在「發現項目」區域中，選擇建立服務角色。
3. 複查要建立之服務角色的相關資訊，然後選擇 [建立]。

若要停用發現項目功能

若要停止使用「發現項目」功能，請從建立該`IncidentManagerIncidentAccessServiceRole`角色的每個帳號中刪除角色。

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在左側導覽窗格中，選擇 Roles (角色)。
3. 在搜尋方塊中，輸入 **`IncidentManagerIncidentAccessServiceRole`**。
4. 選擇角色的名稱，然後選擇 [刪除]。
5. 在對話方塊中輸入角色名稱以確認您要刪除角色，然後選擇 [刪除]。

在事件管理員中使用連絡人

AWS Systems Manager Incident Manager聯繫人是對事件的響應者。聯絡人可以有多種管道，事件管理員可以在事件發生期間參與。您可以定義聯繫人的參與計劃，以描述事件管理器如何以及何時與聯繫人互動。

主題

- 聯絡渠道
- 參與計劃
- 建立聯絡人
- 將聯絡人詳細資料匯入您的通訊錄

聯絡渠道

聯絡管道是事件管理員用來與聯絡人的各種方法。

事件管理員支援下列聯絡管道：

- 電子郵件
- 短訊服務
- 語音

聯繫渠道激活

為了保護你的隱私和安全，事件管理員會在你建立聯絡人時傳送裝置啟動碼給你。若要在事件發生期間與您的裝置互動，您必須先啟用它們。若要這麼做，請在建立聯絡人頁面上輸入裝置啟動碼。

事件管理員的某些功能包括傳送通知至聯絡人管道的功能。使用這些功能，即表示您同意此服務將有關服務中斷或其他事件的通知發送到指定工作流程中包含的聯繫渠道。這包括作為待命計劃輪替的一部分發送給聯繫人的通知。通知可以透過電子郵件、簡訊或語音通話傳送，如連絡人詳細資料中所指定。您可以使用這些功能來確認您已獲授權將您提供的聯絡管道新增至事件管理員。

選擇退出

您可以隨時取消這些通知，方法是將行動裝置移除為聯絡管道。個別通知收件者也可以隨時取消通知，方法是將裝置從其聯絡人中移除。

若要從連絡人移除聯絡人管道

1. 瀏覽至「事件管理員」主控台，然後從左側導覽列選擇「聯絡人」
2. 選取您要移除之聯絡人管道的連絡人，然後選擇 [編輯]。
3. 在您要移除的聯絡管道旁邊選擇 [移除]。
4. 選擇 Update (更新)。

停用連絡人管道

若要停用裝置，請回覆取消訂閱。回覆取消訂閱會阻止「事件管理員」連接你的裝置。

重新啟用聯絡管道

1. 回覆 「事件管理員」寄出的郵件 START。

2. 瀏覽至「事件管理員」主控台，然後從左側導覽列選擇「聯絡人」
3. 選取您要移除之聯絡人管道的連絡人，然後選擇 [編輯]。
4. 選擇「啟動裝置」。
5. 輸入事件管理員傳送至裝置的啟動碼。
6. 選擇 Activate (啟用)。

參與計劃

參與計劃定義事件管理器何時參與聯繫渠道。從參與開始起，您可以在不同階段多次與聯繫渠道互動。您可以在升級計劃或回應計劃中使用參與計劃。要了解有關升級計劃的更多信息，請參閱在事件管理員中使用升級計劃。

建立聯絡人

若要建立連絡人，請使用下列步驟。

1. 開啟「事件管理員」主控台，並從左側導覽列選擇「聯絡人」
2. 選擇建立聯絡人。
3. 輸入連絡人的全名，並提供唯一且可識別的別名。
4. 定義聯絡人管道。我們建議使用兩種或多種不同類型的聯絡管道。
   a. 選擇類型：電子郵件、簡訊或語音。
   b. 輸入聯絡人管道的可識別名稱。
   c. 提供聯繫渠道詳細信息，例如電子郵件：arosalez@example.com
5. 若要定義多個聯絡人管道，請選擇 [新增聯絡人管道]。針對新增的每個新接觸管道重複步驟 4。
6. 定義參與計劃。

> **Important**
> 若要與連絡人互動，您必須定義參與計劃。

   a. 選擇聯絡人管道名稱。
   b. 定義從參與開始算起，需要等待多少分鐘，直到事件管理員參與此聯絡管道為止。

c. 若要新增其他聯絡人管道，請選擇 [新增互動]

7. 定義參與計劃後，選擇「建立」。事件管理員會將啟動碼傳送至每個已定義的聯絡管道。
8. (選擇性) 若要啟動聯絡管道，請輸入「事件管理員」傳送至每個已定義聯絡管道的啟動碼。
9. (選擇性) 若要傳送新的啟動碼，請選擇「傳送新驗證碼」。
10. 選擇 Finish (完成)。

在您定義聯絡人並啟用其聯絡管道之後，您可以將聯絡人新增至升級計畫，以形成升級鏈。要了解有關升級計劃的更多信息，請參閱在事件管理員中使用升級計劃。您可以將聯絡人新增至回應計劃以進行直接參與。若要進一步瞭解如何建立回應計劃，請參閱在事件管理員中使用回應計劃。

將聯絡人詳細資料匯入您的通訊錄

事件發生時，事件管理員可以使用語音或 SMS 通知來通知回應者。為了確保回應者能看到來自事件管理員的來電或簡訊通知，我們建議所有回應者將事件管理員虛擬卡片格式 (.vcf) 檔案下載至其行動裝置上的通訊錄。該文件託管在亞馬遜中CloudFront，可在AWS商業分區中使用。

下載事件管理員 .vcf 檔案

1. 在您的行動裝置上，選擇或輸入下列網址：https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .v cf。
2. 將檔案儲存或匯入至行動裝置上的通訊錄。

在事件管理器中使用待命時間表

事件管理員中的隨時待命排程定義在發生需要操作員介入的事件發生時，誰會收到通知。隨叫排程由您為排程建立的一或多個旋轉組成。每個旋轉最多可包括 30 個觸點。

建立待命中的排程之後，您可以將其作為升級計劃納入升級計劃中。當與該升級計劃相關聯的事件發生時，事件管理員會根據排程通知正在召喚的操作員（或操作員）。然後，該聯繫人可以確認參與。在您的升級計劃中，您可以跨越多個升級階段指定一或多個待命排程，以及一或多個個別聯絡人。如需詳細資訊，請參閱在事件管理員中使用升級計劃。

> **Tip**
>
> 最佳做法是，我們建議在升級計畫中新增聯絡人和隨時待命排程作為上報管道。然後，您應該選擇升級計劃作為響應計劃的參與。此方法可為組織中的事件回應提供最完整的涵蓋範圍。

每個待命排程最多支援八次旋轉。旋轉可以重疊或同時執行。這會增加事件發生時通知回應的操作員數目。您也可以建立連續執行的旋轉。這支援像是「跟隨太陽」事件管理等案例，在這些案例中，您可以在世界各地擁有支援相同服務的群組。

使用本節中的主題可協助您建立和管理事件回應作業的待命排程。

主題

- 在事件管理器中創建隨時待命的計劃和輪替
- 在事件管理器中管理現有的待命排程

在事件管理器中創建隨時待命的計劃和輪替

使用一個或多個輪換聯繫人創建一個隨時待命的計劃，以在輪班期間參與響應事件。

開始之前

在建立隨叫排程之前，請確定您先前已建立要新增至排程中自動重建的連絡人。如需相關資訊，請參閱在事件管理員中使用連絡人 。

日光節約時間 (DST) 變更的說明

當您建立輪替時，您可以指定全域時區，作為您為此輪替指定的工作班次涵蓋時間與日期的基礎。您可以使用互聯網號碼分配機構（IANA）定義的任何時區。例如：America/Los_Angeles、UTC 和 Asia/Seoul。您可以將多個輪換新增至隨叫排程。但是，當每個輪換的回應者位於不同時區的地理位置時，請記住每個旋轉可能會受到的任何 DST 變更。

例如，America/Los_Angeles並Europe/Dublin觀察不同的 DST 時間表。因此，兩個區域之間的時差可能從 6 到 8 小時不等，具體取決於一年中的時間。例如，隨follow-the-sun叫排程在America/Los_Angeles時區中有一個旋轉，而在中有一個旋轉。Europe/Dublin在此範例中，由於 DST 變更，明細表可能包含一小時的班次間隔或一小時的班次重疊。

為了避免這些情況，我們建議採用以下方法：

1. 針對待命排程中的所有旋轉使用單一時區。
2. 當您在特定時區以外指派回應者時，計算當地時間。

如果您決定將每個輪替指派給其當地時區，請在任何 DST 之前檢閱排程。然後，根據需要調整旋轉移次數，以確保在任何 DST 更改生效之前避免在待命覆蓋範圍中出現任何意外間隙或重疊。

按待命排程建立

1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 選擇 [建立隨時待命排程]。
4. 在「排程名稱」中，輸入可協助您識別排程的名稱，例如**MyApp Primary On-call Schedule**。
5. 對於「排程別名」，請輸入目前排程中唯一的別名AWS 區域，例如**my-app-primary-on-call-schedule**。
6. (可選) 在「標籤」區域中，將一個或多個標籤關鍵字名稱和值配對套用至待命明細表。

   標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。例如，您可以標記排程，以識別排程執行的期間、其包含的運算子類型或其支援的提升計劃。如需標記事件管理員資源的詳細資訊，請參閱標記事件管理員中的資源。
7. 將一個或多個自動重建新增至待命排程來繼續進行。

在事件管理器中為待命排程創建輪換

在調用時間表中的旋轉指定當移位是有效的。它還可以指定移動旋轉的接觸。您可以在單一隨時待命排程中包含最多八個自動旋轉。

您可以將您在「事件管理員」中建立為聯絡人的任何個人新增至輪換。如需管理連絡人的詳細資訊，請參閱在事件管理員中使用連絡人。

設定輪換時，您可以在頁面右側的「預覽」行事曆中查看整體排程的外觀。

若要建立待命排程的輪替

1. 在「建立隨叫排程」頁面的「循環 1」段落中，針對輪替名稱，輸入識別輪替的名稱，例如**00:00 - 7:59 Support**、或**Dublin Support Group**。
2. 在「開始日期」中，以YYYY/MM/DD格式輸入此輪替作用中的日期，例如2023/07/14。
3. 針對「時區」，選取全域時區，作為您指定此輪替之工作班次涵蓋範圍時間與日期的基礎。

   您可以使用互聯網號碼分配機構（IANA）定義的任何時區。例如：「美國/洛杉磯」，「UTC」，「亞洲/首爾」。如需詳細資訊，請參閱 IANA 網站上的時區資料庫。

> **Warning**
>
> 您可以根據自己的時區進行每個旋轉。但是，您選取的時區中的任何日光節約時間變更都會影響您預期的涵蓋範圍期間。如需詳細資訊，請參閱本主題稍早的日光節約時間 (DST) 變更計算。

4. 對於「旋轉」開始時間，請輸入此旋轉偏移以 24 小時hh:mm格式開始的時間，例如16:00。

   請注意時區中聯絡人的當地時間差異，與您指定的時區不同。例如，如果您選擇America/Los_Angeles作為時區和00:00旋轉開始時間，則這等於愛爾蘭都柏林的 08:00 和印度孟買的 13:30。

5. 在「旋轉結束時間」中，輸入此旋轉的偏移結束時間為 24 小時hh:mm格式，例如23:59。

> **Note**
>
> 旋轉開始和結束之間的時間長度必須至少為 30 分鐘。

6. (選擇性) 若要將旋轉長度設定為 24 小時，請選取 24 小時涵蓋範圍，然後在「旋轉開始時間」欄位中輸入此旋轉的開始時間。旋轉結束時間值會自動更新。

   例如，如果您希望在上午 11 點有 24 小時值班變更的保險範圍，請選擇 24 小時保險並輸入**11:00**作為開始時間。

7. 對於使用中天數，請選取此輪替作用中的星期幾。例如，如果您的待命計劃不包括週末保險，請選擇星期日和星期六以外的所有日子。

8. 繼續將接觸加入至旋轉。

將聯絡人新增至事件管理員的隨時待命排程中的輪替

對於隨時待命排程中的每個輪替，您可以新增一或多個聯絡人，最多共 30 位。您可以選擇在「事件管理員」組態中設定的連絡人。

當您將聯絡人新增至輪換時，該聯絡人可能會收到通知，作為其隨時待命職責的一部分。通知可以通過電子郵件，SMS 或語音呼叫發送，如聯繫人詳細信息中指定的。

如需管理連絡人和連絡人通知選項的詳細資訊，請參閱在事件管理員中使用連絡人。

在待命排程中將聯絡人新增至輪換

1. 在 [建立隨時待命的排程] 頁面上，在輪換的 [聯絡人] 區段中，選擇 [新增或移除聯絡人]。
2. 在 [新增或移除連絡人] 對話方塊中，選取要包括在旋轉中的連絡人別名。

   您選取連絡人的順序，就是輪替排程中的第一個列出順序。您可以在新增聯絡人後變更順序。
3. 選擇 Confirm (確認)。
4. 若要變更連絡人在訂單中的位置，請選取該使用者的選項按鈕，然後使用「向上」
   ()
   和「向下」
   ()
   按鈕來更新連絡人順序。
5. 透過指定旋轉的個別偏移週期和長度來繼續。

在「事件管理員」中指定班次週期和長度，並將標籤新增至旋轉

Shift 循環指定旋轉中的接點旋轉進出呼叫的頻率。週期長度可以在天數、週數或月數中指定。

指定偏移週期和長度並將標籤加入至旋轉的步驟

1. 在 [建立隨時待命排程] 頁面的循環設定區段中，執行下列動作：

   - 對於 Shift 週期類型，請從、和中選擇，來指定每個待命中的班次是否持續一定的天數`Daily`、`Weekly`週數或月數。`Monthly`
   - 在輪班長度中，輸入一個班次持續的天數、週數或月數。

     例如，如果您選擇`Daily`並輸入**1**，則每個聯繫人的隨叫輪班持續一天。如果您選擇`Weekly`並輸入**3**，則每個聯繫人的待命輪班持續三週。
2. (可選) 在「標籤」區域中，將一個或多個標籤關鍵字名稱和值配對套用至旋轉。

   標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。例如，您可以標記輪換，以識別分配給它的聯繫人的位置，它打算提供的覆蓋類型，或者它將支持的升級計劃。如需標記事件管理員資源的詳細資訊，請參閱標記事件管理員中的資源。
3. (建議使用) 使用行事曆預覽，以確保您隨時待命的排程沒有意外的涵蓋範圍。
4. 選擇 建立 。

您現在可以將待命排程新增為升級計畫中的升級通道。如需相關資訊，請參閱 建立升級計劃。

在事件管理器中管理現有的待命排程

使用本節中的內容可協助您處理已建立的待命排程。

主題

檢視待命的排程詳細資料

您可以在「檢視待命排程詳細資訊」頁面上存取待命排程的at-a-glance摘要。此頁面還包含有關當前正在召喚的人員以及接下來誰在召喚的信息。該頁面包含日曆視圖，顯示在任何特定時間正在召喚哪些聯繫人。

若要檢視待命的排程明細

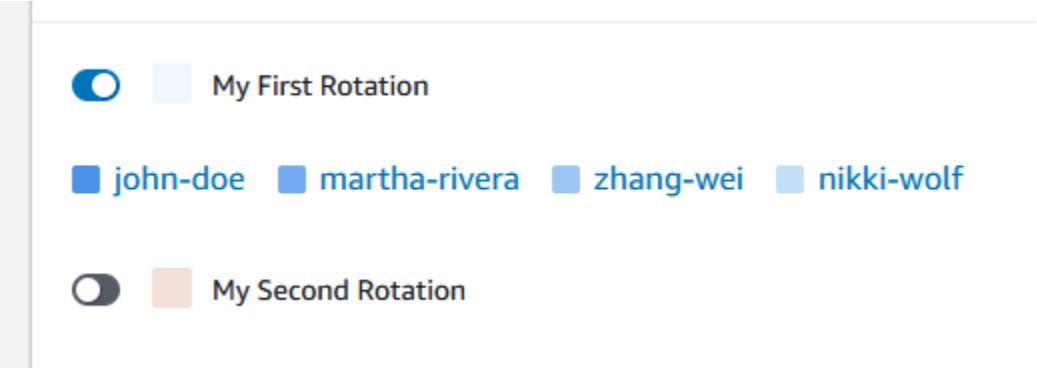
1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 在要檢視的待命排程資料列中，執行下列其中一項作業：
   - 若要開啟行事曆的摘要檢視，請選擇排程別名。

     -或-

     選取列的圓鈕，然後選擇 [檢視]。
   - 若要開啟排程的行事曆檢視，請選擇 [檢視行事曆]

     在日曆視圖中，選擇排程中特定日期的聯繫人姓名，以查看有關指定工作班次的詳細信息或創建覆蓋，。
   - 若要開啟或關閉行事曆中特定旋轉的顯示，請選擇旋轉名稱旁邊的開關。



編輯隨時待命的排程

您可以更新待命排程及其自動重建的組態，但下列詳細資訊除外：

- 排程別名
- 旋轉名稱
- 輪替開始日期

若要使用現有行事曆作為具有變更這些值之新行事曆的基礎，您可以改為複製行事曆。如需相關資訊，請參閱 複製待命排程。

編輯隨時待命的排程

1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 執行下列任意一項：
   - 選取要編輯的待命排程列中的圓鈕，然後選擇編輯。
   - 選擇待命排程的排程別名，以開啟「檢視隨叫排程明細」頁面，然後選擇編輯。
4. 對待命中的排程及其旋轉進行所需的任何修改。您可以變更旋轉組態選項，例如開始和結束時間、連絡人和重複性。您可以依需要在明細表中加入或移除旋轉。行事曆預覽會在您進行變更時反映出來。

   如需有關使用頁面上選項的資訊，請參閱在事件管理器中創建隨時待命的計劃和輪替。
5. 選擇 Update (更新)。

> **Important**
>
> 如果編輯包含取代的明細表，您所做的變更可能會影響取代。為確保覆寫保持如預期般設定，我們建議您在更新排程後仔細檢閱班次優先順序。

複製待命排程

若要使用現有待命排程的組態作為新排程的起點，您可以建立行事曆副本並視需要加以修改。

若要複製待命排程

1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 在資料列中選取要複製的待命排程的圓鈕。
4. 請選擇 Copy (複製)。
5. 對日曆及其旋轉進行所需的任何修改。您可以依需要變更、加入或移除旋轉。

   > **Note**
   >
   > 複製現有排程時，必須為每個輪替指定新的開始日期。複製的排程不支援過去開始日期的自動重建。

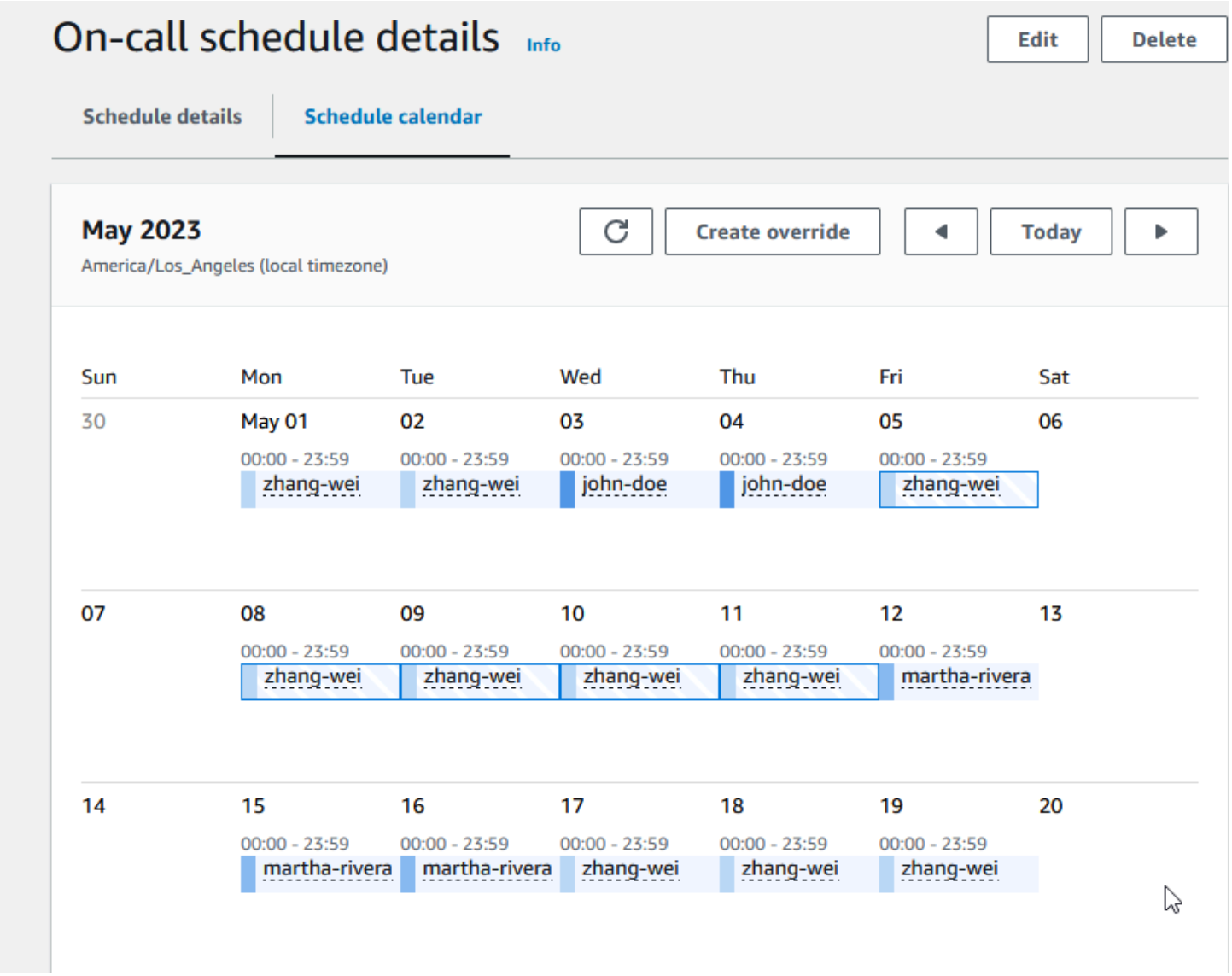
   如需有關使用頁面上選項的資訊，請參閱在事件管理器中創建隨時待命的計劃和輪替。
6. 選擇「建立副本」。

建立待命排程輪替的覆寫

如果您需要對現有的旋轉明細表進行一次性變更，您可以建立取代。取代可讓您以另一個接點取代接觸的全部或部分位移。您也可以建立跨越多個班次的取代。

您只能將接觸指定給旋轉的取代指定。

在行事曆預覽中，取代的班次會以條紋背景顯示，而非純色背景。在下面的圖片中，我們可以看到張偉的聯繫人正在召喚，其中包括約翰·多伊和瑪莎·里維拉的部分班次，從 5 月 5 日到 5 月 11 日結束。



若要建立待命排程的覆寫

1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 在要檢視的待命排程資料列中，執行下列其中一項作業：
   - 選擇排程別名，然後選擇「排程行事曆」標籤。
   - 選擇檢視行事曆。
4. 執行下列任意一項：
   - 選擇「建立覆寫」。
   - 在行事曆預覽中選擇連絡人的名稱，然後選擇 [覆寫班次]。

5. 在「建立班次取代」對話方塊中，執行下列操作：

> **Note**
>
> 覆寫的長度必須至少為 30 分鐘。您只能針對未來發生不超過六個月的工作班次指定修訂。

   a. 對於 「選取旋轉」，請選取要在其中建立取代的旋轉名稱。
   b. 在開始日期中，選取或輸入覆寫開始的日期。
   c. 在「開始時間」中，輸入取代以hh:mm格式開始的時間。
   d. 在結束日期中，選取或輸入覆寫結束的日期。
   e. 在「結束時間」中，以hh:mm格式輸入取代結束的時間。
   f. 對於選取覆寫連絡人，選取覆寫期間內正在召喚的循環聯絡人名稱。
6. 選擇「建立覆寫」。

建立取代後，您可以透過其條紋背景來識別它。當您選擇已覆寫工作班次的聯絡人姓名時，資訊方塊會將其識別為已覆寫工作班次。您可以選擇 [刪除覆寫] 將其移除，並還原原始隨叫指派。

刪除隨叫的排程

當您不再需要特定的待命排程時，可以將其從事件管理員中刪除。

如果有任何升級計劃或響應計劃當前使用待命時間表作為升級渠道，那么您應該在刪除該時間表之前將其從這些計劃中刪除。

若要刪除待命排程

1. 開啟「事件管理員」主控台。
2. 在左側導覽中，選擇待命排程。
3. 在資料列中選取要刪除的待命排程的圓鈕。
4. 選擇 刪除 。
5. 在刪除隨叫的排程中？ 」對話方塊中，**confirm**於文字方塊中輸入。
6. 選擇 刪除 。

在事件管理員中使用升級計劃

AWS Systems Manager Incident Manager透過您定義的聯絡人或待命排程 (統稱為上報管道) 提供上報路徑。您可以將多個上報通道同時將多個上報通道提取到事件。如果升級管道中指定的聯絡人沒有回應，則事件管理員會升級到下一組聯絡人。您也可以選擇計劃是否在使用者確認參與後停止升級。您可以將升級計劃新增到回應計劃，將升級計劃在事件開始時開始升級計劃。您也可以將升級計劃新增至使用中的事件。

主題

階段

升級計劃使用每個階段持續定義的分鐘數的階段。每個階段都有下列資訊：

- 持續時間 — 計劃等待下一個階段開始之前的時間量。升級計劃的第一階段開始一旦參與開始。
- 升級管道 — 升級管道是單一聯絡人或隨時待命排程，由多位聯絡人組成，這些聯絡人會根據定義的時間表輪換職責。升級計劃使用其定義的參與計劃來參與每個渠道。您可以設定每個升級管道，在升級計畫繼續下一階段之前停止進度。每個階段可以有多個上報通道。

  如需設定個別連絡人資訊，請參閱在事件管理員中使用連絡人。如需建立待命排程的資訊，請參閱在事件管理器中使用待命時間表。

建立升級計劃

1. 開啟「事件管理員」主控台，然後從左側導覽列選擇「呈報計劃」
2. 選擇 [建立升級計劃]。
3. 在名稱中，輸入提升計劃的唯一名稱，例如**My Escalation Plan**。
4. 在別名中，輸入別名以協助您識別計劃，例如**my-escalation-plan**。
5. 針對「階段」持續時間，輸入「事件管理員」等待到下一個階段的分鐘數。
6. 對於升級渠道，選擇在此階段參與的一個或多個聯繫人或隨叫時間表。
7. (選擇性) 若要讓聯絡人在確認參與後停止提升計劃，請選取確認停止計劃進展。
8. 若要將其他頻道新增至此階段，請選擇 [新增上報管道]。

9. 若要將其他階段新增至提升計劃，請選擇 [新增階段]。
10. 重複步驟 5 到 9，直到您完成新增此升級計畫所需的上報管道和階段為止。
11. (選用) 在 Tags (標籤) 區域將一個或多個標籤索引鍵名稱和值對套用到提升計劃。

    標籤是您指派給資源的選用性中繼資料。標籤允許您以不同的方式 (例如用途、擁有者或環境) 將資源分類。例如，您可以標記呈報計劃，以識別要用於的事件類型、其包含的呈報通道類型或其支援的升級計畫。如需標記事件管理員資源資源資源資源資源資源資源資源標記事件管理員中的資源
12. 選擇 [建立升級計劃]。

在事件管理員中使用聊天頻道

事件管理器的AWS Systems Manager功能使事件應變人員能夠在事件發生期間直接通過聊天渠道進行通信。聊天頻道是您設定的聊天室AWS Chatbot。然後，您可以將此通道連線至事件管理員中的回應計畫。

在事件發生期間，回應者會使用聊天管道互相溝通事件。事件管理員還會將有關事件的任何更新和通知直接推送到聊天頻道。它會使用您在聊天室組態中指定的一或多個 Amazon Simple Notification Service (Amazon SNS) 主題傳送這些通知。

AWS Chatbot事件管理員支援下列應用程式的聊天頻道：

- Slack
- Microsoft Teams
- Amazon Chime

設定用於事件的聊天頻道的程序包含三個不同 Amazon Web Services 服務中的任務。

任務

- 工作 1：為您的聊天頻道建立或更新 Amazon SNS 主題
- 任務 2：建立聊天頻道AWS Chatbot
- 工作 3：將聊天頻道新增至事件管理員的回應計劃
- 透過聊天頻道進行互動

工作 1：為您的聊天頻道建立或更新 Amazon SNS 主題

Amazon SNS 是一種受管服務，會提供從發佈者到訂閱者到訂閱者的訊息傳遞 (也稱為生產者和消費者)。發佈者透過製作並傳送訊息到主題 (其為邏輯存取點和通訊管道) 與訂閱者進行非同步的通訊。事件管理員會使用您與回應計劃相關聯的一或多個主題，將事件相關的通知傳送給事件回應人員。

在回應計劃中，您可以在事件通知中加入一或多個 Amazon SNS 主題。最佳實務是，您應該在新增到複製組的每AWS 區域個主題中，建立 SNS 主題。

> **Tip**
>
> 如需更線性的設定工作流程，建議您先設定 Amazon SNS 主題，以便與事件管理員搭配使用。配置完成後，您可以創建聊天頻道。

為您的聊天頻道建立或更新 Amazon SNS 主題

1. 按照 Amazon S imple Notification Service 開發人員指南中，建立 Amazon SNS 主題中的步驟進行。

   > **Note**
   >
   > 建立主題之後，您可以對其進行編輯以更新其存取原則。

2. 選擇您建立的主題，記下或複製主題的 Amazon 資源名稱 (ARN)`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`。
3. 選擇 [編輯]，然後展開 [存取原則] 區段，以設定預設值以外的其他存取權限。
4. 將下列陳述式新增至政策的陳述式陣列：

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
```

```
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

取代*#####*，如下所示：

- *sns-topic-arn*是您為此區域建立之主題的 Amazon 資源名稱 (ARN)，格式為arn:aws:sns:us-east-2:111122223333:My_SNS_topic。
- *## ID* 是您正在使用的 ID，例如111122223333。AWS 帳戶

5. 選擇 Save changes (儲存變更)。
6. 在複製組中包含的每個區域中重複此程序。

任務 2：建立聊天頻道AWS Chatbot

您可以在 Slack、微軟團隊或 Amazon Chime 聲中建立聊天頻道。每個回應計劃只需要一個聊天頻道。

對於您的聊天頻道，我們建議遵循最低權限的主體（不要為用戶提供完成任務所需的更多權限）。您還應該定期查看AWS Chatbot聊天頻道的會員資格。評論有助於檢查只有適當的回應者和其他利益相關者才能存取您的聊天頻道。

在AWS Chatbot啟用的 Slack 通道和 Microsoft Teams 通道中，事件回應者可以直接從 Slack 或 Microsoft Teams 應用程式執行數個事件管理員 CLI 命令。如需詳細資訊，請參閱透過聊天頻道進行互動。

> **Important**
>
> 您添加到聊天頻道的用戶必須與您的升級或響應計劃中列出的相同聯繫人。您還可以將其他用戶添加到聊天頻道中，例如利益相關者和事件觀察者。

有關的一般資訊AWS Chatbot，請參閱《AWS Chatbot管理員指南》AWS Chatbot中的內容。

從下列應用程式中選擇建立頻道：

Slack

此程序中的步驟提供建議的權限設定，讓所有頻道使用者都能透過事件管理員使用聊天指令。您的事件回應人員可以使用支援的聊天指令，直接從 Slack 聊天頻道更新並與事件互動。如需相關資訊，請參閱 透過聊天頻道進行互動。

在 Slack 中建立聊天頻道

- 請遵循《AWS Chatbot管理員指南》中教學課程：開始使用 Slack 中的步驟，並在設定中包含下列項目。
  - 在步驟 10 中，針對 [角色設定] 選擇 [通道角色]。
  - 在步驟 10d 中，針對「策略範本」，選取「事件管理員」權限。
  - 在步驟 11 中，針對「通道護欄原則」，選擇「策略名稱」AWSIncidentManagerResolverAccess。
  - 在步驟 12 的 SNS 主題區段中，執行下列動作：
    - 針對區域 1，選取AWS 區域複製組中包含的一個。
    - 在主題 1 中，選取您在該區域中建立的 SNS 主題，用來傳送事件通知至聊天頻道。
    - 針對複製組中的每個額外區域，選擇新增其他區域，然後新增其他區域和 SNS 主題。

Microsoft Teams

此程序中的步驟提供建議的權限設定，讓所有頻道使用者都能透過事件管理員使用聊天指令。您的事件回應人員可以使用支援的聊天指令，直接從 Microsoft Teams 聊天頻道更新事件並與之互動。如需相關資訊，請參閱 透過聊天頻道進行互動。

在微軟團隊中建立聊天頻道

- 請遵循AWS Chatbot系統管理員指南中教學課程：開始使用 Microsoft Teams 中的步驟，並在您的設定中包含下列項目：
  - 在步驟 10 中，針對 [角色設定] 選擇 [通道角色]。
  - 在步驟 10d 中，針對「策略範本」，選取「事件管理員」權限。
  - 在步驟 11 中，針對「通道護欄原則」，選擇「策略名稱」AWSIncidentManagerResolverAccess。
  - 在步驟 12 的 SNS 主題區段中，執行下列動作：
    - 針對區域 1，選取AWS 區域複製組中包含的一個。

- 在主題 1 中，選取您在該區域中建立的 SNS 主題，用來傳送事件通知至聊天頻道。
- 針對複製組中的每個額外區域，選擇新增其他區域，然後新增其他區域和 SNS 主題。

Amazon Chime

在 Amazon Chime 聲中建立聊天頻道

- 請遵循AWS Chatbot管理員指南中教學：開始使用 Amazon Chime 中的步驟，並在您的組態中包含下列項目：
  - 在步驟 11 中，針對策略範本，選取事件管理員權限。
  - 在步驟 12 的 SNS 主題區段中，選取要將通知傳送至 Amazon Chime 網路掛鉤的 SNS 主題：
    - 針對區域 1，選取AWS 區域複製組中包含的一個。
    - 在主題 1 中，選取您在該區域中建立的 SNS 主題，用來傳送事件通知至聊天頻道。
    - 針對複製組中的每個額外區域，選擇新增其他區域，然後新增其他區域和 SNS 主題。

> **Note**
>
> Amazon Chime 不支援事件回應人員可以在 Slack 和 Microsoft Teams 聊天管道中使用的聊天命令。

工作 3：將聊天頻道新增至事件管理員的回應計劃

當您建立或更新回應方案時，您可以新增聊天頻道，讓回應者透過以下方式進行通訊和接收更新。

執行中的步驟時建立回應計劃，請針對區段(選擇性) 指定事件回應聊天通道選取您要用於與此回應計劃相關之事件的通道。

透過聊天頻道進行互動

對於 Slack 和 Microsoft Teams 中的頻道，事件管理員可讓回應者使用下列`ssm-incidents`命令，直接從聊天管道與事件互動：

- 啟動事件
- list-response-plan

- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record
- update-timeline-event

若要在作用中事件的聊天頻道中執行命令，請使用下列格式。將 *cli-options* 取代為指令所包含的任何選項。

```
@aws ssm-incidents cli-options
```

例如：

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

在事件管理員中使用系統管理員自動化手冊

您可以使用 AWS Systems ManagerAutomation 的 AWS Systems Manager Runbook (一種功能) 來自動化AWS 雲端環境中的常見應用程式和基礎結構工作。

每個 runbook 定義了 runbook 工作流程，這是由系統管理員在受管理的節點或其他AWS資源類型上執行的動作組成。您可以使用 runbook 來自動化AWS資源的維護、部署和補救。

在事件管理員中，runbook 驅動事件回應和緩和措施，並指定要用作回應計畫的一部分的 runbook。

在您的回應計畫中，您可以從數十種預先設定的 Runbook 中進行選擇，以處理常用的自動化工作，或是建立自訂的 Runbook。當您在回應計畫定義中指定 runbook 時，系統可以在事件開始時自動啟動 runbook。

> **Important**
>
> 跨區域容錯移轉所建立的事件不會叫用回應計畫中指定的 Runbook。

如需系統管理員自動化、手冊，以及搭配事件管理員使用 Runbook 的相關資訊，請參閱下列主題：

- 若要將 Runbook 新增至回應計畫，請參閱在事件管理員中使用回應計劃。
- 若要瞭解有關 Runbook 的更多資訊，請參閱AWS Systems Manager使用者指南中的AWS Systems Manager自動化和AWS Systems Manager自動化手冊參考資料。
- 如需使用手冊成本的相關資訊，請參閱系統管理員定價。
- 如需在事件是由 Amazon CloudWatch 警示或 Amazon 事件建立時自動呼叫執行手冊的相關資訊，請參閱教學課程：搭配EventBridge事件管理員使用系統管理員自動化手冊。

主題

啟動和執行手冊工作流程所需的 IAM 許可

事件管理員需要執行 Runbook 的權限，做為事件回應的一部分。若要提供這些權限，您可以使用 AWS Identity and Access Management (IAM) 角色、Runbook 服務角色和自動化*AssumeRole*。

Runbook 服務角色是必要的服務角色。此角色為事件管理員提供存取和啟動 runbook 工作流程所需的權限。

自動化AssumeRole提供執行 runbook 中指定的個別命令所需的權限。

> **Note**
>
> 如果未指AssumeRole定，系統管理員自動化會嘗試針對個別命令使用 Runbook 服務角色。如果未指定AssumeRole，則必須將必要的權限新增至 Runbook 服務角色。如果你不這樣做，runbook 無法運行這些命令。
> 不過，為了安全性最佳作法，我們建議您使用個別的AssumeRole。使用單獨的方式AssumeRole，您可以限制必須新增至每個角色的必要權限。

如需有關自動化的詳細資訊AssumeRole，請參閱《AWS Systems Manager使用者指南》中的 < 設定自動化的服務角色 (假定角色) 存取權限 > 。

您可以在 IAM 主控台中自行建立任一類型的角色。-您也可以在建立或更新回應計劃時，讓事件管理員為您建立任何一種角色。

Runbook 服務角色權限

Runbook 服務角色權限是透過類似下列的原則提供。

第一個陳述式允許事件管理員啟動系統管理員StartAutomationExecution作業。然後，此作業會在三種 Amazon 資源名稱 (ARN) 格式所表示的資源上執行。

第二個陳述式允許 Runbook 服務角色在受影響的帳戶中執行時，該 runbook 服務角色扮演另一個帳戶中的角色。如需詳細資訊，請參閱《AWS Systems Manager使用指南》中的「在多個AWS 區域帳戶中執行自動化」。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
        "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
      ]
    },
```

```
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

自動化AssumeRole權限

當您建立或更新回應計劃時，您可以從數個AWS受管理的策略中選擇要附加至「事AssumeRole件管理員」建立的策略。這些原則提供執行在事件管理員 runbook 案例中使用的一些常見作業的權限。您可以選擇這些受管理的策略中的一個或多個來為您的AssumeRole策略提供權限。下表說明從「事件管理員」主控台建立時，您可以AssumeRole從中選擇的策略。

AWS 受管政策名稱	策略描述
AmazonSSMAutomationRole	授予系統管理員自動化服務的權限，以執行 Runbook 中定義的活動。將此政策指派給管理員和信任的高權限使用者。
AWSIncidentManagerResolverAccess	授與使用者啟動、檢視和更新事件的權限。您還可以使用它們在事件儀表板中創建客戶時間表事件和相關項目。

您可以使用這些受管理的原則來授與許多常見事件回應案例的權限。但是，您需要的特定任務所需的權限可能會有所不同。在這些情況下，您需要為AssumeRole. 如需相關資訊，請參閱AWS Systems Manager自動化工作流程簿參考。

使用工作流程簿參數

將 Runbook 加入回應計劃時，您可以指定 Runbook 在執行時間應使用的參數。回應計劃支援具有靜態和動態值的參數。對於靜態值，您可以在定義回應計劃中的參數時輸入值。對於動態值，系統會透過從事件中收集資訊來確定正確的參數值。Incident Manager 支援以下動態參數：

`Incident ARN`

當 Incident Manager 建立事件時，系統會擷取對應事件記錄的 Amazon Resource Name (ARN)，並在 Runbook 中為此參數輸入該名稱。

> **Note**
>
> 此值只能指派給 `String` 類型的參數。如果指派給任何其他類型的參數，則無法執行 Runbook。

`Involved resources`

當 Incident Manager 建立事件時，系統會擷取事件所涉及資源的 ARN。然後，這些資源 ARN 會指派給 Runbook 中的此參數。

關於相關資源

事件管理員可以使用CloudWatch警示、事件和手動建立的EventBridge事件中指定的AWS資源 ARN 填入 runbook 參數值。本節說明在填入此參數時，「事件管理員」可擷取 ARN 的不同資源類型。

CloudWatch 警示

當事件是透過CloudWatch警示動作建立時，事件管理員會自動從關聯的指標中擷取下列類型的資源。然後，它會使用下列相關資源填入所選參數：

AWS 服務	資源類型
Amazon DynamoDB	全域次要索引 串流 資料表
Amazon EC2	映像 執行個體
AWS Lambda	函數別名 函數版本

AWS 服務	資源類型
	函數
Amazon Relational Database Service (Amazon RDS)	叢集 數據庫實例
Amazon Simple Storage Service (Amazon S3)	儲存貯體

EventBridge 規則

當系統從事件建立事件時，EventBridge事件管理員會將事件中的`Resources`屬性填入選擇的參數。如需詳細資訊，請參閱 Amazon EventBridge使用者指南中的 Amazon EventBridge 事件。

手動建立的事件

當您使用 StartIncidentAPI 動作建立事件時，事件管理員會使用 API 呼叫中的資訊填入選擇的參數。具體而言，它會使用在參數中傳遞`INVOLVED_RESOURCE`的類型項目來填入`relatedItems`參數。

> **Note**
>
> 該`INVOLVED_RESOURCES`值只能指定給類型的參數`StringList`。如果指派給任何其他類型的參數，則無法執行 Runbook。

定義一個工作手冊

建立 runbook 時，您可以遵循此處提供的步驟，或者您可以遵循「系統管理員使用者指南」中「使用手冊」一節中提供的更詳細的指南。如果您要建立多帳戶、多區域 Runbook，請參閱《系統管理員使用指南》中的〈在多個帳戶AWS 區域和帳戶中執行自動化〉。

定義一個工作手冊

1. 開啟系統管理員主控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，選擇 Documents (文件)。
3. 選擇 Create automation (建立自動化)。
4. 輸入唯一且可識別的 Runbook 名稱。
5. 輸入工作手冊的描述。

6. 為要承擔的自動化文件提供 IAM 角色。這允許 Runbook 自動運行命令。如需詳細資訊，請參閱設定自動化工作流程的服務角色存取權限。
7. (選擇性) 新增 Runbook 開頭的任何輸入參數。您可以在啟動 runbook 時使用動態或靜態參數。動態參數使用 Runbook 啟動時事件中的值。靜態參數使用您提供的值。
8. (選擇性) 新增目標類型。
9. (選擇性) 新增標籤。
10. 填寫在運行手冊將採取的步驟，當它運行。每個步驟都需要：
    - 名稱。
    - 步驟用途的描述。
    - 要在步驟中執行的動作。Runbook 使用「暫停」動作類型來描述手動步驟。
    - (選擇性) 指令屬性。
11. 添加所有必需的 runbook 步驟後，選擇創建自動化。

若要啟用跨帳戶功能，請與事件期間使用 runbook 的所有應用程式帳戶共用管理帳戶中的 runbook。

共用工作手冊

1. 開啟系統管理員主控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，選擇 Documents (文件)。
3. 在文件清單中，選擇您要共用的文件，然後選擇 [檢視詳細資料]。在 Permissions (許可) 索引標籤中，驗證您是文件的擁有者。只有文件擁有者可以分享文件。
4. 選擇 編輯 。
5. 若要公開共享命令，選擇 Public (公有)，然後選擇 Save (儲存)。若要私下共用命令，選擇 Private (私有)，輸入 AWS 帳戶 ID，選擇 Add permission (新增許可)，然後選擇 Save (儲存)。

事件管理員手冊範本

事件管理員提供下列 runbook 範本，以協助您的小組開始撰寫系統管理員自動化中的 Runbook。您可以直接使用此範本，也可以編輯範本以包含應用程式和資源的特定詳細資訊。

尋找事件管理員工作流程簿範本

1. 開啟系統管理員主控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，選擇 Documents (文件)。

3. 在 [文件] 區域中，**AWSIncidents-**在搜尋欄位中輸入，以顯示所有「事件管理員」Runbook。

> **Tip**
>
> 輸入**AWSIncidents-**為自由文字，而不是使用文件名稱前置詞篩選選項。

使用範本

1. 開啟系統管理員主控台，網址為 https://console.aws.amazon.com/systems-manager/。
2. 在導覽窗格中，選擇 Documents (文件)。
3. 從文件清單中選擇您要更新的範本。
4. 選擇 [內容] 索引標籤，然後複製文件的內容。
5. 在導覽窗格中，選擇 Documents (文件)。
6. 選擇 Create automation (建立自動化)。
7. 輸入唯一且可識別的名稱。
8. 選擇編輯器索引標籤。
9. 選擇 編輯 。
10. 在 [文件編輯器] 區域中貼上或輸入複製的詳細資訊。
11. 選擇 Create automation (建立自動化)。

AWSIncidents-CriticalIncidentRunbookTemplate

這AWSIncidents-CriticalIncidentRunbookTemplate是一個以手動步驟提供事件管理員事件生命週期的範本。這些步驟非常通用，可用於大多數應用程式，但足以讓回應人員開始解決事件。

在事件管理員中使用回應計劃

回應計劃可讓您規劃如何回應影響使用者的事件。回應計畫的運作方式為範本，其中包含有關參與者、事件的預期嚴重性、要啟動的自動執行手冊，以及要監視的指標等資訊。

最佳實務

當您提前規劃事件時，可以減少對團隊事件的影響。當您設計回應計劃時，團隊應該考慮下列最佳作法。

- 簡化參與 — 找出最適合事件的團隊。如果您參與的分配名單太廣，或者您與錯誤的團隊合作，則可能會在事件期間引起混亂並浪費響應者時間。
- 可靠的升級 — 對於您在響應計劃中的參與，我們建議您選擇參與計劃而不是聯繫人或隨時待命的時間表。接合計劃應指定事件期間要互動的個別接觸或待命明細表 (其中包含多個旋轉接點)。由於參與計劃中指定的回應者有時無法連線，因此您應該在回應計劃中設定備份回應者，以涵蓋這些案例。使用備用聯絡人時，如果主要和次要連絡人無法使用，或者在涵蓋範圍內存在其他計劃之外的漏洞，事件管理員仍會通知聯絡人有關事件的聯絡人。
- Runbook — 使用 Runbook 提供可重複、易於理解的步驟，以減輕回應者在事件期間體驗的 stress。
- 協同合作 — 使用聊天管道簡化事件期間的溝通。聊天頻道可協助回應者掌握最新資訊。他們還可以通過這些渠道與其他響應者共享信息。

建立回應計劃

使用下列程序來建立回應計劃並自動化事件回應。

若要建立回應計劃

1. 開啟「事件管理員」主控台，然後在導覽窗格中選擇「回應計劃」。
2. 選擇 [建立回應計劃]。
3. 在名稱中，輸入要在回應計劃的 Amazon 資源名稱 (ARN) 中使用的唯一且可識別的回應計劃名稱。
4. (選擇性) 在「顯示名稱」中，輸入更易於閱讀的名稱，以便在建立事件時識別回應計劃。
5. 請指定未預期事件記錄的預設值來繼續。

指定事件預設值

若要協助您更有效地管理事件，您可以指定預設值。「事件管理員」會將這些值套用至與回應計劃相關聯的所有事件。

指定未預期事件預設值

1. 在「標題」中，輸入此事件的標題，以協助您在「事件管理員」首頁識別該事件。
2. 針對「影響」，請選擇影響等級，以指出從此回應計劃建立之未預期事件的潛在範圍，例如「嚴重」或「低」。如需事件管理員中影響等級的相關資訊，請參閱分類。
3. (選擇性) 在「摘要」中，輸入從此回應計劃建立之未預期事件類型的簡短摘要。

4. (選擇性) 在「刪除重複資料」字串中，輸入去除重複資料字串。事件管理員使用此字串來防止相同的根本原因在相同帳戶中建立多個事件。

   重複資料刪除字串是系統用來檢查重複事件的術語或片語。如果您指定重複資料刪除字串，「事件管理員」會在建立事件時，搜尋dedupeString欄位中包含相同字串的未決事件。如果偵測到重複的事件，「事件管理員」會將較新的事件刪除到現有的事件中。

   > **Note**
   >
   > 預設情況下，事件管理員會自動刪除由相同 Amazon CloudWatch 警示或 Amazon 事件所建立的多個 EventBridge 事件重複資料。您不需要輸入自己的重複資料刪除字串，即可防止這些資源類型重複。

5. (選擇性) 在「事件標記」下，新增標籤索引鍵和值，以指派給從此回應計劃建立的事件。

   您必須擁有事件記錄資源的TagResource權限，才能在回應計劃中設定事件標記。

6. 繼續指定一個選擇性的聊天頻道，讓解析器彼此溝通有關事件。

(選擇性) 指定事件回應聊天通道

當您在回應計劃中加入聊天頻道時，回應者會透過該管道收到事件更新。他們可以通過使用聊天命令直接從聊天頻道與事件進行交互。

使用時AWS Chatbot，您可以建立 Slack 或 Amazon Chime 的管道，以便在您的回應計劃中使用。如需有關在中建立聊天頻道的資訊AWS Chatbot，請參閱《AWS Chatbot管理員指南》。

> **Important**
>
> 事件管理員必須擁有發佈至聊天頻道 Amazon Simple Notification Service (Amazon SNS) 主題的許可。如果沒有發佈至該 SNS 主題的權限，您就無法將其新增至回應計劃。事件管理員會將測試通知發佈至 SNS 主題以驗證權限。

如需聊天頻道的詳細資訊，請參閱在事件管理員中使用聊天頻道。

若要指定事件回應聊天頻道

1. 對於聊天頻道，請選取回應者可在事件期間通訊的AWS Chatbot聊天頻道。

> **Tip**
>
> 要在中創建新的聊天頻道AWS Chatbot，請選擇配置新的 Chatbot 客戶端。

2. 對於聊天頻道 SNS 主題，請選擇事件期間要發佈的其他 SNS 主題。如果某個區域在事件發生時關閉，則新AWS 區域增多個 SNS 主題可增加冗餘性。
3. 繼續選取事件期間要參與的聯絡人、待命排程和升級計畫。

(選擇性) 選取參與事件回應的資源

當事件發生時，確定最合適的響應者是非常重要的。最佳作法是建議您執行下列動作：

1. 將聯絡人和待命排程新增為升級計畫中的上報管道。
2. 選擇升級計劃作為回應計劃的參與。

有關聯系人和升級計劃的更多內容，敬請參閱在事件管理員中使用連絡人和在事件管理員中使用升級計劃。

選擇參與事件回應的資源

1. 對於「參與」，請選擇任意數量的升級計劃、待命排程和個別連絡人。
2. 選擇性地指定要作為事件緩和措施的一部分執行的 runbook 來繼續。

(選擇性) 指定事件緩和措施的 Runbook

您可以使用 AWS Systems ManagerAutomation 的 AWS Systems Manager Runbook (一種功能) 來自動化AWS 雲端環境中的常見應用程式和基礎結構工作。

每個手冊定義一個手冊工作流程。runbook 工作流程包括系統管理員在受管理的節點或其他AWS資源類型上執行的動作。在事件管理器中，Runbook 驅動事件響應和緩解措施。

如需有關在回應計畫中使用 Runbook 的詳細資訊，在事件管理員中使用系統管理員自動化手冊請參閱.

若要指定事件緩和措施的 Runbook：

1. 對於 Runbook，請執行下列其中一項作業：

- 從範本選擇複製 runbook，以製作預設事件管理員工作流程簿的副本。對於 Runbook 名稱，輸入新工作流程簿的描述性名稱。
- 選擇選擇現有的手冊。選取要使用的「擁有者」、「工作手冊」和「版本」。

> **Tip**
>
> 若要從頭開始建立 Runbook，請選擇 [設定新的 Runbook]。
> 如需建立 Runbook 的資訊，請參閱 在事件管理員中使用系統管理員自動化手冊。

2. 在「參數」區域中，為您選取的工作簿提供要求的任何參數。

   可用的參數是由 runbook 指定的參數。一個 runbook 可能需要不同於另一個參數。某些參數可能是必需的，其他參數是可選的

   在許多情況下，您可以選擇手動輸入參數的靜態值，例如 Amazon EC2 執行個體 ID 清單。您也可以讓事件管理員提供事件動態產生的參數值。

3. (選擇性) 對於 AutomationAssumeRole，指定要使用的 AWS Identity and Access Management (IAM) 角色。此角色必須具有執行 runbook 中指定的個別命令所需的權限。

> **Note**
>
> 如果未指`AssumeRole`定，事件管理員會嘗試使用 Runbook 服務角色來執行 runbook 中指定的個別命令。

   請選擇下列項目：

   - 輸入 ARN 值 — 以格式手動輸入的 Amazon 資源名稱 (ARN)。 AssumeRole `arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`*例如 **`arn:aws:iam::123456789012:role/MyAssumeRole`**。
   - 使用現有服務角色 — 從帳戶中的現有角色清單中選擇具有所需權限的角色。
   - 建立新的服務角色 — 從AWS受管理的策略中選擇要附加到您的 AssumeRole. 選取此選項之後，對於AWS受管理的策略，請從清單中選擇一或多個策略。

     您可以接受新角色的建議預設名稱，或輸入您選擇的名稱。

> **Note**
>
> 這個新的 Runbook 服務角色與您選取的特定 Runbook 相關聯。它不能與不同的手冊一起使用。這是因為原則的 [資源] 區段將不支援其他 Runbook。

4. 對於 Runbook 服務角色，請指定要使用的 IAM 角色，以提供存取和啟動 Runbook 本身工作流程所需的許可。

   至少，角色必須允許針對您的特定 runbook 執`ssm:StartAutomationExecution`行動作。若要讓 runbook 跨帳戶工作，角色也必須允許您在期間事件管理員中的跨區域和跨帳戶事件管理建立的`AWS-SystemsManager-AutomationExecutionRole`角色執`sts:AssumeRole`行動作。

   請選擇下列項目：

   - 建立新的服務角色 — 事件管理員會為您建立 Runbook 服務角色，其中包含啟動 runbook 工作流程所需的最低權限。

     對於角色名稱，您可以接受建議的預設名稱，或輸入您選擇的名稱。我們建議使用建議的名稱或保持在名稱中的 runbook 的名稱。這是因為新 AssumeRole 功能與您選取的特定 runbook 相關聯，而且可能不包含其他 Runbook 所需的權限。
   - 使用現有的服務角色 — 您或事件管理員先前建立的 IAM 角色會授予所需的權限。

     對於角色名稱，請選取要使用的現有角色名稱。
5. 展開其他選項，然後選擇下列其中一項，以指定 runbook 工作流程應執行的AWS 帳戶位置。

   - 響應計劃所有者的帳戶 — 啟動在創建它的 AWS 帳戶 runbook 工作流.
   - 受影響的帳戶 — 在開始或報告事件的帳戶中啟動 runbook 工作流程。

     當您針對跨帳戶案例使用事件管理員，且 runbook 需要存取受影響帳戶中的資源以進行修復時，請選擇 [受影響的帳戶]。

6. 選擇性地將 PagerDuty 服務整合至回應計劃，以繼續進行。

(選擇性) 將 PagerDuty 服務整合至回應計劃

若要將 PagerDuty 服務整合至回應計劃

當您將事件管理員與整合時 PagerDuty，每當事件管理員 PagerDuty 建立事件時，都會建立對應的事件。中的事件 PagerDuty 會使用您在此處定義的呼叫工作流程和呈報原則，以及「事件管理員」中所定義的原則。 PagerDuty 附加事件管理員的時間表事件作為事件的附註。

1. 展開第三方整合，然後選擇啟用 PagerDuty 整合核取方塊。
2. 在 [選取密碼] 中，選取您AWS Secrets Manager儲存認證的密碼以存取您的 PagerDuty 帳戶。

   如需將 PagerDuty 認證儲存在 Secret Secrets Manager 碼中的相關資訊，請參閱在 AWS Secrets Manager 密碼中儲 PagerDuty 存存取認證。
3. 如果是PagerDuty 服務，請從您要建立 PagerDuty 事件的 PagerDuty 帳戶中選取服務。
4. 繼續新增選擇性標籤並建立回應計劃。

新增標籤並建立回應計劃

若要新增標籤並建立回應計劃

1. (選擇性) 在「標籤」區域中，將一或多個標籤索引鍵名稱/值配對套用至回應計劃。

   標籤是您指派給資源的選用性中繼資料。使用標籤，您可以使用不同的方式對資源進行分類，例如依目的、擁有者或環境。例如，您可能想要標記回應計劃，以識別要緩解的事件類型、其包含的呈報通道類型，或將與之相關聯的升級計畫。如需標記事件管理員資源的詳細資訊，請參閱標記事件管理員中的資源。
2. 選擇 [建立回應計劃]。

在事件管理員中使用發現項目

在事件管理員中，發現項目是指在事件發生時發生的AWS CodeDeploy部署或AWS CloudFormation堆疊更新，以及涉及一或多個可能與事件相關的資源的相關資訊。每個發現都可以作為事件的潛在原因進行檢查。有關這些潛在原因的資訊會新增至未預期事件的「事件」詳細資訊頁面。有了這些部署和變更的相關資訊，回應者不需要手動搜尋此資訊。這樣可以減少評估潛在原因所需的時間，從而減少從事件復原 (MTTR) 的平均時間。

目前，事件管理員支援從以下兩個方面收集發現項目AWS 服務：AWS CodeDeploy和 AWS CloudFormation

發現項目是一項選擇加入功能。您可以在 [準備好] 精靈、第一次上線至事件管理員時，或稍後在 [設定] 頁面上啟用此功能。

當您啟用「發現項目」功能時，「事件管理員」會為您建立服務角色。此服務角色包含從 CodeDeploy 和擷取發現項目所需的權限 CloudFormation。

若要在跨帳戶案例中使用發現項目，請在管理帳戶中啟用此功能。之後，AWS Resource Access Manager(AWS RAM) 組織中的每個應用程式帳戶都必須建立對應的服務角色。

請參閱下列主題，以協助您使用「發現項目」功能。

主題

- 啟用並建立發現項目的服務角色
- 設定跨帳戶發現項目支援的權限

啟用並建立發現項目的服務角色

當您啟用「發現項目」功能時，「事件管理員」會建立代表您命名`IncidentManagerIncidentAccessServiceRole`的服務角色。此服務角色提供事件管理員在建立事件時所需的權限，以收集有關 CodeDeploy 部署和 CloudFormation 堆疊更新的資訊。

> **Note**
>
> 如果您在組織中使用事件管理員，則會在管理帳戶中建立服務角色。若要使用組織中其他帳戶的發現項目，必須在每個應用程式帳戶中建立服務角色。如需使用 CloudFormation 範本在應用程式帳戶中建立此角色的相關資訊，請參閱中的步驟 4 設定和設定跨帳戶事件管理。

此服務角色與AWS受管理的策略相關聯。如需有關此原則中權限的資訊，請參閱AWS 受管理的策略：AWSIncidentManagerIncidentAccessServiceRolePolicy。

如需在事件管理員上線程序期間啟用發現項目的相關資訊，請參閱開始使用事件管理員。

如需在完成上架程序之後啟用發現項目的相關資訊，請參閱管理發現項目功能。

設定跨帳戶發現項目支援的權限

若要在中設定組織的帳戶間使用「發現項目」功能AWS RAM，每個應用程式帳戶都必須為事件管理員設定權限，才能代表其擔任管理帳戶的服務角色。

這些權限可以在應用程式帳戶中設定，方法是部署由提供的AWS CloudFormation範本AWS，以建立角色`IncidentManagerIncidentAccessServiceRole`。

如需有關在應用程式帳戶中下載和部署此範本的詳細資訊，請參閱中的步驟 4 事件管理員中的跨區域和跨帳戶事件管理。

在事件管理員中建立事件

事件管理員這項功能可協助您管理並快速回應事件。AWS Systems Manager您可以將 Amazon CloudWatch 和 Amazon 設定 EventBridge 為根據 CloudWatch警示和 EventBridge 事件自動建立事件。您也可以在事件清單頁面上手動建立事件，或使用AWS CLI或AWS SDK 中的 StartIncidentAPI 動作來建立事件。事件管理員會將從相同 CloudWatch 警示或事件建立的 EventBridge 事件刪除重複資料至相同的事件。

針對 CloudWatch 警示或事件自動建立的 EventBridge 事件，事件管理員會嘗試建立與事件規則或警示 AWS 區域相同的事件。如果「事件管理員」無法在中使用AWS 區域， CloudWatch 或在複製組中指定的其中一個可用區域中 EventBridge 自動建立事件。如需詳細資訊，請參閱事件管理員中的跨區域和跨帳戶事件管理。

當系統建立事件時，「事件管理員」會自動收集事件所涉及AWS資源的資訊，並將此資訊新增至「相關項目」標籤。如果您在回應計畫中指定了 runbook，當系統建立事件時，事件管理員可以將事件所涉及的AWS資源的資訊傳送至 runbook。然後，系統可以在啟動 runbook 並嘗試修復問題時鎖定這些資源。

系統在建立事件時，它也會在中建立父操作項目 (OpsItem) OpsCenter，它是 Systems Manager 的元件，並將事件連結為相關項目。您可以使用此功能 OpsItem 來追蹤相關工作和 future 事件分析。呼叫 OpsCenter 招致費用。如需有關 OpsCenter 定價的詳細資訊，請參閱 Systems Manager 定價。

> **Important**
>
> 請注意以下重要詳細資訊。
>
> - AWS 區域如果無法使用事件管理員，則只有在您的複製組中至少指定兩個區域時，系統才能容錯移轉並在其他地方建立事件。如需有關配置複製組的資訊，請參閱開始使用事件管理員。
> - 跨區域容錯移轉所建立的事件不會叫用回應計畫中指定的 Runbook。

使用 CloudWatch 警示自動建立事件

CloudWatch 使用您的 CloudWatch 指標來提醒您環境中的變更，並自動執行啟動事件動作。CloudWatch 與 Systems Manager 和事件管理員合作，在警報進入警報狀態時，從響應計劃模板創建事件。這需要下列先決條件：

- 事件管理員已設定並建立複製組。此步驟會在您的帳戶中建立事件管理員服務連結角色，並提供必要的權限。
- 設定的事件管理回應計劃。若要瞭解如何設定事件管理員回應計劃，請參閱在事件管理員中使用回應計劃本指南的事件準備一節。
- 設定 CloudWatch 監控應用程式的指標。如需監控最佳做法，請參閱本指南的事件準備一節監控中的。

使用「開始事件」動作建立警示

1. 在中建立警示 CloudWatch。如需詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南中的使用 Amazon CloudWatch 警示。
2. 選擇要執行的警示動作時，請選取「新增 Systems Manager」動作。
3. 選擇建立未預期事件，然後選取此事件的回應計劃。
4. 完成所選鬧鐘類型指南中的剩餘步驟。

> **Tip**
>
> 您也可以將建立事件動作新增至任何現有警示。

利用事件自動建立 EventBridge 事件

EventBridge 規則會監視事件模式。如果事件符合定義的模式，事件管理員會使用所選的回應計劃建立事件。

使用 SaaS 合作夥伴事件建立事件

您可以設定為接收 EventBridge 來自軟體即服務 (SaaS) 合作夥伴應用程式和服務的事件，以便進行第三方整合。設定 EventBridge 為接收來自第三方合作夥伴的事件後，您可以建立符合合作夥伴事件的規則，以建立事件。若要查看第三方整合清單，請參閱從 SaaS 合作夥伴接收事件。

設定 EventBridge 為接收來自 SaaS 整合的事件。

1. 在以下位置打開亞馬遜 EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇 Partner event sources (合作夥伴事件來源)。

3. 使用搜尋列尋找您想要的合作夥伴，然後選擇 [為該合作夥伴設定]。
4. 選擇 Copy (複製)，將您的帳戶 ID 複製到剪貼簿。

> **Note**
>
> 若要與 Salesforce 整合，請使用亞馬遜使用 AppFlow 者指南中所述的步驟。

5. 前往合作夥伴的網站，並依照指示建立合作夥伴事件來源。請對此使用您的帳戶 ID。您建立的事件來源僅適用於您的帳戶。
6. 返回 EventBridge 主控台，然後在導覽窗格中選擇 [合作夥伴事件來源]。
7. 選取合作夥伴事件來源旁邊的按鈕，然後選擇 Associate with event bus (與事件匯流排建立關聯)。

建立由 SaaS 合作夥伴的事件觸發的規則

1. 在以下位置打開亞馬遜 EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇 Rules (規則)。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的名稱和描述。

   在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。
5. 對於活動匯流排，請選擇與此合作夥伴對應的活動匯流排。
6. 針對 Rule type (規則類型) 選擇 Rule with an event pattern (具有事件模式的規則)。
7. 選擇 下一步。
8. 對於事件來源，請選擇AWS事件或 EventBridge 合作夥伴事件。
9. 對於事件模式，選擇事件模式表單。
10. 對於事件來源，選擇EventBridge合作夥伴
11. 如果是合作夥伴，請選擇合作夥伴的名稱。
12. 針對 Event type (事件類型)，選擇 All Events (所有事件) 或選擇要用於此規則的事件類型。如果您選擇 All Events (所有事件)，此合作夥伴事件來源發出的所有事件都將符合規則。

    如果您想要自訂事件模式，請選擇 Edit (儲存)。
13. 選擇 下一步。
14. 針對 [選取目標]，選擇 [事件管理員] 回應計劃，然後選擇 [回應計劃]。

> **Note**
>
> 選取回應計劃時，您擁有且已與帳戶共用的所有回應計劃都會顯示在 [回應計劃] 下拉式清單中。

15. EventBridge 可建立執行您的規則所需的 IAM 角色：
    - 若要自動建立 IAM 角色，請選擇 Create a new role for this specific resource (為此特定資源建立新角色)。
    - 若要使用您之前建立的 IAM 角色，請選擇 Use existing role (使用現有角色)。
16. 選擇 下一步。
17. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 標籤。
18. 選擇 下一步。
19. 檢閱規則，然後選擇 [建立規則]。

使用AWS服務事件建立事件

EventBridge 也會從「支援AWS服務的事件」中列出的AWS服務接收事件。與為 SaaS 合作夥伴設定規則的方式類似，您可以針對AWS服務進行設定。

建立由AWS服務事件觸發的規則

1. 在以下位置打開亞馬遜 EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇 Rules (規則)。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的名稱和描述。

   在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。
5. 針對 Event bus (事件匯流排) 選擇 default (預設值)。
6. 針對 Rule type (規則類型) 選擇 Rule with an event pattern (具有事件模式的規則)。
7. 選擇 下一步。
8. 對於事件來源，請選擇AWS事件或 EventBridge 合作夥伴事件。
9. 對於事件模式，選擇事件模式表單。

10. 在 Event source (事件來源) 欄位中，選擇 AWS services (服務)。
11. 針對「服務名稱」，選擇用於監控事件的服務。
12. 針對 Event type (事件類型)，選擇 All Events (所有事件) 或選擇要用於此規則的事件類型。如果您選擇 All Events (所有事件)，此合作夥伴事件來源發出的所有事件都將符合規則。

    如果您想要自訂事件模式，請選擇 Edit (儲存)。
13. 選擇 下一步。
14. 針對 [選取目標]，選擇 [事件管理員] 回應計劃，然後選擇 [回應計劃]。

    > **Note**
    >
    > 選取回應計劃時，您擁有且已與帳戶共用的所有回應計劃都會顯示在 [回應計劃] 下拉式清單中。

15. EventBridge 可建立執行您的規則所需的 IAM 角色：

    - 若要自動建立 IAM 角色，請選擇 Create a new role for this specific resource (為此特定資源建立新角色)。
    - 若要使用您之前建立的 IAM 角色，請選擇 Use existing role (使用現有角色)。
16. 選擇 下一步。
17. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的 Amazon EventBridge 標籤。
18. 選擇 下一步。
19. 檢閱規則，然後選擇 [建立規則]。

手動建立事件

回應者可以使用預先定義的回應計劃，使用事件管理員主控台手動追蹤事件。使用下列步驟來建立事件。

1. 開啟「事件管理員」主控台。
2. 選擇 [開始事件]。
3. 針對「回應計劃」，請從清單中選擇回應計劃。
4. (選擇性) 若要覆寫已定義回應計劃所提供的標題，請輸入「事件」標題。
5. (選擇性) 若要覆寫已定義回應計劃所提供的影響，請輸入事件的影響。

追蹤事件管理員中的事件

AWSSystems Manager 事件管理員會追蹤您的事件，從偵測到的那一刻到解決問題，以及透過事件後分析。您可以在「事件管理員」主控台的「事件清單」頁面上找到所有未預期事件，並提供事件詳細資料的直接連結。

主題

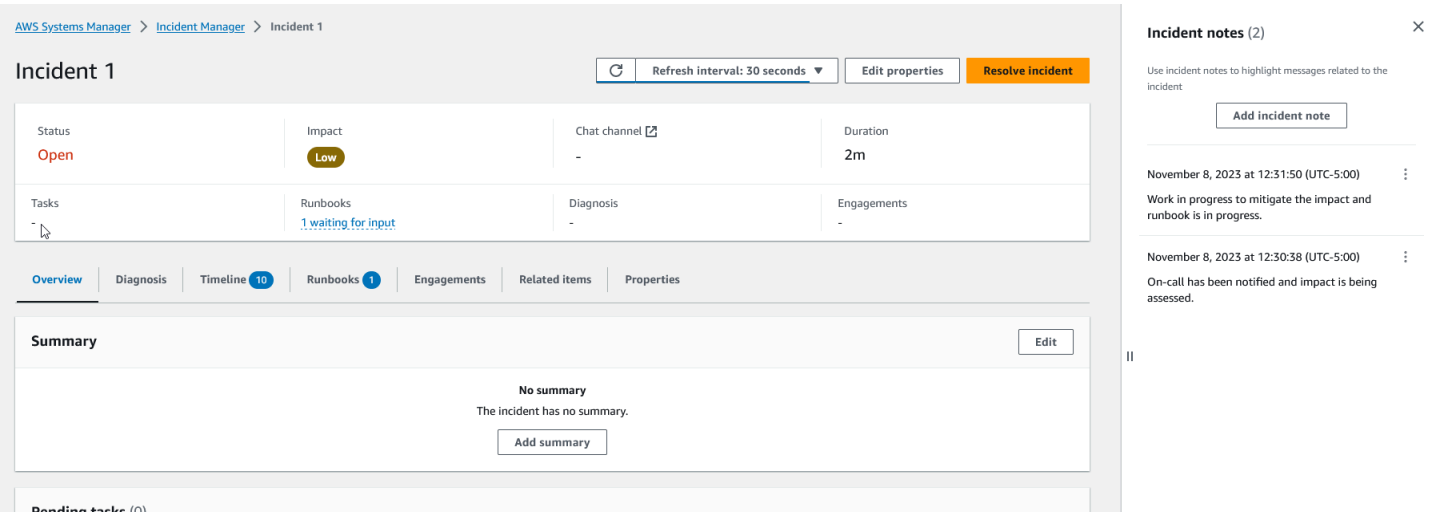
事件清單

「未預期事件清單」頁面包含三個段落：未預期事件、已解決的事件和分析。您可以從此頁面手動追蹤新事件並建立分析。若要深入瞭解如何手動追蹤事件，請參閱手動建立事件本指南的「事件建立」一節。若要瞭解事件後分析，請參閱本指南在事件管理員中執行事件後分析章節。

事件詳細資料會以圖標形塊顯示未決事件，其中包含該事件的標題、影響力、持續時間和聊天頻道。解決事件之後，它會移至「已解決的事件」清單。分析位於第二個標籤中。

事件詳情

「事件詳細資料」頁面提供詳細的見解和工具，讓您用來管理事件。從此頁面，您可以啟動 Runbook 以減輕事件、新增事件備註、使用其他解析程式，以及檢視事件詳細資料，例如時間表、指標、屬性和相關資源。「未預期事件詳細資訊」頁面包含下列段落：頂端橫幅、未預期事件注意事項以及七個包含其他資訊和資源的標籤。依照預設，「頂端」橫幅和「未預期事件備註」區段都會顯示在所有「未預期事件」



本主題說明「未預期事件」詳細資訊頁面的元素，以及您可以從此頁面執行的動作。

頂部橫幅

每個事件詳細資訊頁面上的頂端橫幅包含下列資訊：

- 狀態 — 事件的目前狀態可以是「開啟」或「已解決」。
- 影響 — 事件對您環境的影響。它可以是高，中和低。若要變更未預期事件的影響，請選擇編輯特性。
- 聊天頻道 — 存取聊天頻道的連結，您可以在其中檢視事件更新和通知。
- 持續時間 — 回應者解決事件之前所耗費的時間量。
- Runbook — 與此事件相關聯之執行手冊的狀態。狀態可以是等待輸入、成功或失敗。如果 Runbook 的狀態正在等待輸入，您可以選取 runbook 來檢視動作詳細資訊。您可以選取「未成功」來檢視「逾時」、「失敗」或「已取消」的 Runbook。
- 參與次數 — 參與總數以及每個參與的狀態。當您建立參與時，其狀態為「已參與」。一旦您確認參與，狀態會從「已參與」變更為「已確認」。事件管理員不支援第三方參與的確認。此類活動仍保持在「已參與」狀態。

您可以選擇橫幅右上角的 [編輯]，以編輯事件標題、影響力和聊天頻道。

事件備註

畫面右側會顯示「事件備註」區段。有了備忘錄，您就可以與處理事件的其他使用者共同作業並進行通訊。您可以說明您套用的緩和措施、您識別的潛在根本原因，或事件的目前狀態。最佳做法是使用「事

件備註」區段來張貼狀態更新，以及您或其他人對事件所採取的動作。如果您需要與其他解析器即時通訊，請使用事件管理員中提供的聊天頻道。

若要新增備註，請選擇 [新增事件備註] 按鈕，然後輸入您的備註。附註可以包含有關事件狀態的更新，或任何其他可讓其他使用者看見的相關資訊。如有需要，您也可以編輯或刪除未預期事件備註。

> **Note**
>
> 任何具有 IAM 權限執行`ssm-incidents:UpdateTimelineEvent`和`ssm-incidents:DeleteTimelineEvent`動作的使用者都可以編輯和刪除備註。不過，當您與其他帳號共用事件時，資源策略不會包含該`ssm-incidents:DeleteTimelineEvent`動作。這樣可以防止您與之共用事件的使用者刪除備註。您可以從主控台中的「事件管理員」事件檢視備註的稽核記AWS CloudTrail錄。

標籤

事件詳細資料頁面有七個標籤，可讓回應者更輕鬆地在事件期間尋找及檢視資訊。索引標籤會在索引標籤名稱中顯示計數器，表示索引標籤的更新次數。如需有關每個索引標籤內容以及可用動作的詳細資訊，請繼續閱讀。

概要

[概觀] 索引標籤是回應者的登陸頁面。它包含事件摘要、最近時間表事件的清單，以及目前的 runbook 步驟。

回應者會使用「摘要」來 catch 蹤已採取的動作、任何變更的結果、可能的後續步驟，以及事件影響的相關資訊。若要更新摘要，請選擇「摘要」區段右上角的「編輯」。

> **Important**
>
> 如果有多位回應者同時編輯摘要欄位，提交編輯的回應者最後會覆寫所有其他輸入。

「最近的時間表事件」區段包含事件管理員填入的時間表，其中包含五個最近的事件。您可以在此段落瞭解事件的狀態以及最近發生的情況。若要檢視完整的時間軸，請繼續前往「時間軸」標籤。

概觀頁面也會顯示目前的 Runbook 步驟。此步驟可能是在您的AWS環境中執行的自動步驟，也可能是回應者的一組手動指示。若要檢視完整的 Runbook (包括先前和未來的步驟)，請選擇 Runbook 索引標籤。

診斷

診斷索引標籤包含AWS代管應用程式和系統的重要資訊，包括指標的相關資訊，以及發現項目 (如果啟用)。

使用量度

事件管理員使 CloudWatch 用 Amazon 填入此索引標籤上的指標和警示圖表。若要進一步了解事件管理定義警示和指標的最佳作法，請參閱監控本使用者指南的「事件規劃」一節。

若要新增量度

- 選擇此標籤右上角的「新增」。
  - 若要從現有 CloudWatch 儀表板新增量度，請選擇「從現有 CloudWatch 儀表板」。
    a. 選擇儀表板。這會新增屬於所選儀表板一部分的所有量度和警示。
    b. (選擇性) 您也可以從儀表板選取量度以檢視特定量度。
  - 選取從 CloudWatch並貼上測量結果來源，以新增單一測量結果。若要複製測量結果來源：
    a. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
    b. 在導覽窗格中，選擇 指標。
    c. 在「所有量度」標籤上，在搜尋欄位中輸入搜尋詞彙 (例如測量結果名稱或資源名稱)，然後選擇 Enter。

       例如，如果您搜尋指標，您會看到與此`CPUUtilization`量度相關聯的命名空間和維度。
    d. 從搜尋中選擇其中一個結果以檢視指標。
    e. 選擇「來源」頁標並複製來源。

測量結果警示圖表只能透過相關回應計劃新增至事件詳細資訊，或在新增測量結果時選取「從現有CloudWatch儀表板」。

若要移除量度，請選擇 [移除]，然後從提供的量度下拉式清單中選擇要移除的量度。

檢視AWS CodeDeploy與的發現項目 AWS CloudFormation

啟用「發現項目」並設定所有必要權限之後，任何可能與特定事件相關的發現項目都會附加至事件。回應者可以在「事件詳細資料」頁面上檢視這些發現項目的相關資

若要檢視來源 CodeDeploy 與發現項目 CloudFormation

1. 開啟「事件管理員」主控台。
2. 選擇要調查的事件名稱。
3. 在「診斷」標籤的「發現項目」區域中，比較任何已報告發現項目的開始時間與事件的開始時間。
4. 若要檢視有關發現項目的更多詳細資訊，請在「參考」欄中選擇 CodeDeploy或 CloudFormation 發現項目的連結。

時間表

使用時間軸索引標籤來追蹤事件期間發生的事件。事件管理員會自動填入時間表事件，以識別事件發生期間的重大事件。回應者可以根據手動偵測到的事件來新增自訂事件。在事件後分析期間，「時間表」標籤會提供寶貴的見解，讓您瞭解如何更有效地準備和回應 future 的事件。如需事件後分析的更多資訊，請參閱在事件管理員中執行事件後分析。

若要新增自訂時間軸事件，請選擇 [新增]。使用行事曆選取日期，然後輸入時間。所有時間均以您當地的時區顯示。提供時間表中顯示之事件的簡短描述。

若要編輯現有的自訂事件，請在時間軸上選取事件，然後選擇 [編輯]。您可以變更自訂事件的時間、日期和描述。您只能編輯自訂事件。

手冊

事件詳細資料頁面的 [Runbook] 索引標籤是回應者可以在其中檢視 Runbook 步驟並啟動新的 Runbook。

若要啟動新的 Runbook，請選擇 [R unbook] 區段中的 [開始手冊]。使用搜尋欄位來尋找您要啟動的 Runbook。提供任何必要的參數和要啟動 runbook 時使用的 runbook 的版本。從 Runbook 索引標籤發生事件期間啟動的 Runbook 會使用目前登入帳戶的權限。

若要導覽至 Systems Manager 中的 Runbook 定義，請在 Runbook 下選擇工作手冊的標題。若要瀏覽至 Systems Manager 中的 runbook 執行個體，請在 [執行詳細資料] 下選擇執行詳細資料。這些頁面會顯示用來啟動 runbook 的範本，以及目前執行中的自動化文件執行個體的特定詳細資訊。

Runbook 步驟區段會顯示所選 Runbook 自動執行或回應者手動執行的步驟清單。步驟會隨著步驟成為目前步驟而展開，顯示完成步驟所需的資訊，或是步驟作業的詳細資訊。自動化完成後，自動執行手冊步驟解析。手動步驟要求回應者選擇每個步驟底部的 [下一步]。步驟完成後，步驟輸出會顯示為下拉式清單。

若要取消 Runbook 執行，請選擇 [取消手冊]。這將停止 runbook 的執行，並沒有完成在 runbook 中的任何進一步的步驟。

參與

事件詳細資料的「參與」標籤可促進回應者和團隊的參與度。在此標簽中，您可以查看誰已經參與，誰已經回應，以及哪些響應者將作為升級計劃的一部分參與。回應者可以直接從此標籤與其他連絡人互動。要了解有關創建聯系人和升級計劃的更多信息，請參閱本指南的在事件管理員中使用連絡人和在事件管理員中使用升級計劃各節。

您可以設定包含聯絡人和升級計畫的回應計劃，以便在事件開始時自動開始互動。若要進一步瞭解如何設定回應計劃，請參閱本指南在事件管理員中使用回應計劃章節。

您可以在表中找到有關每個聯繫人的信息。此表格包含下列資訊：

- 名稱 — 連結至連絡人詳細資料頁面，該頁面會顯示其聯絡方式和參與計劃。
- 升級計劃 — 鏈接到參與聯繫人的升級計劃。
- 連絡人來源 — 識別參與此連絡人的服務，例如AWS Systems Manager或 PagerDuty。
- 已參與 — 顯示計劃何時與聯絡人互動，或何時與某位連絡人作為升級計劃的一部分互動。
- 已確認 — 顯示連絡人是否確認參與。

若要確認參與，回應者可以執行下列其中一項作業：

- 電話 — 出現提示**1**時輸入。
- SMS — 使用提供的代碼回覆訊息，或在事件的「參與」標籤上輸入提供的代碼。
- 電子郵件 — 在事件的「參與」標籤上輸入提供的代碼。

相關項目

[相關項目] 索引標籤可用來收集與事件緩解相關的資源。這些資源可以是 ARN、外部資源的連結或上傳到 Amazon S3 儲存貯體的檔案。此表格會顯示描述性標題以及 ARN、連結或值區詳細資訊。在使用 S3 儲存貯體之前，請參閱 Amazon S3 使用者指南中的 Amazon S3 安全最佳實務。

將檔案上傳到 Amazon S3 儲存貯體時，該儲存貯體上的版本控制會啟用或暫停。在值區上啟用版本控制後，上傳的檔案名稱與現有檔案相同，會新增為檔案的新版本。如果版本控制暫停，上傳的檔案與現有檔案名稱相同，會覆寫現有檔案。若要進一步了解版本控制，請參閱 Amazon S3 使用者指南中的在 S3 儲存貯體中使用版本控制。

移除檔案相關項目時，檔案會從事件中移除，但不會從 Amazon S3 儲存貯體中移除。若要進一步了解如何從 Amazon S3 儲存貯體移除物件，請參閱 Amazon S3 使用者指南中的刪除 Amazon S3 物件。

屬性

「特性」頁籤提供下列有關未預期事件的詳細資訊。

您可以在「未預期事件特性」段落中檢視下列項目：

- 狀態 — 描述事件的目前狀態。事件可以是「開啟」或「已解決」。
- 開始時間 — 在「事件管理員」中建立事件的時間。
- 解決時間 — 在「事件管理員」中解決事件的時間。
- Amazon 資源名稱（ARN）— 事件的 ARN。從聊天或 by AWS Command Line Interface (AWS CLI) 命令引用事件時，請使用 ARN。
- 回應計劃 — 識別所選未預期事件的回應計劃。選擇回應計劃會開啟回應計劃的詳細資訊頁面。
- 父項 OpsItem — 將 OpsItem建立的物件識別為事件的父項。父項 OpsItem 可以有多個相關事件和後續行動項目。選取父項會在中 OpsItem開啟 OpsItems 詳細資訊頁面 OpsCenter。
- 分析 — 識別從此事件建立的分析。從已解決的事件建立分析，以改善您的事件回應程序。選擇分析以開啟「分析詳細資訊」頁面。
- 「所有者」— 在其中創建事件的帳戶。

在「標籤」區段中，您可以檢視和編輯與事件記錄相關聯的標籤鍵和值。如需事件管理員中標籤的詳細資訊，請參閱標記事件管理員中的資源。

在事件管理員中執行事件後分析

發佈事件分析會引導您找出事件回應的改進措施，包括偵測和緩解的時間。分析還可以幫助您了解事件的根本原因。事件管理員建立建議的行動項目，以改善您的事件回應。

事件後分析的優點

- 改進事件回應
- 瞭解問題的根本原因
- 解決可傳送作業行動項目的根本原因
- 分析事件的影響
- 在組織內捕捉和分享學習

什麼不使用分析

分析是無可指責的，不會以名字呼喚人們。

「無論我們發現什麼，我們都了解並真正相信每個人都會做到最好的工作，考慮到他們當時所知道的，他們的技能和能力，可用的資源以及手頭的情況。」 -規範克斯，項目回顧：團隊審查手冊

分析詳細

分析詳細資訊頁面會引導您完成收集資訊、評估改進和建立行動項目。「分析詳細資訊」頁面與事件詳細資訊類似，但有一些主要差異，例如歷史測量結果、可編輯的時間表，以及改善 future 事件的問題。

概要

概觀是事件的摘要。此摘要包括背景、發生的情況、發生的原因、如何緩解、持續時間和重要行動項目，以防止事件再次發生。概述是高層次的。您將在分析的 [問題] 索引標籤中探索更多詳細資訊。

指標

使用指標索引標籤，以視覺化方式呈現事件期間應用程式中的關鍵指標。您可以在此處新增度量圖表，其中包含在相同圖表中描述一或多個量度。此索引標籤會自動填入事件期間使用的測量結果。我們建議您在事件期間新增關鍵時間點的說明、標題和註解。

分析量度圖表時可以考慮的一些關鍵時間點：

- 部署變更
- 組態變更
- 事件開始時間
- 鬧鈴時間
- 參與時間
- 緩解措施開始
- 事件解決時間

限制

- CloudWatch 警示和量度運算式不會從事件匯入。
- 事件管理員不支援的區域中的量度不會從事件匯入。
- 應用程式帳戶中的量度需要`CloudWatch-CrossAccountSharingRole`先設定，才能建立分析。如需角色的詳細資訊，請參閱 CloudWatch 使用手冊中的跨帳戶跨區域 CloudWatch 主控台。

時間表

當您深入了解事件時，請描述時間軸上的關鍵時間點。事件時間表會自動填入此索引標籤中。您可以刪除與分析無關的時間點。您也可以新增和編輯時間點，以更準確地描述事件及其影響。

使用時間軸標籤來回答您在「問題」標籤中找到的有關事件回應的問題。

問題

使用事件管理員問題來縮短解決應用程式中事件的時間，並減少事件的發生。回答問題時，請更新「量度」和「時間軸」標籤以確保準確性。問題集中在事件回應的這些關鍵方面：

- 偵測 — 您能縮短偵測時間嗎？ 是否有更新的指標和警報可以更快地檢測到事件？
- 診斷 — 您可以改善診斷時間嗎？ 您的響應計劃或升級計劃是否有更新可以更快地吸引正確的響應者？
- 緩解 — 您可以縮短緩解的時間嗎？ 是否有 runbook 步驟，你可以添加或改進？
- 預防 — 您可以防止 future 發生事件嗎？ 為了發現事件的根本原因，Amazon 在問題調查中使用 5 為什麼方法。

動作

事件管理員會建立建議的行動項目，供您在完成問題時檢閱。您可以選擇從此標籤接受並完成這些動作，也可以關閉這些動作。您可以選擇「已關閉的行動項目」來檢閱已關閉的行動項目。行動項目是連結至中 OpsItem 的分析和未預期事件的一種類型 OpsCenter。

清單

在結束分析之前，請使用檢查清單來檢閱回應者應採取的動作。當回應者完成檢查清單中的動作時，動作旁邊的圖示會從橢圓形變更為核取記號，表示動作已完成。如果您尚未完成檢查清單項目，事件管理員會顯示一則訊息，以確認回應者想要關閉分析而不完成分析。

分析模板

分析範本提供了一組深入探討事件根本原因的問題。您可以使用這些問題的答案來改善應用程式效能和事件回應。

AWS標準範本

事件管理員根據AWS事件回應和問題分析最佳做法 (標題為)，提供標準的問題範本`AWSIncidents-PostIncidentAnalysisTemplate`。

建立分析範本

我們建議您使用預設`AWSIncidents-PostIncidentAnalysisTemplate`範本，並新增適合您使用案例的其他問題或區段。根據預設範本建立分析範本使用此範本作為起點，在您的管理帳戶中建立分析範本。然後，您可以將分析範本複製到啟用事件管理員的每個區域。

建立分析範本

1. 呼叫動`GetDocument`作並使用其`Name`參數進行下載`AWSIncidents-PostIncidentAnalysisTemplate`。如需有關`GetDocument`語法的詳細資訊，請參閱 Systems Manager API 參考。
2. 回應中的內容包含用於分析的 JSON 建置區塊。使用問題建置區塊在分析中插入其他問題。我們建議您在區段中新增問題或`Incident questions`區段。
3. 若要建立新範本，請搭配上一個步驟中已更新的 JSON 使用此`CreateDocument`作業。您必須包括以下內容，其中*`Analysis_Template_Name`*是模板的名稱，

   - `DocumentFormat: "JSON"`

- DocumentType: "ProblemAnalysisTemplate"
- Name: "*Analysis_Template_Name*"

建立分析

1. 若要建立分析，請從已關閉未預期事件的事件詳細資訊頁面中選擇建立分析。
2. 選擇要從中建立此分析的分析範本，然後輸入分析的描述性名稱。
3. 選擇 建立 。

列印格式化的事件分析

您可以產生已格式化以供列印之完整或不完整分析的副本。您也可以將此副本儲存為 PDF。您一次可以列印一個分析。目前不支援 Batch 列印。

列印格式化分析的步驟

1. 開啟「事件管理員」主控台。
2. 選擇「分析」頁標。
3. 選擇您要列印的分析標題。
4. 在分析詳細資訊頁面右上角，選擇「列印」。
5. 在 [列印事件分析] 對話方塊中，清除您不想包含在列印版本中的分析區段。依預設，會選取所有區段。
6. 選擇「列印」以開啟裝置的本機列印控制項。
7. 選擇列印目的地或格式。您可以選擇本機或網路印表機，也可以將分析儲存為 PDF。如果需要，對其餘列印選項進行任何變更，然後選擇「列印」。

> **Note**
>
> 本地打印控件是指 Web 瀏覽器和設備提供的用戶界面。
> 列印目的地是為您的裝置設定並可從中存取的目的地。

事件管理器教學

這些 AWS Systems Manager 事件管理員教學課程可協助您建置更強大的事件管理系統。這些教學課程涵蓋事件或支援事件回應期間發生的常見活動。

主題

搭配事件管理員使用系統管理員自動化手冊

您可以使用AWS Systems Manager 自動化執行手冊來簡化 AWS 服務的常見維護、部署和補救工作。在本教程中，您將創建自定義 runbook 以自動在事件管理器中的事件響應。本教學的案例涉及指派給 Amazon EC2 指標的亞馬遜 CloudWatch 警示。當執行個體進入觸發警示的狀態時，事件管理員會自動執行下列工作：

1. 在事件管理員中建立事件。
2. 起始嘗試修復問題的 runbook。
3. 將 runbook 結果發佈至「事件管理員」中的事件詳細資訊頁面。

本教學中描述的程序也可以搭配 Amazon EventBridge 事件和其他類型的 AWS 資源使用。藉由自動化您對警示和事件的補救回應，您可以減少事件對組織及其資源的影響。

本教學說明如何針對事件管理員回應計劃編輯指派給 Amazon EC2 執行個體的 CloudWatch 警示。如果您沒有設定警示、執行個體或回應計劃，建議您在開始之前先設定這些資源。如需詳細資訊，請參閱下列主題：

- 在 Amazon 用 CloudWatch 戶指南中使用 Amazon CloudWatch 警報
- Amazon EC2 用戶指南中的 Amazon EC2 實例
- Amazon EC2 用戶指南中的 Amazon EC2 實例
- 在事件管理員中使用回應計劃

> **Important**
>
> 您將通過創建 AWS 資源和使用 runbook 自動化步驟產生成本。如需詳細資訊，請參閱 AWS 定價。

主題

任務 1：創建工作手冊

請使用下列程序，在 Systems Manager 主控台中建立 Runbook。從事件管理員事件叫用時，runbook 會重新啟動 Amazon EC2 執行個體，並使用有關執行手冊執行的資訊更新事件。在開始之前，請確認您具有建立 runbook 的權限。如需詳細資訊，請參閱《AWS Systems Manager 使用指南》中的〈設定自動化〉。

> **Important**
>
> 檢閱下列有關建立此教學課程 runbook 的重要詳細資料：
>
> - 該 runbook 是用於從 CloudWatch 警報源創建的事件。如果您將此 runbook 用於其他類型的事件 (例如手動建立的事件)，則不會在第一個 runbook 步驟中找到時間軸事件，而且系統會傳回錯誤。
> - runbook 要求 CloudWatch 報警包括一個名為`InstanceId`的尺寸。Amazon EC2 執行個體指標的警示具有此維度。如果您使用此 runbook 與其他度量 (或與其他事件來源，如 EventBridge)，然後您必須變更`JsonDecode2`步驟，以符合您的案例中擷取的資料。
> - 執行手冊嘗試透過重新啟動 Amazon EC2 執行個體來修復觸發警示的問題。對於真正的事件，您可能不想重新啟動執行個體。使用您希望系統採取的特定補救動作來更新 runbook。

若要取得有關建立 Runbook 的更多資訊，請參閱《使用指南》中的〈AWS Systems Manager 使用手冊〉。

建立工作手冊的步驟

1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/
2. 在導覽窗格中，選擇 Documents (文件)。
3. 選擇自動化。
4. 在「名稱」中，輸入工作簿的描述性名稱，例如**IncidentResponseRunbook**。
5. 選擇 Editor (編輯器) 標籤，然後選擇 Edit (編輯)。
6. 將下方內容貼入編輯工具中：

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
 CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
```

```
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
```

```
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. 選擇 Create automation (建立自動化)。

工作 2：建立 IAM 角色

請使用下列教學課程來建立 AWS Identity and Access Management (IAM) 角色，該角色授予事件管理員權限，以隱藏回應計劃中指定的 Runbook。本教學中的執行手冊會重新啟動 Amazon EC2 執行個體。當您將 runbook 連接到您的回應計畫時，您將在下一個任務中指定此 IAM 角色。

建立 IAM 角色，從回應計畫隱藏工作流程簿

1. 在以下網址開啟 IAM 主控台：https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
3. 在 [信任的實體類型] 下，確認已選取AWS 服務。
4. 在 [使用案例] 下的 [其他 AWS 服務使用案例] 欄位中，輸入**Incident Manager**。
5. 選擇事件管理員，然後選擇下一步。
6. 在 [新增權限] 頁面上，選擇 [建立原則]。權限編輯器將在新的瀏覽器窗口或選項卡中打開。
7. 在編輯器中，選擇 JSON 索引標籤。
8. 將以下權限原則複製並貼到 JSON 編輯器中。用您的 ID 替換*## ID* AWS 帳戶 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
```

```
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
        }
    ]
}
```

9. 選擇下一步：標籤。
10. (選擇性) 如有需要，請將標籤新增至您的原則。
11. 選擇下一步：檢閱。
12. 在「名稱」欄位中，輸入可協助您識別此角色用於此教學課程的名稱。
13. (選擇性) 在「說明」欄位中輸入說明。
14. 選擇建立政策。
15. 切換作業選項至您要建立之角色的瀏覽器視窗或頁標。接著顯示 [新增權限] 頁面。
16. 選擇 [重新整理] 按鈕 (位於 [建立原則] 按鈕旁邊)，然後在篩選方塊中輸入您建立的 perimssions 原則名稱。
17. 選擇您建立的權限原則，然後選擇 [下一步]。
18. 在 [名稱、檢閱和建立] 頁面的 [角色名稱] 中，輸入可協助您識別此角色用於本教學課程的名稱。

19. (選擇性) 在「說明」欄位中輸入說明。
20. 檢閱角色詳細資料、視需要新增標籤，然後選擇 [建立角色]。

任務 3：將 Runbook 連接到您的響應計劃

通過將 runbook 連接到您的事件管理器響應計劃，您可以確保一致，可重複和及時的緩解過程。該 runbook 也作為一個起點為解析器，以確定他們的下一個行動過程。

若要將 Runbook 指派給您的回應計畫

1. 開啟「事件管理員」主控台。
2. 選擇「回應計劃」。
3. 針對「回應計劃」，請選擇現有的回應計劃，然後選擇編輯。如果您沒有現有的回應計劃，請選擇 [建立回應計劃] 以建立新計劃。

   完成下列欄位：

   a. 在 [Runbook] 區段中，選擇 [選取現有的工作手冊]。
   b. 對於「擁有者」，確認已選取「我擁有」。
   c. 對於 Runbook，請選擇您在中建立的工作流程簿。任務 1：創建工作手冊
   d. 對於「版本」，請在執行時選擇「預設」。
   e. 在「輸入」段落中，為 IncidentRecordArn 參數選擇未預期事件 AR N。
   f. 在「執行許可」區段中，選擇您在其中建立的 IAM 角色工作 2：建立 IAM 角色。
4. 儲存您的變更。

工作 4：指派 CloudWatch 警示給您的回應計劃

使用下列程序將 Amazon EC2 執行個體的 CloudWatch 警示指派給您的回應計劃。

若要指派 CloudWatch 警示給您的回應計劃

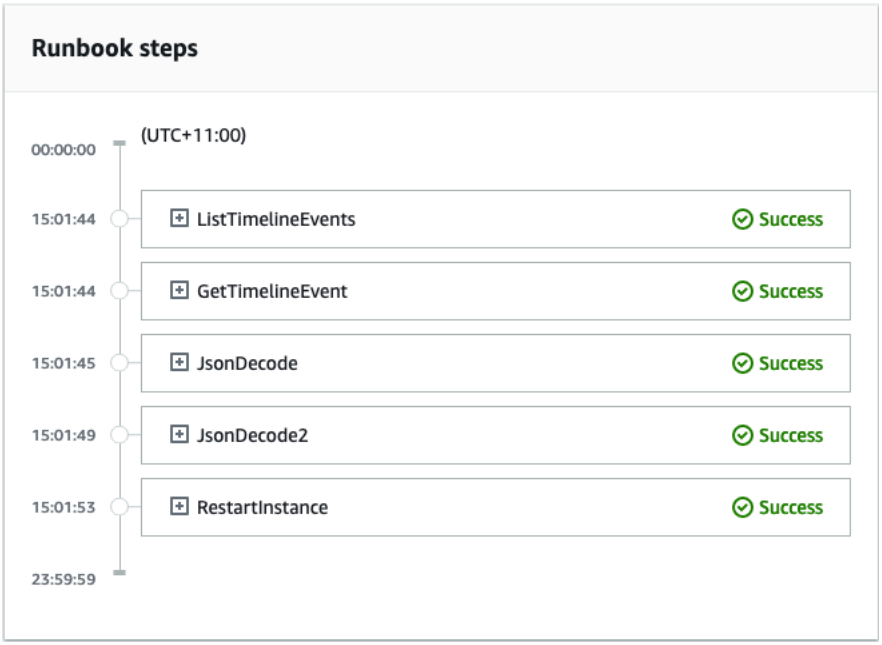
1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在功能窗格的 [警報] 下，選擇 [所有鬧鐘]。
3. 為您要連接到回應計劃的 Amazon EC2 執行個體選擇警示。
4. 選擇動作，然後選擇編輯。確認量度具有名為的維度`InstanceId`。

5. 選擇下一步。
6. 對於 [設定動作精靈]，請選擇 [新增 Systems Manager]
7. 選擇 [建立事件]。
8. 選擇您在中建立的回應計劃任務 3：將 Runbook 連接到您的響應計劃。
9. 選擇 Update alarm (更新警示)。

工作 5：驗證結果

若要驗證 CloudWatch 警示是否建立事件，然後處理您的回應計畫中指定的 runbook，您必須觸發警示。觸發警報和 runbook 完成處理之後，您可以使用下列程序驗證 runbook 的結果。若要取得有關觸發警示的資訊，請參閱《指令參考》中的設定警報狀態。AWS CLI

1. 開啟「事件管理員」主控台。
2. 選擇 CloudWatch 警示所建立的事件。
3. 選擇 [工作手冊] 索引標籤。
4. 在執行手冊步驟區段中檢視在 Amazon EC2 執行個體上執行的動作。以下影像是一個範例，展示您在本自學課程中建立的 runbook 所採取的步驟。每個步驟都會列出時間戳記和狀態訊息。



若要檢視 CloudWatch 警示中的所有詳細資料，請展開 JsonDecode2 個步驟，然後展開 [輸出]。

> **Important**
>
> 您必須清除您在本教學課程中實施的任何資源變更，但您不想保留。這包括 Event Manager 資源的變更，例如資源計劃和事件、 CloudWatch 警示變更，以及您為本教學課程建立的 IAM 角色。

在事件管理員中管理安全事件

您可以使用 AWS Security Hub Amazon EventBridge 和事件管理員一起識別和管理 AWS 託管應用程式中的安全事件。本教學課程會逐步引導您設定 EventBridge 規則，以根據 Security Hub 自動傳送的發現項目來建立事件。

> **Note**
>
> 本教程使用 EventBridge Security Hub。您可能因使用這些服務而產生費用。

必要條件

- 設定 Security Hub。如需詳細資訊，請參閱設定 AWS Security Hub。
- 建立或更新安全中心中的發現項目。如需詳細資訊，請參閱 AWS Security Hub。
- 設定回應計劃，讓事件管理員在建立安全性事件時將用作範本。如需詳細資訊，請參閱 事件管理員中的事件做好準備。

在本自學課程中，我們使用預先定義的樣式來建立 EventBridge 規則。若要使用自訂模式建立規則，請參閱使用指南中的使用自訂模式建立規則。 AWS Security Hub

建立 EventBridge 規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入規則的 Name (名稱) 與 Description (描述)。

   在同一個區域和同一個事件匯流排上，規則不能與另一個規則同名。
5. 針對事件匯流排選擇預設值。

6. 針對規則類型選擇具有事件模式的規則。
7. 選擇下一步。
8. 對於事件來源，請選擇AWS 事件或 EventBridge合作夥伴事件。
9. 針對事件模式，選擇事件模式表單。
10. 在事件來源欄位中，選擇 AWS 服務。
11. 對於AWS 服務，請選擇 Security Hub。
12. 針對「事件類型」，選擇「Security Hub 發現項目-匯入
13. 依預設，設 EventBridge 定不含任何篩選器值的事件模式。針對每個屬性，都會選取「任何###」選項。更新這些篩選器，以根據對環境影響最大的安全性發現項目建立事件。
14. 按一下 Next (下一步)。
15. 在目標類型欄位中，選擇 AWS 服務。
16. 針對 「選取目標」，選擇「事件管理員」回應計劃。
17. 針對「回應計劃」，請選擇要用作已建立事件範本的回應計劃。
18. EventBridge 可以建立規則執行所需的 IAM 角色。
    - 若要自動建立 IAM 角色，請選擇 [為特定資源建立新角色]。
    - 若要使用帳戶中已存在的 IAM 角色，請選擇 [使用現有角色]。
19. (選用) 為規則輸入一或多個標籤。
20. 選擇下一步。
21. 檢閱規則的詳細資訊，然後選擇建立規則。

現在您已建立此 EventBridge 規則，符合您定義之屬性值的安全性發現項目將會在事件管理員中建立事件。您可以對這些事件進行分類、管理、監控和建立事件後分析。

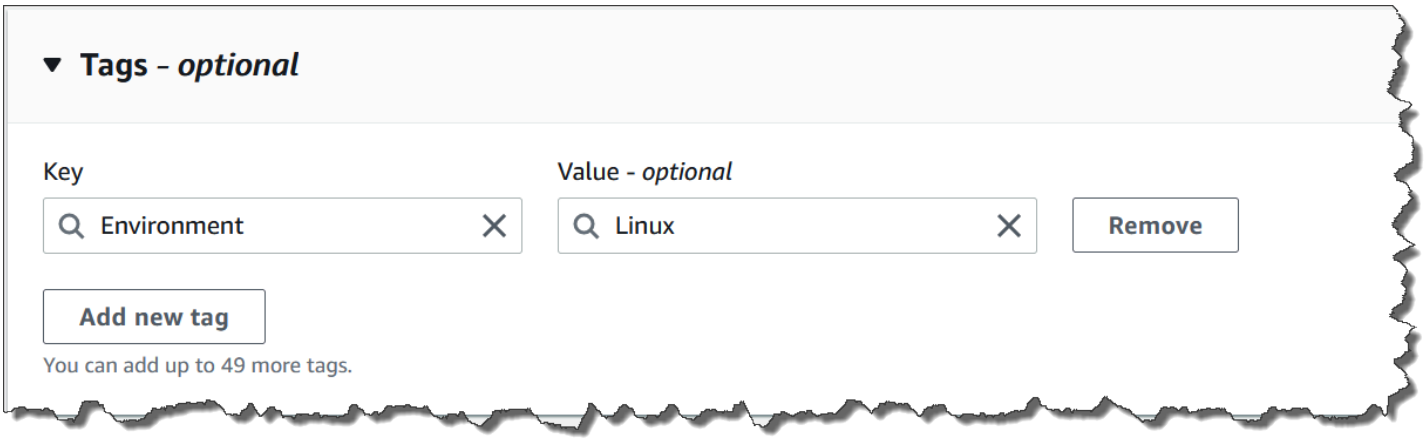
標記事件管理員中的資源

標籤是選擇性地，可指派給複製組中AWS 區域指定的事件管理員資源中的事件管理員資源中的資料。您可以為回應計劃、事件記錄和連絡人指派標籤。您也可以將標籤新增至待命排程和輪換。您也可以將標記新增至複製組本身。標籤可讓您以不同方式來分類與控制這些資源的存取。每個標籤皆包含由您定義的一個金鑰與一個選用值。我們建議您為每種事件管理員資源類型建立符合您需求的標籤金鑰。使用一致的標籤金鑰，可讓您更輕鬆的管理這些資源和管理它們的存取。您可以根據標籤搜尋和篩選資源。如需有關使用標籤控制資源存取的詳細資訊，請參閱 IAM 使用者指南中的使用標籤控制AWS資源的存取。

建立回應計劃時，您可以在「事件預設值」區段中指定標記。使用回應計劃建立事件時，這些標記會套用至事件記錄。

> **Note**
>
> 標籤沒有任何語義意義。它們會嚴格解譯為字元字串。

您可以使用事件管理員主控台新增或移除標籤。下列螢幕擷取畫面顯示建立新回應計劃時的標籤區段。



若要以程式地新增標籤，請使用下列 API 動作：

- TagResource
- UntagResource
- ListTagsForResource

Important

只能從資源擁有者帳號檢視和修改套用至回應計劃、事件記錄、連絡人、待命排程與輪換以及複製組的標籤。

中的安全性 AWS Systems Manager Incident Manager

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護 AWS 服務 中執行的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Systems Manager Incident Manager，請參閱合規計劃的AWS 服務範圍範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用「事件管理程式」時套用共同的責任模型。下列主題說明如何設定事件管理員，以符合安全性和合規性目標。您也會學到如何使用其他協助 AWS 服務 您監控和保護事件管理員資源的其他資源。

主題

事件管理員中的資料保護

AWS 共用責任模型適用於中的資料保護 AWS Systems Manager Incident Manager。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。您也同時負責所使用 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

FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。如此一來，每個使用者都只會獲得授與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：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 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 Amazon S3 的敏感資料。
- 如果 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS如需有關可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

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文字欄位中，例如名稱欄位。這包括當您使用事件管理員或其他 AWS 服務 使用主控台API、 AWS CLI、或時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

根據預設，事件管理員會使用SSL/TLS來加密傳輸中的資料。

資料加密

事件管理員使用 AWS Key Management Service (AWS KMS) 金鑰來加密您的「事件管理員」資源。如需詳細資訊 AWS KMS，請參閱AWS KMS 開發人員指南。 AWS KMS 結合安全、高可用性的硬體和軟體，提供專為雲端擴充的金鑰管理系統。事件管理員會使用您指定的金鑰加密您的資料，並使用 AWS 擁有的金鑰加密中繼資料。若要使用事件管理員，您必須設定複製組，其中包括設定加密。事件管理員需要資料加密才能使用。

您可以使用 AWS 擁有的金鑰來加密複製組，也可以使用您在其中建立的自己的客戶管理金鑰 AWS KMS 來加密複製組中的區域。事件管理員僅支援對稱式加密 AWS KMS 金鑰來加密您在其中 AWS KMS建立的資料。事件管理員不支援包含匯入 AWS KMS 金鑰材料、自訂金鑰存放區、雜湊型訊息驗證碼 (HMAC) 或其他類型金鑰的金鑰的金鑰。如果您使用客戶受管金鑰，您可以使用AWS KMS 主控台或 AWS KMS APIs集中建立客戶受管金鑰，並定義金鑰政策，以控制事件管理員如何使用客戶管理的金鑰。當您透過事件管理員使用客戶管理金鑰進行加密時， AWS KMS 客戶管理金鑰必須與資源位於相同的區域。若要深入瞭解如何在事件管理員中設定資料加密，請參閱準備精靈。

使用 AWS KMS 客戶管理的金鑰需支付額外費用。如需詳細資訊，請參閱AWS Key Management Service 開發人員指南和AWS KMS 定價中的AWS KMS 概念-KMS 金鑰。

> **Important**
>
> 如果您使用客戶管理的金鑰 (CMK) 來加密複製組和事件管理員資料，但稍後決定刪除複製組，請務必在停用或刪除複製組之前先刪除複製組CMK。

若要允許事件管理員使用您的客戶管理金鑰來加密您的資料，您必須在客戶管理金鑰的金鑰政策中新增下列政策聲明。若要深入瞭解如何設定和變更帳戶中的金鑰政策，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的使用金鑰政策。此原則提供下列權限：

- 允許事件管理員執行唯讀操作，以尋找您帳戶中的「CMK事件管理員」。
- 允許事件管理員使CMK用建立授權和描述金鑰，但只有當金鑰代表帳戶中有權使用事件管理員的主體時。如果原則陳述式中指定的主體沒有使用KMS金鑰和使用事件管理員的權限，即使來自事件管理員服務，呼叫也會失敗。

```
    {
    "Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "ssm-incidents.amazonaws.com",
          "ssm-contacts.amazonaws.com"
        ]
      }
    }
  }
```

將`Principal`值取代為建立複製組的IAM主參與者。

事件管理員會在所有要求中使用加密內容來 AWS KMS 進行密碼編譯作業。您可以使用此加密內容來識別事件管理員使用您KMS金鑰的 CloudTrail 記錄事件。事件管理員使用下列加密內容：

- `contactArn=ARN of the contact or escalation plan`

的 Identity and Access Management AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM系統管理員控制誰可以驗證 (登入) 和授權 (有權限) 使用事件管理員資源。IAM是您 AWS 服務 可以免費使用的。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何 AWS Systems Manager Incident Manager 使用 IAM
- AWS Systems Manager Incident Manager的身分型政策範例
- 以資源為基礎的政策範例 AWS Systems Manager Incident Manager
- 事件管理器中的跨服務混淆副預防
- 針對事件管理員使用服務連結角色
- AWS 受管理的政策 AWS Systems Manager Incident Manager
- 疑難排解 AWS Systems Manager Incident Manager 身分和存取

物件

根據您在「事件管理員」中執行的工作， AWS Identity and Access Management (IAM) 的使用方式會有所不同。

服務使用者 — 如果您使用事件管理員服務執行工作，則系統管理員會提供您所需的認證和權限。當您使用更多事件管理員功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取「事件管理員」中的功能，請參閱疑難排解 AWS Systems Manager Incident Manager 身分和存取。

服務管理員 — 如果您負責公司的事件管理員資源，您可能擁有事件管理員的完整存取權。決定您的服務使用者應存取哪些事件管理員功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配事件管理員使用，請參閱如何 AWS Systems Manager Incident Manager 使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理事件管理員存取權限的詳細資料。若要檢視可在中使用的事件管理員身分型原則範例IAM，請參閱。AWS Systems Manager Incident Manager的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，

請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。

- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2實例中存儲訪問密鑰更好。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

如何 AWS Systems Manager Incident Manager 使用 IAM

在您用IAM來管理事件管理員的存取權限之前，請先了解可搭配事件管理員使用哪些IAM功能。

IAM您可以搭配使用的功能 AWS Systems Manager Incident Manager

IAM特徵	事件管理員支援
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵	否
ACLs	否
ABAC(策略中的標籤)	否
暫時性憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要深入瞭解事件管理員和其他 AWS 服務如何搭配大部分IAM功能運作，請參閱IAM使用者指南IAM中的可使用AWS 服務。

事件管理員不支援拒絕存取使用共用資源的原則 AWS RAM。

事件管理員的身分識別原則

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

事件管理員的身分識別原則範例

若要檢視事件管理員身分型原則的範例，請參閱。AWS Systems Manager Incident Manager的身分型政策範例

事件管理員中的資源型政策

支援以資源為基礎的政策：是

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

「事件管理員」服務僅支援兩種類型的資源型政策，使用 AWS RAM 主控台或 PutResourcePolicy 動作 (附加至回應計劃或連絡人)。此原則定義哪些主參與者可對回應計劃、連絡人、升級計劃和事件執行動作。事件管理員使用以資源為基礎的策略，跨帳號共用資源。

事件管理員不支援拒絕存取使用共用資源的原則 AWS RAM。

若要瞭解如何將以資源為基礎的原則附加至回應計劃或連絡人，請參閱事件管理員中的跨區域和跨帳戶事件管理。

事件管理員中的資源型政策範例

若要檢視「事件管理員」資源型策略的範例，請參閱以資源為基礎的政策範例 AWS Systems Manager Incident Manager。

事件管理員的政策動作

支援政策動作：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看事件管理員動作清單，請參閱服務授權參考 AWS Systems Manager Incident Manager中所定義的動作。

事件管理員中的原則動作會在動作之前使用下列前置詞：

```
ssm-incidents
ssm-contacts
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "ssm-incidents:Get*"
```

若要檢視事件管理員身分型原則的範例，請參閱。AWS Systems Manager Incident Manager的身分型政策範例

事件管理員會在兩個不同的命名空間 (ssm-事件和ssm-聯絡人) 中使用動作。建立事件管理員的原則時，請務必使用正確的動作命名空間。SSM-事件用於響應計劃和事件相關行動。SSM-聯繫人用於與聯繫人和聯繫人參與相關的操作。例如：

- ssm-contacts:GetContact
- ssm-incidents:GetResponsePlan

事件管理員的政策資源

支援政策資源：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看事件管理員資源類型及其清單ARNs，請參閱服務授權參考資料 AWS Systems Manager Incident Manager中所定義的資源。若要瞭解您可以針對每個資源指定哪些動作，請參閱由定義ARN的動作 AWS Systems Manager Incident Manager。

若要檢視事件管理員身分型原則的範例，請參閱。AWS Systems Manager Incident Manager的身分型政策範例

事件管理員資源可用於建立事件、在聊天通道中協作、解決事件並與回應人員互動。如果使用者擁有回應計劃的存取權，則他們可以存取由該計劃建立的所有事件。如果用戶可以訪問聯繫人或升級計劃，則可以與升級計劃中的聯繫人或聯繫人進行交互。

事件管理員的原則條件金鑰

支援服務特定政策條件金鑰：否

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

事件管理員中的存取控制清單 (ACLs)

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

以屬性為基礎的存取控制 (ABAC) 與事件管理員

支援 ABAC (策略中的標籤): 否

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

搭配事件管理員使用臨時登入

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱IAM。

事件管理員的跨服務主體權限

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

事件管理員的服務角色

支援服務角色：是

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷事件管理員功能。只有在事件管理員提供指引時，才編輯服務角色。

選擇事件管理員中的IAM角色

當您在事件管理員中建立回應計劃資源時，您必須選擇一個角色，以允許事件管理員代表您執行 Systems Manager 自動化文件。如果您先前已建立服務角色或服務連結角色，則事件管理員會提供一份可供您選擇的角色清單。選擇允許存取權的角色來執行自動化文件執行個體非常重要。如需詳細資訊，請參閱在事件管理員中使用系統管理員自動化手冊。當您建立要在事件期間使用的 AWS Chatbot 聊天頻道時，您可以選取一個服務角色，讓您直接從聊天中使用命令。若要深入瞭解如何建立聊天管道以進行事件協作，請參閱在事件管理員中使用聊天頻道。若要進一步了解中的IAM原則 AWS Chatbot，請參閱《管理AWS Chatbot 員指南》 AWS Chatbot中的〈管理使用〉管理執行命令的權限

事件管理員的服務連結角色

支援服務連結角色：是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需建立或管理事件管理員服務連結角色的相關資訊，請參閱針對事件管理員使用服務連結角色。

AWS Systems Manager Incident Manager的身分型政策範例

根據預設，使用者和角色沒有建立或修改「事件管理員」資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

如需有關事件管理員所定義之動作和資源類型的詳細資訊，包括每個資源類型的格式，請參閱服務授權參考 AWS Systems Manager Incident Manager中的動作、資源和條件索引鍵。ARNs

主題

- 政策最佳實務
- 使用事件管理員主控台
- 允許使用者檢視他們自己的許可
- 存取回應計劃

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的事件管理員資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。

- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

使用事件管理員主控台

若要存取 AWS Systems Manager Incident Manager 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。相反地，只允許存取符合他們嘗試執行之API作業的動作。

為了確保使用者和角色可以使用事件管理員主控台解決事件，請同時將事件`IncidentManagerResolverAccess` AWS 管理員管理的原則附加至實體。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

```
IncidentManagerResolverAccess
```

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

存取回應計劃

在此範例中，您想要授與 Amazon Web Services 帳IAM戶中的使用者存取您其中一個事件管理員回應計劃的權限exampleplan。您也想要允許使用者新增、更新及刪除回應計劃。

此原則會將ssm-incidents:ListResponsePlanssm-incidents:GetResponsePlan、ssm-incidents:UpdateResponsePlan和ssm-incident:ListResponsePlan權限授與使用者。

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
      },
      {
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
      }
   ]
}
```

以資源為基礎的政策範例 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 支援事件管理員回應計劃和聯絡人的資源型權限原則。

事件管理員不支援以資源為基礎的政策，拒絕使用共用 AWS RAM的資源存取。

若要瞭解如何建立回應計劃或連絡人，請參閱在事件管理員中使用回應計劃和在事件管理員中使用連絡人。

依組織限制事件管理員回應計劃存取

下列範例會將權限授與組織中具有組織 ID 的使用者：o-abc123def45回應使用回應計劃建立的事件myplan。

該Condition塊使用StringEquals條件和條aws:PrincipalOrgID件鍵，這是一個 AWS Organizations 特定的條件鍵。如需有關這些條件索引鍵的詳細資訊，請參閱「在政策中指定條件」。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": “*”,
      "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"o-abc123def45"}
      },
      "Action": [
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:UpdateRelatedItems",
        "ssm-incidents:ListRelatedItems"
      ],
      "Resource": [
        "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
        "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
      ]
    }
  ]
}
```

提供事件管理員連絡人存取主體

下列範例會授與主參與者建立ARNarn:aws:iam::999988887777:root連絡mycontact人參與的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

事件管理器中的跨服務混淆副預防

混淆的副問題是當沒有執行動作權限的實體呼叫更具權限的實體來執行動作時，就會發生資訊安全性問題。這可允許惡意行為者執行命令或修改他們無權執行或存取的資源。

在中 AWS，跨服務模擬可能會導致混淆的副案例。跨服務模擬是指某個服務（呼叫服務）呼叫另一個服務（稱為服務）的時候。惡意行為者可以使用呼叫服務，使用他們通常沒有的權限來更改另一個服務中的資源。

AWS 為服務主體提供對您帳戶資源的受管存取權限，以協助您保護資源的安全性。我們建議您在資源策略中使用aws:SourceArn和aws:SourceAccount全域條件內容索引鍵。這些金鑰會限制將另一個服務 AWS Systems Manager Incident Manager 提供給該資源的權限。如果您同時使用全域條件內容索引鍵，則在相同政策陳述式中使用時，aws:SourceArn值中參照的值和帳戶必須使用相同的帳戶ID。aws:SourceAccount

的值aws:SourceArn必須是受影響事件記錄ARN的值。如果您不知道資源ARN的完整內容，或者您要指定多個資源，請使用aws:SourceArn全域內容條件索引鍵搭*配萬用字元來表示的未知部分ARN。例如，您可以aws:SourceArn將設定為arn:aws:ssm-incidents::*111122223333*:*。

在下列信任原則範例中，我們使用aws:SourceArn條件索引鍵，根據事件記錄限制對服務角色的存取ARN。只myresponseplan有從回應計劃建立的事件記錄才能使用此角色。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

針對事件管理員使用服務連結角色

AWS Systems Manager Incident Manager 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至「事件管理員」的唯一IAM角色類型。服務連結角色由事件管理員預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您更輕鬆地設定事件管理員，因為您不需要手動新增必要的權限。事件管理員會定義其服務連結角色的權限，除非另有定義，否則只有事件管理員可以擔任其角色。定義的權限包括信任原則和權限原則，而且該權限原則無法附加至任何其他IAM實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的事件管理員資源，因為您無法意外移除存取資源的權限。

如需支援服務連結角色之其他服務的相關資訊，請參閱使用的AWS 服務，IAM並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

事件管理員的服務連結角色權限

事件管理員使用名為的服務連結角色 AWSServiceRoleforIncidentManager— 可讓事件管理員代表您管理事件管理員事件記錄和相關資源。

服 AWSServiceRoleforIncidentManager 務連結角色會信任下列服務擔任該角色：

- `ssm-incidents.amazonaws.com`

角色權限原則AWSIncidentManagerServiceRolePolicy可讓事件管理員對指定的資源完成下列動作：

- 動作：針ssm-incidents:ListIncidentRecords對與動作相關的所有資源。
- 動作：針ssm-incidents:CreateTimelineEvent對與動作相關的所有資源。
- 動作：針ssm:CreateOpsItem對與動作相關的所有資源。
- 動作：all resources related to the action. 上的 ssm:AssociateOpsItemRelatedItem
- 動作：針ssm-contacts:StartEngagement對與動作相關的所有資源。
- 動作:cloudwatch:PutMetricData在AWS/IncidentManager命名空間內的 CloudWatch 度量上

您必須設定權限，才能允許IAM實體 (例如使用者、群組或角色) 建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱IAM使用指南中的服務連結角色權限。

為事件管理員建立服務連結角色

您不需要手動建立一個服務連結角色。當您在、或中建立複製組時 AWS Management Console AWS API，事件管理員會為您建立服務連結角色。 AWS CLI

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立複製組時，事件管理員會再次為您建立服務連結角色。

編輯事件管理員的服務連結角色

事件管理員不允許您編輯 AWSServiceRoleforIncidentManager 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。但是，您可以使用編輯角色的描述IAM。如需詳細資訊，請參閱IAM使用指南中的編輯服務連結角色。

刪除事件管理員的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

若要刪除服務連結角色，您必須先刪除複製組。刪除複製組會刪除「事件管理員」中建立並儲存的所有資料，包括回應計劃、連絡人和上報計劃。您也會遺失所有先前建立的事件。任何指向已刪除回應計劃的警示和 EventBridge 規則，都不會在警示或規則符合時建立事件。若要刪除複製組，您必須刪除複製組中的每個區域。

> **Note**
>
> 當您嘗試刪除資源時，如果事件管理員服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除複製組中使用的區域 AWSServiceRoleforIncidentManager

1. 開啟事件管理員主控台，然後從左側導覽列選擇「設定」。
2. 在複製組中選取一個區域。
3. 選擇 刪除 。
4. 若要確認刪除「區域」，請輸入「區域」名稱，然後選擇「刪除」。
5. 重複這些步驟，直到您刪除複製組中的所有區域為止。刪除最終「區域」時，主控台會通知您刪除該區域的複製組。

若要使用手動刪除服務連結角色 IAM

使用IAM主控台 AWS CLI、或刪除 AWSServiceRoleforIncidentManager服務連結角色。 AWS API如需詳細資訊，請參閱IAM使用指南中的刪除服務連結角色。

事件管理員服務連結角色的支援區域

事件管理員支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

AWS 受管理的政策 AWS Systems Manager Incident Manager

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新API作業可供現有服務使 AWS 服務 用時，最有可能更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AWS 受管理的策略： AWSIncidentManagerIncidentAccessServiceRolePolicy

您可以附加AWSIncidentManagerIncidentAccessServiceRolePolicy到您的IAM實體。事件管理員也會將此原則附加至「事件管理員」角色，讓「事件管理員」代表您執行動作。

此原則會授與唯讀權限，讓事件管理員讀取其他特定資源， AWS 服務 以識別與這些服務中事件相關的發現項目。

許可詳細資訊

此政策包含以下許可。

- cloudformation— 允許主參與者描述 AWS CloudFormation 堆疊。這是必需的事件管理器來識別與 CloudFormation 事件相關的事件和資源。
- codedeploy— 允許主參與者讀取 AWS CodeDeploy 部署。事件管理員必須這樣做才能識別與事件相關的 CodeDeploy 部署和目標。
- autoscaling— 允許主體判斷 Amazon 彈性運算雲端 (EC2) 執行個體是否屬於 Auto Scaling 群組。這是必要的，因此事件管理員可以為屬於 Auto Scaling 群組的EC2執行個體提供發現項目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

若要檢視有關策略的詳細資訊 (包括最新版本的JSON原則文件)，請參閱《AWS 受管理策略參考指南》AWSIncidentManagerIncidentAccessServiceRolePolicy中的。

AWS 受管政策：**AWSIncidentManagerServiceRolePolicy**

您無法附加AWSIncidentManagerServiceRolePolicy至您的IAM實體。此原則附加至服務連結角色，可讓事件管理員代表您執行動作。如需詳細資訊，請參閱針對事件管理員使用服務連結角色。

此原則授予事件管理員權限，以列出事件、建立時間表事件、建立相關項目 OpsItems、將相關項目關聯至 OpsItems、開始參與，以及發佈與事件相關的 CloudWatch指標。

許可詳細資訊

此政策包含以下許可。

- ssm-incidents— 允許主參與者列出事件並建立時間表事件。這是必需的，以便響應者可以在事件儀表板上進行事件期間進行協作。
- ssm— 允許主參與者建立 OpsItems 及關聯相關項目。這是在事件開始 OpsItem 時建立父項所必需的。
- ssm-contacts— 允許主參與者開始參與。這是事件管理員在事件期間與聯繫人所必需的。
- cloudwatch— 允許主參與者發行 CloudWatch 量度。事件管理員發佈與事件相關的指標是必要的。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IncidentManager"
                }
            }
        }
    ]
}
```

若要檢視有關策略的詳細資訊 (包括最新版本的JSON原則文件)，請參閱《AWS 受管理策略參考指南》AWSIncidentManagerServiceRolePolicy中的。

AWS 受管理的策略：**AWSIncidentManagerResolverAccess**

您可以附加AWSIncidentManagerResolverAccess至IAM實體，以允許他們啟動、檢視和更新事件。這也允許他們在事件儀表板中創建客戶時間表事件和相關項目。您也可以將此政策附加至 AWS Chatbot 服務角色，或直接附加至與任何用於事件協同作業的聊天管道相關聯的客戶管理角色。若要

進一步瞭解中的IAM原則 AWS Chatbot，請參閱《管理指南》 AWS Chatbot中的〈管理使用〉AWS Chatbot 管理執行命令的權限。

許可詳細資訊

此政策包含以下許可。

- ssm-incidents— 允許您啟動事件，列出響應計劃，列出事件，更新事件，列出時間表事件，創建自定義時間表事件，更新自定義時間表事件，刪除自定義時間表事件，列出相關項目，創建相關項目以及更新相關項目。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:CreateTimelineEvent",
```

```
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
}
```

若要檢視有關策略的詳細資訊 (包括最新版本的JSON原則文件)，請參閱《AWS 受管理策略參考指南》AWSIncidentManagerResolverAccess中的。

事件管理員更新受 AWS 管理的策略

檢視事件管理員 AWS 受管理原則的詳細資料，因為此服務開始追蹤這些變更後。如需有關此頁面變更的自動警示，請訂閱「事件管理員文件歷史記錄」頁面上的動RSS態消息。

變更	描述	日期
AWSIncidentManagerIncidentAccessServiceRolePolicy — 政策更新	事件管理員為支援「發現項目」功能新增了新的權限，可讓執行個體檢查EC2執行個體是否屬於 Auto Scaling 群組。AWSIncidentManagerIncidentAccessServiceRolePolicy	2024年2月20日
AWSIncidentManagerIncidentAccessServiceRolePolicy – 新政策	事件管理員新增了一項新政策，授予事件管理員權限 AWS 服務 ，讓他人在管理事件時進行呼叫。	2023 年 11 月 17 日
AWSIncidentManagerServiceRolePolicy — 政策更新	事件管理員新增了一項新權限，可讓事件管理員將指標發佈到您的帳戶。	2022年12月16日

變更	描述	日期
AWSIncidentManagerResolverAccess – 新政策	事件管理員新增了一項新政策，可讓您啟動事件、列出回應計劃、列出事件、更新事件、列出時間表事件、建立自訂時間表事件、更新自訂時間表事件、刪除自訂時間表事件、列出相關項目、建立相關項目，以及更新相關項目。	2021 年 4 月 26 日
AWSIncidentManagerServiceRolePolicy – 新政策	事件管理員新增了一項新政策，授予事件管理員權限，以列出事件、建立時間表事件、建立相關項目 OpsItems、將相關項目與事件相關聯 OpsItems，以及開始與事件相關的參與。	2021 年 4 月 26 日
事件管理員開始追蹤變更	事件管理員開始追蹤其 AWS 受管理政策的變更。	2021 年 4 月 26 日

疑難排解 AWS Systems Manager Incident Manager 身分和存取

使用下列資訊可協助您診斷及修正使用事件管理員和時可能會遇到的常見問題IAM。

主題

- 我無權在事件管理員中執行動作
- 我沒有授權執行 iam：PassRole
- 我想要允許 Amazon Web Services 帳戶以外的人員存取我的事件管理員資源

我無權在事件管理員中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的ssm-incidents:*GetWidget*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-incidents:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 ssm-incidents:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，您必須更新原則，才能將角色傳遞給事件管理員。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的使用IAM者marymajor嘗試使用主控台在事件管理員中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 Amazon Web Services 帳戶以外的人員存取我的事件管理員資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解事件管理員是否支援這些功能，請參閱如何 AWS Systems Manager Incident Manager 使用 IAM。
- 若要瞭解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM使用者指南》中 AWS 帳戶 的〈提供存取權給其他IAM使用者〉。
- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。

- 若要瞭解如何透過身分聯盟提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權(身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

在事件管理員中使用共用聯絡人和回應計劃

透過聯絡人共用，身為聯絡人擁有者，您可以與其他人 AWS 帳戶 或 AWS 組織內部共用連絡人資訊、升級計劃和參與。您可以集中創建和管理聯繫人和升級計劃，並確保其他人可以在事件發生期間與正確的聯繫人互動。

透過回應計劃共用，身為回應計劃擁有者，您可以與其他人 AWS 帳戶 或 AWS 組織內部共用回應計劃及相關事件。您可以集中建立和管理回應計劃，讓消費者帳戶中的回應者可以在事件發生時與事件互動。

連絡人或回應方案擁有者可以與下列方式共用連絡人和回應計劃：

- 特定組織 AWS 帳戶 內部或外部 AWS Organizations
- 其組織內部的組織單位 AWS Organizations
- 它的整個組織 AWS Organizations

目錄

共用連絡人和回應計劃的先決條件

若要與您的組織或組織單位共用連絡人或回應計劃，請執行下列步 AWS Organizations驟：

- 您必須擁有 AWS 帳戶. 您無法共享已與您分享的聯絡人或回覆計劃。
- 您必須啟用與共用 AWS Organizations。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的透過 AWS Organizations啟用共用。

相關服務

聯繫人和響應計劃共享與 AWS Resource Access Manager （ AWS RAM ）集成。使用 AWS RAM，您可以與任何 AWS 帳戶 或通過共享您的 AWS 資源 AWS Organizations。您可以透過建立資源共用來共用您擁有的資源。資源共享指定要共用的資源，以及共用它們的消費者。消費者可以是中的個人 AWS 帳戶、組織單位或整個組織 AWS Organizations。

若要取得有關的更多資訊 AWS RAM，請參閱AWS RAM 使用者指南。

分享聯絡人或回應計劃

在您共用回應計劃之後，消費者就可以存取使用該回應計劃建立的所有過去、目前和 future 的事件。

在您分享連絡人之後，消費者可以存取事件期間發生的聯絡資訊、參與計劃、升級計劃和參與。消費者還可以在事件期間參與聯繫人或升級計劃。

如果您是組織的一員， AWS Organizations 且已啟用組織內的共用功能，則組織中的消費者會自動獲得共用連絡人或回應計劃的存取權。否則，取用者會收到加入資源共用的邀請，並在接受邀請後授予共用連絡人或回應計劃的存取權。

您可以使用 AWS RAM 主控台或共用您擁有的連絡人或回應計劃 AWS CLI。

使用 AWS RAM 主控台分享您擁有的聯絡人或回應計劃

請參閱《AWS RAM 使用者指南》中的建立資源共享。

若要分享您擁有的連絡人或回應計劃，請使用 AWS CLI

使用指create-resource-share令。

停止共享聯絡人或回應計劃

當資源擁有者停止與消費者共用聯絡人或回應計劃時，消費者的主控台中不會再顯示聯絡人、回應計劃、升級計劃、參與和事件。

> **Note**
>
> 如果消費者正在主控台中檢視連絡人、回應計劃、升級計劃、參與或未更新的事件，直到他們重新整理頁面或瀏覽離開頁面為止。

若要停止共用您擁有的共用連絡人或回應計劃，您必須將其從資源共用中移除。您可以使用主 AWS RAM 控台或 AWS CLI.

使用 AWS RAM 主控台停止分享您擁有的共用聯絡人或回應計劃

請參閱《AWS RAM 使用者指南》中的更新資源共享。

若要停止分享您擁有的共用連絡人或回應計劃，請使用 AWS CLI

使用指disassociate-resource-share令。

識別共用的聯絡人或回應計劃

擁有者和消費者可以使用事件管理員主控台和來識別共用的聯絡人和回應計劃 AWS CLI。

使用事件管理員主控台識別共用的聯絡人或回應計劃

> **Note**
>
> 通常，聯繫人，響應計劃，升級計劃，參與和事件在事件管理器控制台中無法識別為共享資源。在 Amazon 資源名稱 (ARN) 可見的地方，ARN包含擁有者的帳戶 ID。

若要識別共用的連絡人或回應計劃，請使用 AWS CLI

使用ListResponsePlans或ListContacts指令。此命令會傳回您擁有的連絡人和回應計劃，以及與您共用的聯絡人和回應計劃。ARN會顯示聯絡人或回應計劃擁有者的 AWS 帳戶 ID。

共用聯絡人與回應方案權限

擁有者的許可

擁有者可以更新、檢視、共用、停止分享，以及使用聯絡人和回應計劃。聯絡人和回應計劃包括相關的參與和事件。

消費者的許可

消費者只能使用和檢視回應計劃和連絡人。聯絡人和回應計劃包括相關的參與和事件。

計費和計量

資源的擁有者會針對資源收費。消費者不會為與他們共用的資源收費。共享資源不會產生額外費用。

執行個體限制

共用資源不會影響擁有者或消費者帳號中資源的限制。只有擁有者的帳號可用來計算資源限制。

符合性驗證 AWS Systems Manager Incident Manager

協力廠商稽核員會評估其安全性與合規性， AWS Systems Manager Incident Manager 做為多個 AWS 合規計畫的一部分。這些措施包括 SOC PCIRAMP, 美聯儲HIPAA, 和其他.

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全控制。ISO

- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性在 AWS Systems Manager Incident Manager

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

事件管理員是一項全球區域服務，目前不支援可用區域。

除了 AWS 全球基礎架構外，事件管理員還提供多種功能，協助支援您的資料復原能力和備份需求。在 [取得準備] 精靈期間，系統會要求您設定複製組。此區域複寫組可確保您的資料和資源可從多個區域存取，讓雲端網路的事件管理更易於管理。此複寫還可確保您的資料在其中一個區域故障時安全且可存取。

如需有關使用事件管理員複製組的詳細資訊，請參閱使用事件管理員複製組。

基礎結構安全 AWS Systems Manager Incident Manager

作為託管服務， AWS Systems Manager Incident Manager 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的通API話，透過網路存取事件管理員。使用者端必須支援下列專案：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

使用 AWS Systems Manager Incident Manager 和介面VPC端點 (AWS PrivateLink)

您可以在VPC和之間建立私人連線，方 AWS Systems Manager Incident Manager 法是建立介面VPC端點。界面端點是採用 AWS PrivateLink技術。有了 AWS PrivateLink，您可以在沒有網際網路閘道、NAT裝置、連線或VPN AWS Direct Connect 連線的情況下，私密存取事件管理員API作業。您中的執行個體VPC不需要公用 IP 位址即可與事件管理員API作業通訊。您VPC和事件管理員之間的流量會保留在 Amazon 網路中。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的介面VPC端點 (AWS PrivateLink)。

事件管理員VPC端點的考量

在為事件管理員設定介面VPC端點之前，請務必先檢閱 Amazon VPC 使用者指南中的界面端點屬性以及限制和AWS PrivateLink 配額。

事件管理器支持從您的VPC. API 若要使用所有事件管理員，您必須建立兩個VPC端點：一個用於端點`ssm-incidents`，另一個用於`ssm-contacts`。

為事件管理員建立介面VPC端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為事件管理員建立VPC端點。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立介面端點。

使用下列服務名稱為事件管理員建立VPC端點：

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

如果您DNS對端點使用 private，則可以使用「區域」的預設DNS名稱向事件管理員提出API要求。例如，您可以使用名稱`ssm-incidents.us-east-1.amazonaws.com`或`ssm-contacts.us-east-1.amazonaws.com`.

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的透過介面端點存取服務。

為事件管理員建立VPC端點策略

您可以將端點策略附加到VPC端點，以控制對事件管理器的訪問。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可以執行這些動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用VPC端點控制對服務的存取。

範例：事件管理員動作的VPC端點策略

以下是事件管理員的端點策略範例。連接至端點時，此策略會授與所有資源上所有主參與者列出的「事件管理員」動作的存取權。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

事件管理器中的配置和漏洞分析

配置和 IT 控制是與您（我們的客戶）AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

安全性最佳做法 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

主題

事件管理員的預防性安全性最佳做法

實作最低權限存取

授與權限時，您可以決定誰取得哪些事件管理員資源的權限。您還需針對這些資源啟用允許執行的動作，因此，只授與執行工作所需的權限。對降低錯誤或惡意意圖所引起的安全風險和影響而言，實作最低權限存取是相當重要的一環。

下列工具可用來實作最低權限存取：

- 使用IAM實體的原則和權限界限來控制 AWS 資源的存取
- 服務控制政策

建立和管理連絡人

啟用聯絡人時，事件管理員會聯絡裝置以確認啟用。在激活設備之前，請確保設備信息正確無誤。如此可減少事件管理員在啟用期間與錯誤裝置或人員聯絡的可能性。

定期審查您的聯繫人和升級計劃，以確保只有在事件期間需要聯繫的聯繫人才能與之聯繫。定期檢查聯繫人以刪除過時或不正確的信息。如果聯絡人在事件發生時不再收到通知，請將他們從相關的上報計劃中移除，或將他們從事件管理員中移除。

將聊天頻道設為私人

您可以將事件聊天頻道設為私有，以實施最低權限訪問。考慮使用不同的聊天頻道，其中包含每個響應計劃模板的用戶列表範本。這樣可以確保只有正確的回應者被拉入可能包含敏感資訊的聊天頻道。

AWS Chatbot 啟用的 Slack 通道會繼承用於設定 AWS Chatbot之IAM角色的權限。這可讓 AWS Chatbot 已啟用 Slack 頻道中的回應者呼叫任何允許列出的動作，例如事件管理員APIs和擷取指標圖表。

使 AWS 工具保持在最新狀態

AWS 定期發布您可以在 AWS 操作中使用的工具和插件的更新版本。將這些資源保持在最新狀態，可確保帳戶中的使用者和執行個體可以存取這些工具的最新功能和安全功能。

- AWS CLI — AWS Command Line Interface (AWS CLI) 是開放原始碼工具，可讓您使用命令列殼層中的命令與 AWS 服務互動。若要更新 AWS CLI，請執行與用於安裝 AWS CLI相同的命令。建議您在本機電腦上建立排程任務，至少每兩週執行一次適合您作業系統的命令。若要取得有關安裝指令的資訊，請參閱《指 AWS 令行介面使用指南》中的〈安裝指AWS 令行介面〉。
- AWS Tools for Windows PowerShell — 適用於 Windows 的工具 PowerShell 是一組模組，這些 PowerShell 模組是建立在 AWS SDK為公開的功能之上。 NET。Windows 工具可 PowerShell 讓您從命令列對資 AWS 源執行指 PowerShell 令碼作業。當 Windows PowerShell 工具的更新版本發行時，您應該定期更新在本機執行的版本。如需相關資訊，請參閱AWS Tools for Windows PowerShell 在視窗上更新或 AWS Tools for Windows PowerShell 在 Linux 或 macOS 上更新。

相關內容

Systems Manager 的安全性最佳作法

事件管理員的 Detective 安全最佳做法

識別並稽核您所有的事件管理員資源

識別 IT 資產是控管和保障安全的重要環節。識別您的 Systems Manager 資源，以評估其安全狀態，並針對潛在的弱點區域採取行動。為您的事件管理員資源建立資源群組。如需詳細資訊，請參閱《AWS Resource Groups 使用者指南》中的什麼是 Resource Groups？。

使用 AWS CloudTrail

AWS CloudTrail 提供「事件管理員」中使用者、角色或 AWS 服務所採取的動作記錄。使用收集的資訊 AWS CloudTrail，您可以判斷向事件管理員提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。如需詳細資訊，請參閱使用記錄 AWS Systems Manager Incident Manager API 呼叫 AWS CloudTrail。

監控 AWS 安全建議

定期檢查發布的 AWS 帳戶安全建議。 Trusted Advisor 您可以通過編程方式使用 describe-trusted-advisor-checks.

此外，主動監控您每個人註冊的主要電子郵件地址 AWS 帳戶。 AWS 將使用此電子郵件地址與您聯繫，以了解可能影響您的新興安全問題。

AWS 具有廣泛影響的作業問題會張貼在 AWS Service Health Dashboard 上。也會透過 AWS Health Dashboard將操作問題張貼至個別帳戶。如需詳細資訊，請參閱 AWS Health 文件。

相關內容

Amazon Web Services：安全程序概觀 (白皮書)

入門：在設定 AWS 資源時遵循安全性最佳做法 (AWS 安全性部落格)

IAM最佳做法

安全性最佳做法 AWS CloudTrail

在事件管理器中監控

AWS Systems Manager 事件管理員與下列服務整合，提供監控與記錄功能：

CloudWatch 度量

您可以使用 CloudWatch 測量結果，擷取 AWS Systems Manager 事件管理員作業之資料點的相關統計資料，做為一組排序的時間序列資料 (稱為測量結果)。您可以使用這些指標來確認您的系統是否依照預期執行。如需詳細資訊，請參閱 事件管理器中的 Amazon CloudWatch 指標。

CloudTrail 日誌

用 AWS CloudTrail 於擷取有關對 AWS API 進行呼叫的詳細資訊。您可以將這些調用作為日誌文件存儲在 Amazon 簡單存儲服務中。您可以使用這些 CloudTrail 記錄來判斷這類資訊，例如撥打哪個呼叫、來源 IP 位址、撥打電話的人員以及撥打電話的時間。記 CloudTrail 錄檔包含事件管理員呼叫 API 動作的相關資訊。如需詳細資訊，請參閱使用記錄 AWS Systems Manager Incident Manager API 呼叫 AWS CloudTrail。

Trusted Advisor

AWS Trusted Advisor 可協助您監控 AWS 資源，以改善效能、可靠性、安全性和成本效益。所有使用者均可使用四 Trusted Advisor 項檢查；擁有商業或企業支援方案的使用者可使用超過 50 項檢查。對於事件管理員，請 Trusted Advisor 檢查複製組的組態是否使用多個組態 AWS 區域 來支援區域容錯移轉和回應。如需詳細資訊，請參閱《AWS Support 使用者指南》中的 AWS Trusted Advisor。

事件管理器中的 Amazon CloudWatch 指標

事件管理員提供可在 Amazon 中監控的彙總指標 CloudWatch。您可以使用這些測量結果來識別事件和回應計劃趨勢。

這些指標包括：

- 指定期間內建立的未預期事件數目
- 回應及解決這些事件的時間
- 已解決的事件數目

您可以監控 Event Manager 指標，進一步瞭解您的營運狀況，並採取有意義的行動來推動事件回應的卓越營運。所有「事件管理員」區域均提供「事件管理員」指標 加入事件管理員時，您可以在

Amazon CloudWatch 中檢視您在複寫組中指定的所有區域的指標。您可以在「區域」中檢視已針對事件採取動作的已發佈量度。這些指標不收取額外費用。

在 CloudWatch 主控台上，您可以使用以下指標建立儀表板，以：

- 測量和審查您現有的事件負載
- 追蹤事件負載是否增加、減少或保持不變
- 更有效地使用事件管理器來減少事件發生的頻率、持續時間和影響

此頁面說明 CloudWatch 主控台上可用的「事件管理員」測量結果。

> **Important**
>
> 對於客戶產生的事件，如果中`TriggerDetails`的來源值使用非 ASCII 字元命名，則不會在不支援非 ASCII 文字的 Amazon CloudWatch 指標中報告該事件的指標。 `source`只能以編程方式提供，例如使用 SDK 或. AWS CLI

事件管理員會將下列指標傳送至 CloudWatch。

指標	描述
`NumberOfCreateIncidents`	建立的未預期事件數目。 有效尺寸:[] (空白維度)、[ResponseP lan Impact]、[]、[Source]、[ResponseP lan ,Impact]、[ResponsePlan ,Source] 單位：計數
`NumberOfResolveIncidents`	已解決的事件數目。 有效尺寸:[] (空白維度)、[ResponseP lan Impact]、[]、[Source]、[ResponseP lan ,Impact]、[ResponsePlan ,Source] 單位：計數

指標	描述
TimeToFirstAcknowledgement	事件建立時間與事件第一次確認的時間之間的時間差異。 有效尺寸:[] (空白維度)、[ResponseP lan Impact]、[]、[Source]、[ResponseP lan ,Impact]、[ResponsePlan ,Source] 單位：秒
TimeToResolveIncident	事件建立與解決事件的時間差異。 有效尺寸:] (空白維度)、[ResponsePlan Impact]、[Source]、[]、[ResponsePlan ,Impact]、[ResponsePlan ,Source] 單位：秒

在 CloudWatch主控台檢視事件管理員測量結果

在 CloudWatch 主控台中檢視事件管理員測量結果

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 指標。
3. 选择 IncidentManager 命名空间。
4. 在「量度」標籤上，選擇維度，然後選擇量度。

如需使用指 CloudWatch 標的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的以下主題：

- 指標
- 使用 Amazon CloudWatch 指標

指標的維度

「事件管理員」測量結果會使用IncidentManager命名空間，並提供下列維度的測量結果：

維度	描述
By Response Plan	依回應計劃檢視彙總測量結果。
By Impact Level	依嚴重性層級檢視彙總測量結果。
By Source	檢視由 CloudWatch 警示或事件手動建立之 EventBridge 事件的測量結果。
Across All Incidents	檢視目前「 AWS 區域」中所有事件的彙總測量結果。
Response Plan name and Source	檢視每個回應計劃與來源組合的彙總測量結果。
Response Plan Name and Impact Level	檢視每個回應計劃與嚴重性層級組合的彙總測量結果。

使用記錄 AWS Systems Manager Incident Manager API 呼叫 AWS CloudTrail

AWS Systems Manager Incident Manager 與提供使用者AWS CloudTrail、角色或使用者所採取之動作記錄的服務整合 AWS 服務。 CloudTrail 將事件管理員的所有 API 呼叫擷取為事件。擷取的呼叫包括來自事件管理員主控台的呼叫，以及對事件管理員 API 作業的程式碼呼叫。使用收集的資訊 CloudTrail，您可以判斷向事件管理員提出的要求、提出要求的 IP 位址、提出要求的時間，以及其他詳細資訊。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是使用根使用者還是使用者憑證提出。
- 請求是否代表 IAM 身分中心使用者提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

CloudTrail 在您創建帳戶 AWS 帳戶 時處於活動狀態，並且您自動可以訪問 CloudTrail 事件歷史記錄。 CloudTrail 事件歷史記錄提供了過去 90 天中記錄的管理事件的可查看，可搜索，可下載和不可變

的記錄。 AWS 區域若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。查看活動歷史記錄不 CloudTrail收取任何費用。

如需過 AWS 帳戶 去 90 天內持續的事件記錄，請建立追蹤或 CloudTrailLake 事件資料存放區。

CloudTrail 小徑

追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。使用建立的所有系統線 AWS Management Console 都是多區域。您可以使用建立單一區域或多區域系統線。 AWS CLI建議您建立多區域追蹤，因為您會擷取帳戶 AWS 區域 中的所有活動。如果您建立單一區域追蹤，則只能檢視追蹤記錄中的 AWS 區域事件。如需有關追蹤的詳細資訊，請參閱《AWS CloudTrail 使用指南》中的「為您的建立追蹤」 AWS 帳戶和「為組織建立追蹤」。

您可以透 CloudTrail 過建立追蹤，免費將一份正在進行的管理事件副本傳遞到 Amazon S3 儲存貯體，但是需要支付 Amazon S3 儲存費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail 湖泊事件資料存放區

CloudTrail L@@ ake 可讓您針對事件執行 SQL 型查詢。 CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。若要取得有關 CloudTrail Lake 的更多資訊，請參閱使用指南中的〈AWS CloudTrail 使用 AWS CloudTrail Lake 〉。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

事件管理員管理事件 CloudTrail

管理事件提供有關在您的資源上執行的管理作業的資訊 AWS 帳戶。這些也稱為控制平面操作。依預設，會 CloudTrail 記錄管理事件。

AWS Systems Manager Incident Manager 將所有事件管理員控制平面作業記錄為管理事件。如需事件管理員記錄到的 AWS Systems Manager Incident Manager 控制平面作業清單 CloudTrail，請參閱 AWS Systems Manager Incident Manager API 參考。

事件管理員事件範例

事件代表來自任何來源的單一請求，並包括有關請求的 API 操作，操作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此事件不會以任何特定順序顯示。

下列範例顯示示範`StartIncident`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

下列範例顯示示範`DeleteContactChannel`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```


若要取得有關 CloudTrail 記錄內容的資訊，請參閱AWS CloudTrail 使用指南中的CloudTrail記錄內容。

與事件管理器的產品和服務整合

事件管理員是一項與下列產品、服務和工具整合的 AWS Systems Manager功能。

與整合 AWS 服務

事件管理員 AWS 服務 與下表所述的和工具整合。

AWS CDK	AWS CDK 這是一個開發框架，用於使用代碼來定義您的雲基礎架構並用 AWS CloudFormation 於佈建。 AWS CDK 支援多種程式設計語言 TypeScript，包括 JavaScript、PythonJava、和 C#/.NET。 如需 AWS CDK 搭配事件管理員搭配使用的詳細資訊，請參閱 AWS CDK API 參考中的下列各節： • @aws-cdk/aws-ssmincidents模組 • @aws-cdk/aws-ssmcontacts模組
AWS Chatbot	AWS Chatbot使軟件 DevOps 開發團隊能夠使用消息傳遞程序聊天室來監視和響應其中的操作事件 AWS 雲端。 AWS Chatbot 與事件管理員搭配使用時，您可以建立聊天頻道，以供回應者用來監控和回應事件。 AWS Chatbot 支援Slack聊天室、Microsoft Teams頻道和 Amazon Chime 聊天室做為聊天頻道。 在建立聊天頻道的過程中，您還可以在 Amazon Simple Notification Service (Amazon SNS) 中建立主題。Amazon SNS 是一種受管服務，可提供從發佈者傳送訊息給訂閱者的訊息。在事件回應計劃中，當您建立的聊天頻道與方案建立關聯時，您也可以選擇與該聊天頻道相關聯的一或多

	個主題。這些 SNS 主題可用來傳送事件相關通知給事件回應者。 如需詳細資訊，請參閱 在事件管理員中使用聊天頻道。
AWS CloudFormation	AWS CloudFormation 是一項服務，您可以使用它來建立包含應用程式所需之所有資源的範本，然後為您配置和佈建資源。它還將配置所有依賴關係，因此您可以更專注於應用程序，而不用於管理資源。 如需 AWS CloudFormation 搭配「事件管理員」使用的詳細資訊，請參閱使AWS CloudFormation 用指南中的下列主題： • 事件管理員資源類型參照 • 聯絡人資源類型參考資源類型參考
Amazon CloudWatch	CloudWatch即時監控您的 AWS 資源和執行 AWS 的應用程式。您可以用 CloudWatch 來收集和追蹤指標，這些指標是您可以針對資源和應用程式測量的變數。 您可以在事件管理員中設定 CloudWatch 警示以建立事件。 CloudWatch 與 Systems Manager 和事件管理員合作，在警報進入警報狀態時，從響應計劃模板創建事件。 如需詳細資訊，請參閱 使用 CloudWatch 警示自動建立事件。

Amazon Chime	Amazon Chime 是一個結合了會議、聊天和商務電話的線上工作場所。您可以使用 Amazon Chime 在組織內外開會、聊天和撥打商務電話。 您可以建立 Amazon Chime in 的聊天管道 AWS Chatbot，然後將該頻道新增至回應計劃，將 Amazon Chime 會議室整合到事件管理員作業中。 如需詳細資訊，請參閱 在事件管理員中使用聊天頻道。
Amazon EventBridge	EventBridge是一種使用事件連接應用程式元件的無伺服器服務，讓您更輕鬆地建置可擴充的事件驅動型應用程式。 您可以設定 EventBridge 規則來監視資 AWS 源中的事件模式，並在事件符合您定義的模式時，在事件管理員中建立事件。您的規則可以監控數十種 AWS 服務 和第三方應用程式和服務中的事件模式。 如需詳細資訊，請參閱 利用事件自動建立 EventBridge 事件。
AWS Secrets Manager	Secrets Manager 可協助您在整個生命週期中管理、擷取和輪換資料庫登入資料、應用程式憑證、OAuth 權杖、API 金鑰和其他機密。 當您將事件管理員與 PagerDuty 服務整合時，您會在 Secrets Manager 中建立包含您 PagerDuty 認證的密碼。 如需詳細資訊，請參閱 在 AWS Secrets Manager 密碼中儲 PagerDuty 存存取認證。

AWS Systems Manager	Systems Manager 是一個作業中心，您可以使用它來檢視和控制應用程式基礎結構，以及適用於雲端環境的安全 end-to-end 管理解決方案。下列 Systems Manager 功能可直接與事件管理員整合： • 自動化 — 自動化手冊定義 Systems Manager 對您的 AWS 資源執行的動作。在事件管理器中，runbook 定義了一系列用於解決事件的自動化和手動步驟。 如需建立與事件管理員搭配使用的自動化 Runbook 的相關資訊，請參閱在事件管理員中使用系統管理員自動化手冊。 • OpsCenter— OpsCenter 提供一個集中位置，讓作業工程師和 IT 專業人員可以管理與 AWS 資源相關的OpsItems作業工作項目。您可以 OpsItems直接從事件後分析建立，以跟進相關工作。 如需詳細資訊，請參閱 在事件管理員中執行事件後分析。
AWS Trusted Advisor	Trusted Advisor是具有基本或開發人員支援方案的 AWS 客戶可使用的工具。 Trusted Advisor 檢查您的 AWS 環境，然後在存在機會時提出建議，以節省資金、改善系統可用性和效能，或協助縮小安全性漏洞。 對於事件管理員，請 Trusted Advisor 檢查複製組的組態是否使用多個組態 AWS 區域 來支援區域容錯移轉和回應。

與其他產品及服務整合

您可以將事件管理員與下表所述的第三方服務整合或使用。

Jira Cloud	使用 AWS Service Management Connector，您可以將事件管理器與第三方雲端工作流程平台 Jira Cloud (Atlassian) 整合。 設定與 Jira Cloud 的整合後，當您在事件管理員中建立新事件時，整合也會在 Jira Cloud 中建立事件。如果您在事件管理員中更新事件，它會對 Jira Cloud 中的對應事件進行這些更新。如果您在事件管理員或 Jira Cloud 中解決事件，整合會根據您設定的偏好設定，解決這兩項服務中的事件。 如需詳細資訊，請參閱《AWS Service Management Connector 管理員指南》中的「整合 AWS Systems Manager Incident Manager (Jira Cloud)」。
吉拉服務管理	使用 AWS Service Management Connector，您可以將事件管理器與第三方雲端工作流程平台 Jira 服務管理整合。 設定與「Jira 服務管理」的整合之後，當您在「事件管理員」中建立新的事件時，整合也會在「Jira 服務管理」中建立事件。如果您更新事件管理員中的事件，它會對「Jira 服務管理」中的對應事件進行這些更新。如果您在「事件管理員」或「Jira 服務管理」中解決事件，整合會根據您設定的偏好設定，解決這兩項服務中的事件。 如需詳細資訊，請參閱《管理AWS Service Management Connector 員指南》中的〈配置 Jira 服務管理〉。
Microsoft Teams	Microsoft Teams為團隊傳訊、音訊和視訊會議以及檔案共用提供協作雲端工具。

	您可以建立Microsoft Team中的聊天Microsoft Teams頻道，然後將該頻道新增至回應計劃 AWS Chatbot，將頻道整合到事件管理員作業中。 如需詳細資訊，請參閱 在事件管理員中使用聊天頻道。
PagerDuty	PagerDuty是支援分頁工作流程和上報原則的事件回應工具。 將事件管理員與整合時 PagerDuty，您可以將 PagerDuty 服務新增至您的回應計劃。之後，每當在「事件管理員」中建立事件 PagerDuty 時，就會建立對應的事件。中的事件 PagerDuty 會使用您在此處定義的呼叫工作流程和呈報原則，以及「事件管理員」中所定義的原則。 PagerDuty 附加事件管理員的時間表事件作為事件的附註。 若要將「事件管理員」與「事件管理員」整合 PagerDuty，您必須先在中建立包含 AWS Secrets Manager 認 PagerDuty 證的密碼。 如需將 PagerDuty REST API 金鑰和其他必要詳細資訊新增至中的密碼的相關資訊 AWS Secrets Manager，請參閱在 AWS Secrets Manager 密碼中儲 PagerDuty 存存取認證。 如需在事件管理員中將 PagerDuty 服務從您的 PagerDuty 帳戶新增至回應計劃的相關資訊，請參閱主題中的將 PagerDuty 服務整合至回應計劃的步驟建立回應計劃。

ServiceNow	使用 AWS Service Management Connector，您可以將事件管理器與ServiceNow第三方雲端工作流程平台整合。 設定整合後 ServiceNow，當您在事件管理員中建立新的事件時，整合也會在中 ServiceNow 建立事件。如果您更新事件管理員中的事件，它會對中的對應事件進行這些更新 ServiceNow。如果您在「事件管理員」或「事件管理員」中解決事件 ServiceNow，整合會根據您設定的偏好設定，解決這兩項服務中的事件。 如需詳細資訊，請參閱《AWS Service Management Connector 管理員指南》AWS Systems Manager Incident Manager ServiceNow中的〈整合〉。
Slack	Slack為團隊傳訊、音訊和視訊會議以及檔案共用提供協作雲端工具。 您可以建立Slack中的聊天Slack頻道，然後將該頻道新增至回應計劃 AWS Chatbot，將頻道整合到事件管理員作業中。 如需詳細資訊，請參閱 在事件管理員中使用聊天頻道。

地形	HashiCorp Terraform 是一種開放原始碼基礎架構即程式碼 (IaC) 軟體工具，提供命令列介面 (CLI) 工作流程來管理各種雲端服務。對於事件管理員，您可以使用 Terraform 來管理或佈建下列項目： SSM 事件管理員連絡人資源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aw_s 接觸器 _ 旋轉 SSM 連絡人資料來源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aw_s 接觸器 _ 旋轉 SSM 事件管理員資源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM 事件管理員資料來源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

在 AWS Secrets Manager 密碼中儲 PagerDuty 存存取認證

PagerDuty 針對回應計劃開啟與整合之後，事件管理員會以下列方式使 PagerDuty 用：

- 當您在事件管理器中創建新的事件 PagerDuty 時，事件管理器創建一個相應的事件。

- 您在中建立的分頁工作流程和提升原則 PagerDuty 會在 PagerDuty 環境中使用。不過，事件管理員不會匯入您的 PagerDuty 設定。
- 事件管理員會將時間表事件發佈為中事件的附註 PagerDuty，最多可發佈 2,000 個備註。
- 您可以選擇在「 PagerDuty 事件管理員」中解決相關事件時自動解決事件。

若要將「事件管理員」與「事件管理員」整合 PagerDuty，您必須先在中建立包含 AWS Secrets Manager 認 PagerDuty 證的密碼。這些可讓事件管理員與您的 PagerDuty服務進行通訊。然後，您可以將 PagerDuty 服務納入您在「事件管理員」中建立的回應計劃中。

您在密碼管理員中建立的這個密碼必須以適當的 JSON 格式包含下列項目：

- 您 PagerDuty 帳戶中的 API 金鑰。您可以使用一般存取 REST API 金鑰或使用者權杖 REST API 金鑰。
- 子 PagerDuty 網域的有效使用者電子郵件地址。
- 您部署子網域的 PagerDuty 服務區域。

> **Note**
>
> PagerDuty 子網域中的所有服務都會部署至相同的服務區域。

必要條件

在秘密管理員中建立密碼之前，請確定您符合下列需求。

KMS 金鑰

您必須使用您在 AWS Key Management Service (AWS KMS) 中建立的客戶管理金鑰來加密您建立的密鑰。您可以在建立儲存 PagerDuty 認證的密碼時指定此金鑰。

> **Important**
>
> Secrets Manager 提供使用加密密碼的選項 AWS 受管金鑰，但不支援此加密模式。

客戶管理的金鑰必須符合下列需求：

- 金鑰類型：選擇「對稱」。

- 金鑰使用方式：選擇「加密並解密」。
- 地區性：如果您要將回應計劃複製為多個 AWS 區域，請務必選取「多區域金鑰」。

金鑰政策

設定回應計劃的使用者必須擁有金鑰以資源為基礎的原則kms:GenerateDataKey和kms:Decrypt權限。ssm-incidents.amazonaws.com服務主體必須在金鑰的資源型原則kms:Decrypt中具有kms:GenerateDataKey和的權限。

下列原則示範這些權限。將每個*#########*替換為自己的資訊。

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
```

```
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

如需建立新客戶受管金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的建立對稱加密 KMS 金鑰。如需 AWS KMS 索引鍵的詳細資訊，請參閱AWS KMS 概念。

如果現有客戶受管金鑰符合先前所有需求，您可以編輯其政策以新增這些權限。如需更新客戶受管金鑰中政策的相關資訊，請參閱AWS Key Management Service 開發人員指南中的變更金鑰政策。

> **Tip**
>
> 您可以指定條件鍵來進一步限制存取。例如，下列原則只允許透過美國東部 (俄亥俄) 區域 (US-east-2) 的「Secrets Manager」進行存取：
>
> ```
> {
>     "Sid": "Enable IM Permissions",
>     "Effect": "Allow",
>     "Principal": {
>         "Service": "ssm-incidents.amazonaws.com"
>     },
>     "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
>     "Resource": "*",
>     "Condition": {
>         "StringEquals": {
>             "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
>         }
>     }
> }
> ```

`GetSecretValue`權限

建立回應計劃的 IAM 身分 (使用者、角色或群組) 必須具有 IAM 權限`secretsmanager:GetSecretValue`。

將存 PagerDuty 取認證儲存在 AWS Secrets Manager 密碼中

1. 請按照「AWS Secrets Manager 使用者指南」中「建立 AWS Secrets Manager 密碼」中的步驟 3a 中的步驟進行操作。
2. 對於步驟 3b，對於鍵/值配對，請執行以下操作：
   - 選擇「明文」標籤。
   - 以下列 JSON 結構取代方塊的預設內容：

     ```
     {
         "pagerDutyToken": "pagerduty-token",
         "pagerDutyServiceRegion": "pagerduty-region",
         "pagerDutyFromEmail": "pagerduty-email"
     }
     ```

   - 在您貼上的 JSON 範例中，取代*#####*，如下所示：
     - *######*自您帳戶的一般訪問 REST API 密鑰或用戶令牌 REST API 密鑰的值。 PagerDuty

       如需相關資訊，請參閱PagerDuty 知識庫中的 API 存取金鑰。
     - *##########*之 PagerDuty 資料中心的服務區域。 PagerDuty

       如需相關資訊，請參閱PagerDuty 知識庫中的服務區域。
     - *######*：屬於您子網域之使用者的有效電子郵件地址。 PagerDuty

       如需相關資訊，請參閱管理PagerDuty 知識庫中的使用者。

     下列範例顯示包含必要 PagerDuty認證的完整 JSON 密碼：

     ```
     {
         "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
         "pagerDutyServiceRegion": "US",
         "pagerDutyFromEmail": "JohnDoe@example.com"
     }
     ```

3. 在步驟 3c 中，針對加密金鑰，選擇您建立的客戶管理金鑰，該金鑰符合上一個先決條件區段中列出的需求。
4. 在步驟 4c 上，對於資源權限，執行下列操作：
   - 展開 [資源權限]。

- 選擇 [編輯權限]。
- 以下列 JSON 結構取代原則方塊的預設內容：

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- 選擇儲存。

5. 在步驟 4d 中，如果您將回應計劃複製到多個 AWS 區域密碼，請執行下列動作：
   - 展開複製密碼。
   - 針對 AWS 區域，選取您複製回應計劃的目標區域。
   - 對於加密金鑰，請選擇您在此區域中建立或複製到的客戶管理金鑰，該金鑰符合「先決條件」區段中列出的需求。
   - 對於其他每一個 AWS 區域，選擇新增區域，然後選取區域名稱和客戶管理金鑰。
6. 完成《AWS Secrets Manager 使用者指南》中建立 AWS Secrets Manager 密碼中的其餘步驟。

如需如何將 PagerDuty 服務新增至「事件管理員」事件工作流程的相關資訊，請參閱主題中的將 PagerDuty 服務整合至回應計劃建立回應計劃。

相關資訊

如何使用 PagerDuty 和自動化事件回應 AWS Systems Manager Incident Manager (AWS 雲端 作業和移轉部落格)

AWS Secrets Manager 用戶指南 AWS Secrets Manager中的秘密加密

故障診斷AWS Systems Manager

如果您在使用AWS系統管理員事件管理員時遇到問題，可以根據我們的最佳做法，使用下列資訊來解決問題。如果您遇到的問題超出了下列資訊的範圍，或者在您嘗試解決問題後仍然存在，請連絡AWS Support。

主題

錯誤訊息：ValidationException – We were unable to validate the AWS Secrets Manager secret

問題 1：建立回應計劃的AWS Identity and Access Management (IAM) 身分識別 (使用者、角色或群組) 沒有`secretsmanager:GetSecretValue` IAM 權限。IAM 身分必須擁有此權限才能驗證機 Secrets Manager 密碼。

- 解決方案：針對建立回應計劃的 IAM 身分，將遺失的`secretsmanager:GetSecretValue`權限新增至 IAM 政策。如需詳細資訊，請參閱 IAM 使用者指南中的新增 IAM 身分許可 (主控台AWS CLI) 或新增 IAM 政策 ()。

問題 2：密碼沒有附加可讓 IAM 身分執行`GetSecretValue`動作的資源型政策，或者以資源為基礎的政策拒絕對該身分的許可。

- 解決方案：在機密的資源型政策中建立或新增`Allow`陳述式，以授`secrets:GetSecretValue`予 IAM 身分的權限。或者，如果您使用包含 IAM 身分的`Deny`陳述式，請更新政策，以便身分識別可以執行動作。如需詳細資訊，請參閱《AWS Secrets Manager使用指南》中的「將權限原則附加至AWS Secrets Manager密碼」。

問題 3：密碼沒有附加以資源為基礎的原則，允許存取事件管理員服務主體、`ssm-incidents.amazonaws.com`.

- 解決方案：針對密碼建立或更新以資源為基礎的政策，並包含下列權限：

```
{
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

問題 4：AWS KMS key選取要加密密碼的不是客戶受管金鑰，或者選取的客戶受管金鑰未提供 IAM 許可`kms:Decrypt`和`kms:GenerateDataKey*`事件管理員服務主體。或者，建立回應計劃的 IAM 身分可能沒有 IAM 許可`GetSecretValue`。

- 解決方案：請確定您符合主題中必要條件下所述的需求在 AWS Secrets Manager 密碼中儲 PagerDuty 存存取認證。

問題 5：包含一般存取權限 REST API 金鑰或使用者權杖 REST API 金鑰的秘密 ID 無效。

- 解決方案：確定您已正確輸入 Secret 管理員密碼的 ID，且沒有結尾空格。您必須使用存儲要使用的密碼的相同AWS 區域工作。您無法使用已刪除的密碼。

問題 6：在極少數情況下，Secrets Manager 服務可能會遇到問題，或事件管理員可能無法與其通訊。

- 解決方案：請等待幾分鐘後再試一次。檢查是否AWS Health Dashboard有任何可能影響任一服務的問題。

其他故障診斷問

如果上述步驟無法解決您的問題，您可以從下列資源尋求其他協助：

- 如需存取事件管理員主控台時事件管理員特定的 IAM 問題，請參閱疑難排解 AWS Systems Manager Incident Manager 身分和存取。
- 有關存取時的一般身份驗證和授權問題AWS Management Console，請參閱 IAM 使用者指南中的 IAM 疑難排解

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

事件管理員的文件記錄

變更	描述	日期
更新到受管理的策略 AWSIncidentManagerIncidentAccessServiceRolePolicy	事件管理員為支援「發現項目」功能新增了新的權限，可讓其檢查 EC2 執行個體是否屬於 Auto Scaling 群組。AWSIncidentManagerIncidentAccessServiceRolePolicy 如需詳細資訊，請參閱事件管理員對 AWS 受管理策略的更新。	2024年2月20日
額外的 HashiCorp 地形支持：隨叫旋轉	Terraform 已添加到其對事件管理器的支持中。您現在可以使用 Terraform 佈建或管理事件管理員待命資源。如需此功能以及其他第三方與事件管理員整合的相關資訊，請參閱與其他產品和服務整合。	2024年2月2日
新功能：來自其他的發現 AWS 服務	發現項目會提供您與 AWS CloudFormation 堆疊和 AWS CodeDeploy 部署相關變更的相關資訊，這些變更大約在事件管理員中建立事件的時間內發生。在「事件管理員」主控台中，您可以檢視這些變更的摘要資訊，並在許多情況下存取 CloudFormation 或主控 CodeDeploy 台的連結，以取得有關變更的完整詳細資訊。發現項目可減少評估事件潛在原因所需的時間。它們還可以減少回應者存取錯誤帳戶或主	2023 年 11 月 15 日

	控台來調查事件原因的機會。此功能也引進了新的受管理政策`AWSIncidentManagerIncidentAccessServiceRolePolicy`，可讓事件管理員讀取其他資源， AWS 服務 以識別與事件相關的發現項目。如需詳細資訊，請參閱下列主題： • 使用發現項目 • AWS 受管理的策略：AWSIncidentManagerIncidentAccessServiceRolePolicy	
更新與事件管理員的整合清單	與事件管理員的產品和服務整合主題已擴展到列出並說明您可以與事件管理員整合到事件偵測和回應作業中的所有 AWS 服務 和第三方工具。	2023 年 6 月 9 日

與整合 AWS Trusted Advisor	Trusted Advisor 現在會檢查複製組的組態是否使用多個 AWS 區域 來支援區域容錯移轉和回應。針對 CloudWatch警示或事件所建立的 EventBridge 事件，事件管理員會以警示或事件規則 AWS 區域 相同的方式建立事件。如果該區域暫時無法使用 Incident Manager，則系統會嘗試在複製集的另一個區域中建立事件。如果複製集僅包含一個區域，則系統無法在 Incident Manager 無法使用時建立事件記錄。為協助避免此情況，請在僅針對一個區域設定複製組時 Trusted Advisor 報告。若要取得有關使用的資訊 Trusted Advisor，請參閱《AWS Support 使用者指南》AWS Trusted Advisor中的。	2023 年 4 月 28 日

使用 Microsoft 團隊做為回應計劃中的聊天頻道	透過與 Microsoft 團隊的整合 AWS Chatbot，您現在可以在回應計劃中使用 Microsoft Teams 進行聊天頻道。除了支援 Slack 和 Amazon Chime 聊天頻道之外，還支援此功能。事件發生期間，事件管理員會將狀態通知直接傳送至聊天頻道，讓所有回應者隨時掌握最新資訊。回應者也可以在 Microsoft Teams 應用程式中彼此通訊及與事件相關的 AWS CLI 命令，以更新事件並與事件互動。如需詳細資訊，請參閱在事件管理員中使用聊天頻道。	2023 年 4 月 4 日
新功能：待命排程	事件管理員中的隨時待命排程定義在發生需要操作員介入的事件發生時，誰會收到通知。隨叫排程由您為排程建立的一或多個旋轉組成。每個旋轉最多可包括 30 個觸點。建立待命中的排程之後，您可以將其作為升級計劃納入升級計劃中。當與該升級計劃相關聯的事件發生時，事件管理員會根據排程通知正在召喚的操作員（或操作員）。如需詳細資訊，請參閱在事件管理員中使用待命中排程。	2023 年 3 月 28 日

列印格式化的事件分析或另存為 PDF	事件分析頁面現在包含「列印」按鈕，可產生格式化為列印的分析版本。使用為裝置設定的印表機目的地，您可以將事件分析儲存為 PDF，或傳送至本機或網路印表機。如需詳細資訊，請參閱列印格式化的事件分析。	2023 年 1 月 17 日
PagerDuty 整合：事件管理員現在將事件時間表事件複製到 PagerDuty事件	當您在回應計劃 PagerDuty 中開啟整合時，事件管理員會將從該計劃建立的時間表事件新增至中的對應事件記錄 PagerDuty。 PagerDuty 將時間軸事件新增為事件的附註，最多可加入 2,000 個備註。若要深入瞭解這些變更，請參閱下列主題： • 將存 PagerDuty 取認證儲存在 AWS Secrets Manager 密碼中 • 將 PagerDuty 服務整合至回應計劃	2022 年 12 月 15 日
事件管理器與 CloudWatch 指標集成。	您現在可以在中發佈與事件相關的量度。 CloudWatch如需詳細資訊，請參閱CloudWatch量度。 AWSIncidentManagerServiceRolePolicy 已包含額外權限，允許我們的服務代表您發佈指標。	2022 年 12 月 15 日

啟動事件備註並更新「事件詳細資料」畫面	您可以使用事件備註與處理事件的其他使用者共同作業和通訊。此外，您也可以從「事件詳細資料」畫面檢視 Runbook 和業務參與狀態。如需詳細資訊，請參閱事件詳細資訊。	2022 年 11 月 16 日
將 PagerDuty 升級計畫和呼叫工作流程整合至事件管理員回應計劃	您現在可以將事件管理員與回應計劃整合， PagerDuty 並將 PagerDuty 服務新增至回應計劃。設定整合後，事件管理員可以在中為「事件管理員」中建立 PagerDuty 的每個新事件建立對應的事件。 PagerDuty 使用您在 PagerDuty 環境中定義的分頁工作流程和上報原則。 如需詳細資訊，請參閱下列主題： • 與事件管理器的產品和服務整合 • 將存 PagerDuty 取認證儲存在 AWS Secrets Manager 密碼中 • 將 PagerDuty 服務整合至主題的回應計劃 建立回應計劃 • 疑難排解	2022 年 11 月 16 日

啟動事件注意事件並更新了「事件詳細資料」畫	您可以使用事件備註與處理事件的其他使用者共同作業和通訊。此外，您也可以從「事件詳細資料」畫面檢視 Runbook 和業務參與狀態。如需詳細資訊，請參閱事件詳細資訊。	2022 年 11 月 16 日
複製組的標記支援	您現在可以在中為複製組指派標籤 AWS Systems Manager Incident Manager。這會增加現有的支援，可將標籤指派給複製組中 AWS 區域 指定的回應計劃、事件記錄和連絡人。如需詳細資訊，請參閱以下主題： • 準備精靈 • 標記事件管理員資源	2022 年 11 月 2 日
事件管理器與阿特拉西亞 Jira 服務管理集成	您可以使用「Jira 服務管理」的「服務管理」連接器，將「事件管理員」與「Jira AWS 服務管理」整合。設定整合之後，在「事件管理員」中建立的新事件會在 Jira 中建立對應的事件。如果您在事件管理員中更新事件，則更新會新增至 Jira 中對應的事件。如果您在「事件管理員」或「Jira」中解決事件，也會根據設定的偏好設定來解決對應的事件。如需詳細資訊，請參閱《服務管理連接器管理指南》中的〈設定 Jira AWS 服務管理〉。	2022 年 10 月 6 日

增強的標記支援	事件管理員支援將標籤指派給複製組中 AWS 區域 指定的回應計劃、事件記錄和連絡人。事件管理員還支持自動為響應計劃創建的事件分配標籤。如需詳細資訊，請參閱標記事件管理員資源。	2022 年 6 月 28 日
事件管理器整合 ServiceNow	您可以使用的 AWS 服務管理連接器ServiceNow來整合事件管理員與 ServiceNow。設定整合之後，在「事件管理員」中建立的新事件會在中建立對應的事件 ServiceNow。如果您在「事件管理員」中更新事件，更新會新增至中的對應事件 ServiceNow。如果您在「事件管理員」中解決事件 ServiceNow，或者，對應的事件也會根據設定的偏好設定來解決。如需詳細資訊，請參閱整合中的 AWS Systems Manager 事件管理員 ServiceNow。	2022 年 6 月 9 日
匯入聯絡資料	事件發生時，事件管理員可以使用語音或 SMS 通知來通知回應者。為了確保回應者能看到來自事件管理員的來電或簡訊通知，我們建議所有回應者將事件管理員虛擬卡片格式 (.vcf) 檔案下載至其行動裝置上的通訊錄。如需詳細資訊，請參閱將連絡人詳細資料匯入您的通訊錄。	2022 年 5 月 18 日

多項功能改進，可強化事件建立與補救	事件管理員推出了下列功能改良功能，以加強事件的建立與補救： • 在其他地方自動建立事件 AWS 區域：如果 Amazon CloudWatch 或 Amazon EventBridge 建立事件 AWS 區域 時無法使用事件管理員，這些服務現在會在複寫組中指定的其中一個可用區域中自動建立事件。如需詳細資訊，請參閱跨區域事件管理。 • 使用事件中繼資料自動填入 runbook 參數：您現在可以設定事件管理員，以便從事件收集資 AWS 源的相關資訊。事件管理員然後可以填入 Runbook 參數與收集的資訊。如需詳細資訊，請參閱教學課程：搭配事件管理員使用系統管理員自動化手冊。 • 自動收集 AWS 資源資訊：系統建立事件時，事件管理員現在會自動收集事件所涉及 AWS 資源的資訊。事件管理員接著會將這項資訊新增至「相關項目」標籤。	2022 年 5 月 17 日
多手冊支持	事件管理員現在支援在事件詳細資料頁面發生事件期間執行多個 Runbook。	2022 年 1 月 14 日

事件管理器在新推出 AWS 區域	事件管理員現已在下列新區域推出：美國西部 -1、東南 -2、AP-南 -1、CA-中央 -1、歐盟西部 -2、歐盟西部 -3。如需事件管理員區域和配額的詳細資訊，請參閱AWS 一般參考參考指南。	2021 年 11 月 8 日
主控台參與確認	您現在可以直接從「事件管理員」主控台確認參與。	2021 年 8 月 5 日
「屬性」頁	「事件管理員」在「未預期事件詳細資訊」頁面中加入了「特性」頁籤，提供有關未預期事件 OpsItem、父項和相關事件後分析的詳細資訊。	2021 年 8 月 3 日
事件管理器啟動	事件管理員是一個事件管理主控台，旨在協助使用者減輕影響其 AWS 託管應用程式的事件並從中復原。	2021 年 5 月 10 日

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。