aws

使用者指南

Incident Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Incident Manager: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS Systems Manager Incident Manager？ 1
主要元件和功能 1
使用 Incident Manager 的優點 2
相關服務 4
存取 Incident Manager 4
Incident Manager 區域和配額 4
Incident Manager 的定價 4
事件生命週期 5
提醒和參與 6
分類 7
調查和緩解 7
事後分析 8
設定 10
註冊 AWS 帳戶 10
建立具有管理存取權的使用者 10
授與程式設計存取權 12
Incident Manager 設定的必要角色 13
開始使用 14
先決條件 14
準備精靈 14
跨 AWS 帳戶 和 區域管理事件 20
跨區域事件管理 20
跨帳戶事件管理 20
最佳實務 21
設定跨帳戶事件管理 21
限制 22
準備事件 24
監控 26
設定複寫集和調查結果 26
複寫集 27
管理複寫集的標籤 28
管理問題清單功能 28
建立和設定聯絡人 29
聯絡管道 29

參與計劃 31
建立聯絡人 31
將聯絡人詳細資訊匯入您的通訊錄 32
使用隨叫隨到排程管理回應者輪換 32
建立通話中排程和輪換 33
管理現有的通話中排程 37
建立回應者參與的呈報計畫 42
階段 42
建立升級計畫 42
為回應者建立和整合聊天頻道 43
任務 1：建立或更新聊天頻道的 Amazon SNS 主題 44
任務 2：在聊天應用程式中建立 Amazon Q Developer 中的聊天頻道 45
任務 3：將聊天頻道新增至 Incident Manager 中的回應計劃 47
透過聊天管道互動 47
整合 Systems Manager Automation Runbook 進行事件修復 48
啟動和執行 Runbook 工作流程所需的 IAM 許可 49
使用 Runbook 參數 52
定義 Runbook 53
Incident Manager Runbook 範本 55
建立和設定回應計劃 56
建立回應計劃 56
識別來自其他服務之事件的潛在原因 62
啟用和建立問題清單的服務角色 62
設定跨帳戶調查結果支援的許可 63
自動或手動建立事件 64
使用 CloudWatch 警示自動建立事件 64
使用 EventBridge 事件自動建立事件 65
使用 SaaS 合作夥伴事件建立事件 65
使用 AWS 服務事件建立事件 67
手動建立事件 68
手動啟動事件所需的 IAM 許可 69
在主控台中檢視事件詳細資訊 71
在主控台中檢視事件清單 71
在主控台中檢視事件詳細資訊 71
頂端橫幅 72
事件備註 72

標籤 73
概觀 73
診斷 73
時間表 75
執行手冊 75
參與 76
相關項目 76
屬性 77
執行事後分析 78
分析詳細資訊 78
概觀 78
指標 78
時間表 79
問題 79
動作 80
檢查清單 80
分析範本 80
AWS 標準範本 80
建立分析範本 80
建立分析 81
列印格式化的事件分析 81
教學課程 82
搭配 Incident Manager 使用 Runbook 82
任務 1：建立 Runbook 83
任務 2：建立 IAM 角色 86
任務 3：將 Runbook 連接到您的回應計劃 88
任務 4：將 CloudWatch 警示指派給您的回應計劃 88
任務 5：驗證結果 89
管理安全事件 90
標記 資源 92
安全 94
資料保護 94
資料加密 95
身分和存取權管理 97
目標對象 97
使用身分驗證 98

使用政策管理存取權 101
AWS Systems Manager Incident Manager 如何使用 IAM 103
身分型政策範例 109
資源型政策範例 113
預防跨服務混淆代理人 114
使用服務連結角色 115
AWS Incident Manager 的 受管政策 118
故障診斷 124
在 Incident Manager 中使用共用聯絡人和回應計劃 126
共用聯絡人和回應計畫的先決條件 126
相關服務 127
共用聯絡或回應計畫 127
停止共用聯絡人或回應計劃 127
識別共用聯絡人或回應計劃 128
共用聯絡和回應計畫許可 128
計費和計量 129
執行個體限制 129
法規遵循驗證 129
恢復能力 130
基礎架構安全 130
使用 VPC 端點 (AWS PrivateLink) 131
Incident Manager VPC 端點的考量事項 131
為 Incident Manager 建立介面 VPC 端點 131
為 Incident Manager 建立 VPC 端點政策 132
組態與漏洞分析 133
安全最佳實務 133
Incident Manager 的預防性安全最佳實務 133
Incident Manager 的 Detective 安全最佳實務 134
監控 136
使用 Amazon CloudWatch 監控指標 136
在 CloudWatch 主控台上檢視 Incident Manager 指標 138
指標的維度 138
使用 記錄 API 呼叫 AWS CloudTrail 139
CloudTrail 中的 Incident Manager 管理事件 140
Incident Manager 事件範例 141
產品和服務整合 143

與 整合 AWS 服務 143
與其他產品及服務整合 146
將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中 150
故障診斷 156
錯誤訊息：ValidationException – We were unable to validate the AWS Secrets Manager secret 156
其他疑難排解問題 157
文件歷史紀錄 158
..... clxx

什麼是 AWS Systems Manager Incident Manager？

Incident Manager 是 中的工具 AWS Systems Manager，旨在協助您減輕並復原影響託管應用程式的事件 AWS。

就 而言 AWS，事件是指任何非預期的中斷或服務品質降低，可能會對業務營運產生重大影響。因此，組織必須建立回應策略，以有效地緩解和復原事件，並實作動作來防止未來的事件。

Incident Manager 有助於縮短解決事件的時間，方法如下：

- 提供自動化計劃，以有效率地吸引負責回應事件的人員。
- 提供相關的故障診斷資料。
- 使用預先定義的 Automation Runbook 啟用自動回應動作。
- 提供與所有利益相關者協作和溝通的方法。

內建於 Incident Manager 的功能和工作流程，是以 Amazon 自成立以來幾乎一直在開發的事件回應最佳實務為基礎。Incident Manager 與 整合， AWS 服務 例如 Amazon CloudWatch AWS CloudTrail AWS Systems Manager、 和 Amazon EventBridge。

主要元件和功能

本節說明您用來設定事件回應計劃的 Incident Manager 功能。

回應計劃

回應計畫可做為範本，定義事件發生時必須到位的項目。它包含以下資訊：

- 事件發生時，需要回應的人員。
- 建立的自動化回應，以緩解事件。
- 回應者必須使用的協作工具來通訊和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，在偵測到影響 AWS 資源的條件或變更時建立事件。

Runbook 自動化支援

您可以從 Incident Manager 內啟動 Automation Runbook，以自動化對事件的關鍵回應，並提供詳細步驟給第一個回應者。

參與和呈報

參與計畫會指定每個人針對每個唯一事件通知 。您可以指定已新增至 Incident Manager 的個別聯絡人，或指定您在 Incident Manager 中建立的待命排程。參與計劃也會指定呈報路徑，以協助確保利益相關者之間的可見性，以及在事件回應過程中主動參與。

待命排程

Incident Manager 中的待命排程包含您為排程建立的一或多個輪換。每次輪換時，您最多可以包含 30 個聯絡人。新增至呈報計劃或回應計劃時，隨需排程會定義發生需要回應者介入的事件時，通知的人員。隨需排程有助於確保事件回應所需的完整備援全年無休涵蓋範圍。

主動協同合作

事件回應者透過與聊天應用程式用戶端中的 Amazon Q 開發人員整合主動回應事件。聊天應用程式中的 Amazon Q Developer 支援為使用 Slack、 Microsoft Teams或 Amazon Chime 的 Incident Manager 建立聊天頻道。回應者可以直接彼此通訊、接收有關事件的自動通知，以及Microsoft Teams直接在 Slack和 中執行一些 Incident Manager 命令列界面 (CLI) 操作。

事件診斷

在事件發生期間，回應者可以在 Incident Manager 主控台中檢視up-to-date。根據資訊中的變更，回應者接著可以建立後續項目，並使用 Automation Runbook 進行修復。

來自其他服務的調查結果

若要支援回應者的事件診斷，您可以在 Incident Manager 中啟用調查結果功能。調查結果是有關在事件發生前後發生的 AWS CodeDeploy 部署和 AWS CloudFormation 堆疊更新，以及可能涉及與事件相關的一或多個資源的資訊。擁有此資訊可縮短評估潛在原因所需的時間，進而減少從事件復原的平均時間 (MTTR)。

事後分析

事件解決後，您可以使用事件後分析來識別事件回應的改進，包括偵測和緩解的時間。分析也可以協助您了解事件的根本原因。Incident Manager 會建立建議的後續動作項目，供您用來改善事件回應。

使用 Incident Manager 的優點

了解在事件偵測和回應操作中使用 Incident Manager 的好處。

本節說明您的組織在實作 Incident Manager 回應計劃時可以獲得的優勢。

有效且立即地診斷問題

您設定的 Amazon CloudWatch 警示和 Amazon EventBridge 事件，可在您的服務品質發生任何意外中斷或降低時自動建立事件。

CloudWatch 警示會偵測並報告指標或表達式的值在多個期間內相對於閾值的變更。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。當您建立警示或事件時，您可以指定要在 Incident Manager 中建立事件的動作，以及適當的回應計劃，以促進事件的參與、升級和緩解。

Incident Manager 可讓您透過使用 CloudWatch 指標，自動收集和追蹤與事件相關的指標。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，以為事件中的回應者提供額外的內容和資料。

使用 Incident Manager 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，以描述他們做了什麼或發生了什麼。自動化的興趣點包括：

- CloudWatch 警示或 EventBridge 規則會建立事件。
- 事件指標會報告給 Incident Manager。
- 回應者已參與。
- Runbook 步驟已成功完成。

有效參與

Incident Manager 透過使用聯絡人、待命排程、升級計畫和聊天管道，將事件回應者集合在一起。您可以直接在 Incident Manager 中定義個別聯絡人，並指定聯絡偏好設定（電子郵件、簡訊或語音）。您可以將聯絡人新增至通話中排程輪換，以判斷在特定期間內處理事件的參與對象。使用定義的聯絡人和通話中排程，您可以建立升級計劃，以在事件發生期間適時與必要的回應者互動。

即時協作

事件期間的通訊是更快解決的關鍵。在聊天應用程式中使用 Amazon Q 開發人員 用戶端設定使用 Slack、 Microsoft Teams或 Amazon Chime，您可以在他們偏好的連線聊天頻道中將回應者集合在一起，讓他們直接與事件互動，並彼此互動。Incident Manager 也會在聊天頻道中顯示事件回應者的即時動作，為其他人提供內容。

自動化服務還原

Incident Manager 可讓您的回應者專注於透過使用 Automation Runbook 解決事件所需的關鍵任務。在 Incident Manager 中，執行手冊是為解決事件而採取的一系列預先定義動作。它們會視需要結合自動化任務的強大功能與手動步驟，讓回應者更易於分析和回應影響。

防止未來的事件

使用 Incident Manager 事件後分析，您的團隊可以開發更強大的回應計劃，並影響應用程式之間的變更，以防止未來的事件和停機時間。事件後分析也提供反覆學習和改善 Runbook、回應計劃和指標。

相關服務

Incident Manager 與數個其他 AWS 服務 和第三方服務和工具整合，以協助您偵測和解決事件，以及間接與其 API 操作互動和管理基礎設施。如需相關資訊，請參閱 與 Incident Manager 的產品和服務整合。

存取 Incident Manager

您可以透過下列任何方式存取 Incident Manager：

- Incident Manager 主控台
- AWS CLI – 如需一般資訊，請參閱AWS Command Line Interface 《 使用者指南》中的 入門 AWS CLI。如需 Incident Manager 的 CLI 命令相關資訊，請參閱 AWS CLI 命令參考ssm-contacts中的ssm-incidents和 。
- Incident Manager API – 如需詳細資訊，請參閱 AWS Systems Manager Incident Manager API 參考。
- AWS SDKs – 如需詳細資訊，請參閱要建置的工具 AWS。

Incident Manager 區域和配額

Systems Manager 不支援所有 AWS 區域 支援的 Incident Manager。

若要檢視有關 Incident Manager 區域和配額的資訊，請參閱 中的AWS Systems Manager Incident Manager 端點和配額Amazon Web Services 一般參考。

Incident Manager 的定價

使用 Incident Manager 需要付費。如需詳細資訊，請參閱 AWS Systems Manager 定價。

> **Note**
>
> 與此服務相關的其他 AWS 服務、 AWS 內容和第三方內容可能需另外付費，並受其他條款的約束。

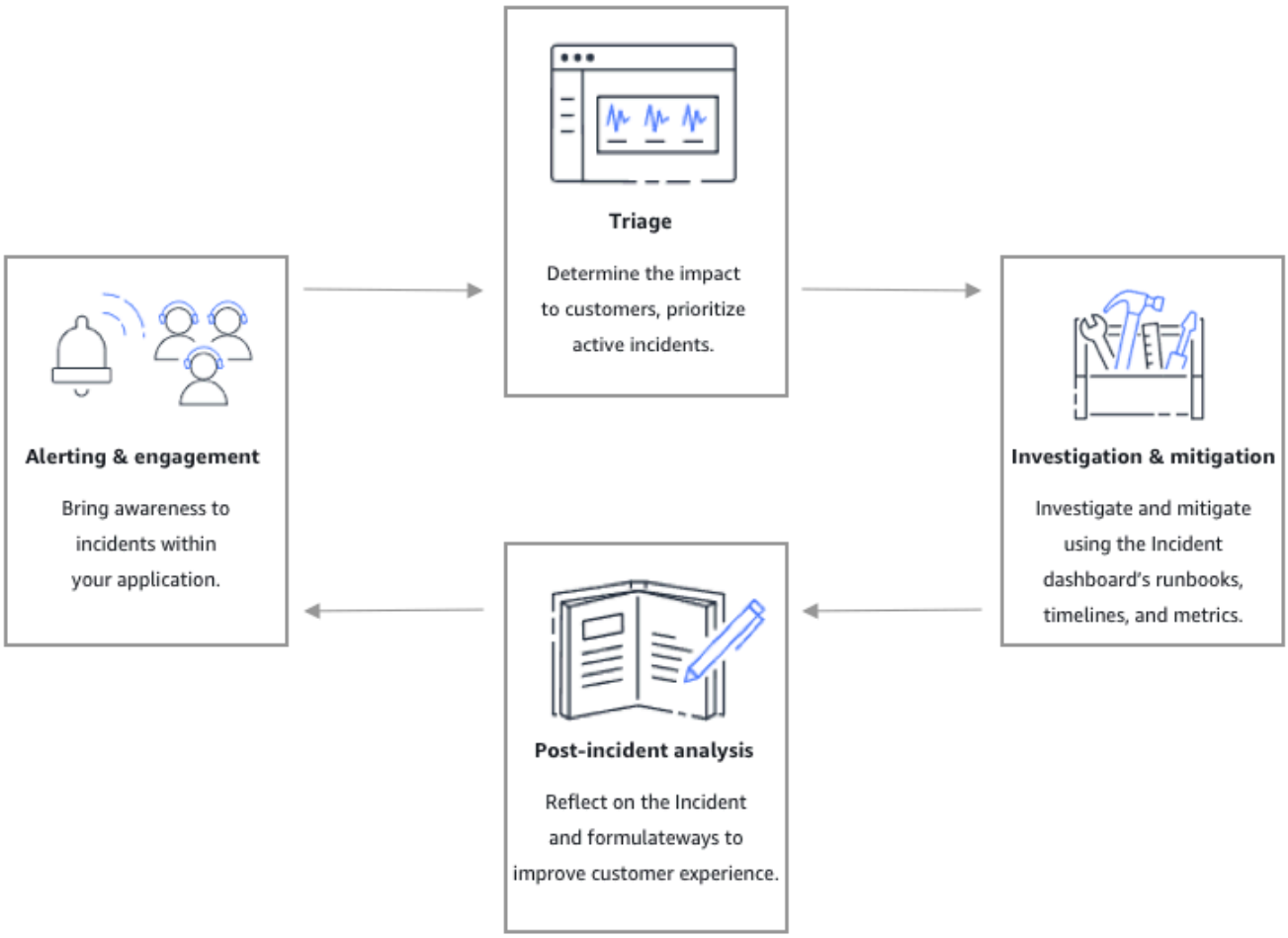
如需 的概觀 Trusted Advisor，此服務可協助您最佳化 AWS 環境的成本、安全性和效能，請參閱 AWS 支援 使用者指南AWS Trusted Advisor中的 。

Incident Manager 中的事件生命週期

AWS Systems Manager Incident Manager 根據最佳實務提供step-by-step架構，以識別和回應事件，例如服務中斷或安全威脅。Incident Manager 的主要重點是協助透過完整的事件生命週期管理解決方案，盡快將受影響的服務或應用程式還原至正常狀態。

如下圖所示，Invent Manager 為事件生命週期的每個階段提供工具和最佳實務：

- 提醒和參與
- 分類
- 調查和緩解
- 事後分析



提醒和參與

事件生命週期的提醒和參與階段著重於將意識帶入應用程式和服務內的事件。此階段會在偵測到事件之前開始，且需要深入了解您的應用程式。您可以使用 Amazon CloudWatch 指標來監控應用程式效能的資料，或使用 Amazon EventBridge 彙整來自不同來源、應用程式和服務的提醒。設定應用程式監控之後，您可以開始提醒偏離歷史常態的指標。若要進一步了解監控最佳實務，請參閱 監控。

若要支援回應者的事件診斷，您可以在 Incident Manager 中啟用調查結果功能。調查結果是有關事件發生前後發生的 AWS CodeDeploy 部署和 AWS CloudFormation 堆疊更新的資訊。擁有此資訊可縮短評估潛在原因所需的時間，進而減少從事件復原的平均時間 (MTTR)。

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。若要進一步了解如何建立回應計劃，請參閱 在 Incident Manager 中建立和設定回應計劃。Amazon EventBridge 事件

或 CloudWatch Alarms 可以使用 搭配回應計劃作為範本來自動建立事件。若要進一步了解事件建立，請參閱 在 Incident Manager 中自動或手動建立事件。

回應計劃會啟動相關的呈報計劃和參與計劃，將第一個回應者帶入事件。如需設定升級計劃的詳細資訊，請參閱建立升級計畫。同時，聊天應用程式中的 Amazon Q Developer 會使用聊天管道通知回應者，引導他們前往事件詳細資訊頁面。使用聊天管道和事件詳細資訊，團隊可以溝通和分類事件。如需在 Incident Manager 中設定聊天頻道的詳細資訊，請參閱 任務 2：在聊天應用程式中建立 Amazon Q Developer 中的聊天頻道。

分類

分類是指第一個回應者嘗試判斷對客戶的影響。Incident Manager 主控台中的事件詳細資訊檢視會提供回應者時間表和指標，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、解決方案和通訊奠定了基礎。回應者使用影響評分從 1（關鍵）到 5（無影響）來排定事件的優先順序。

您的組織可以定義每個影響評分的確切範圍，無論您選擇的為何。下表提供通常如何定義每個影響層級的範例。

影響碼	影響名稱	範例定義的範圍
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故障。
3	Medium	部分應用程式故障會影響客戶。
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，但需要採取緊急動作以避免影響。

調查和緩解

事件詳細資訊檢視可為您的團隊提供 Runbook、時間表和指標。若要了解如何使用事件，請參閱 在主控台中檢視事件詳細資訊。

Runbook 通常提供調查步驟，並且可以自動提取資料或嘗試常用的解決方案。Runbook 也提供明確、可重複的步驟，讓您的團隊發現這些步驟有助於緩解事件。Runbook 索引標籤著重於目前的 Runbook 步驟，並顯示過去和未來的步驟。

Incident Manager 與 Systems Manager Automation 整合，以建置 Runbook。使用 Runbook 執行下列任何動作：

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

如需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 Automation 動作參考。

時間軸索引標籤會顯示已採取的動作。時間軸會使用時間戳記記錄每個 ，並自動建立詳細資訊。若要將自訂事件新增至時間軸，請參閱本使用者指南的事件詳細資訊頁面中的時間表一節。

診斷索引標籤會顯示自動填入的指標和手動新增的指標。此檢視會在事件期間提供寶貴的應用程式活動資訊。

參與索引標籤可讓您將其他聯絡人新增至事件，並協助為參與的聯絡人提供資源，以便在事件發生後快速趕上進度。聯絡人是透過定義的呈報計畫或個人參與計畫來參與。

使用聊天頻道，您可以直接與事件和團隊中的其他回應者互動。在聊天應用程式中使用 Amazon Q Developer，您可以在 Slack、 Microsoft Teams和 Amazon Chime 中設定聊天頻道。在 Slack和 Microsoft Teams頻道中，回應者可以使用多個`ssm-incidents`命令，直接從聊天頻道與事件互動。如需詳細資訊，請參閱透過聊天管道互動。

事後分析

Incident Manager 提供架構，用於反映事件、採取必要步驟，防止事件在未來再次發生，並改善整體的事件回應活動。改善項目可能包括：

- 事件中涉及的應用程式變更。您的團隊可以利用這段時間來改善系統，並提高容錯能力。
- 事件回應計劃的變更。花時間納入學到的教訓。
- Runbook 的變更。您的團隊可以深入探討解決方案所需的步驟，以及您可以自動化的步驟。
- 提醒的變更。事件發生後，您的團隊可能注意到指標中的關鍵點，您可以使用這些指標來更快地提醒團隊有關事件的事項。

Incident Manager 透過使用一組事後分析問題和動作項目，以及事件時間表，來促進這些潛在的改進。若要進一步了解透過分析改善，請參閱 在 Incident Manager 中執行事件後分析。

設定 AWS Systems Manager Incident Manager

我們建議您在用來管理 操作的帳戶中設定 AWS Systems Manager Incident Manager。第一次使用 Incident Manager 之前，請先完成下列任務：

主題

- 註冊 AWS 帳戶
- 建立具有管理存取權的使用者
- 授與程式設計存取權
- Incident Manager 設定的必要角色

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。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。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立 管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。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)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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 Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center《 使用者指南》中的使用預設值設定使用者存取權 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 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 Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》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 Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

授與程式設計存取權

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS Management Console。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

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	根據
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《 使用者指南》中的設定 AWS CLI 要使用 AWS IAM Identity Center的 。 • AWS SDKs、工具和 AWS APIs，請參閱 AWS SDKs 和工具參考指南中的 IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	遵循《IAM 使用者指南》中將臨時登入資料與 AWS 資源搭配使用的指示。
IAM	(不建議使用) 使用長期登入資料來簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《 使用者指南》中的使用 IAM 使用者憑證進行身分驗證。 • AWS SDKs和工具，請參閱 AWS SDKs和工具參考指

哪個使用者需要程式設計存取權？	到	根據
		南中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，請參閱《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰。

Incident Manager 設定的必要角色

開始之前，您的帳戶必須具有 IAM 許可 `iam:CreateServiceLinkedRole`。Incident Manager 會使用此許可在您的`AWSServiceRoleforIncidentManager`帳戶中建立 。如需詳細資訊，請參閱針對 Incident Manager 使用服務連結角色。

Incident Manager 入門

本節逐步解說 Incident Manager 主控台中的準備。您需要在主控台中完成準備，才能將其用於事件管理。精靈會逐步引導您設定複寫集、至少一個聯絡人和一個呈報計畫，以及第一個回應計畫。下列指南將協助您了解 Incident Manager 和事件生命週期：

- 什麼是 AWS Systems Manager Incident Manager？
- Incident Manager 中的事件生命週期

先決條件

如果您是第一次使用 Incident Manager，請參閱 設定 AWS Systems Manager Incident Manager。我們建議您在用來管理 操作的帳戶中設定 Incident Manager。

建議您先完成 Systems Manager 快速設定，再開始 Incident Manager 準備精靈。使用 Systems Manager 快速設定，以建議的最佳實務設定常用 AWS 服務和功能。Incident Manager 使用 Systems Manager 功能來管理與您的 相關聯的事件， AWS 帳戶 以及先設定 Systems Manager 的好處。

準備精靈

第一次使用 Incident Manager 時，您可以從 Incident Manager 服務首頁存取 Get prepared 精靈。若要在第一次完成設定後存取準備精靈，請在事件清單頁面上選擇準備。

1. 開啟 Incident Manager 主控台。
2. 在 Incident Manager 服務首頁上，選擇準備。

一般設定

1. 在一般設定下，選擇設定。
2. 閱讀條款和條件。若您同意 Incident Manager 的條款與條件，請選取我已閱讀並同意 Incident Manager 的條款與條件，然後選擇下一步。
3. 在區域區域中，您目前的 AWS 區域 會顯示為複寫集的第一個區域。若要將更多區域新增至複寫集，請從區域清單中選擇它們。

   我們建議至少包含兩個區域。如果某個區域暫時無法使用，事件相關的活動仍然可以路由到另一個區域。

> **Note**
>
> 建立複寫集會在您的帳戶中建立`AWSServiceRoleforIncidentManager`服務連結角色。若要進一步了解此角色，請參閱 針對 Incident Manager 使用服務連結角色。

4. 若要設定複寫集的加密，請執行下列其中一項操作：

> **Note**
>
> 所有 Incident Manager 資源都會加密。若要進一步了解如何加密您的資料，請參閱 Incident Manager 中的資料保護。如需 Incident Manager 複寫集的詳細資訊，請參閱 設定 Incident Manager 複寫集。

- 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，請選擇選擇現有的 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 Resource Name (ARN)。

> **Tip**
>
> 如果您沒有可用的 AWS KMS key，請選擇建立 AWS KMS key。

5. （選用）在標籤區域中，將一或多個標籤新增至複寫集。標籤包含索引鍵和選擇性的值。

   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Incident Manager 中的標記資源。

6. （選用）在服務存取區域中，若要啟用問題清單功能，請在此帳戶核取方塊中選擇建立問題清單的服務角色。

   問題清單是有關在建立事件時大約同時發生的程式碼部署或基礎設施變更的資訊。問題清單可以檢查為事件的潛在原因。這些潛在原因的相關資訊會新增至事件的事件詳細資訊頁面。透過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，請選擇檢視許可詳細資訊。

7. 選擇建立。

   若要進一步了解複寫集和彈性，請參閱 中的彈性 AWS Systems Manager Incident Manager。

聯絡人 (在準備期間選用)

Incident Manager 會在事件期間與聯絡人互動。如需聯絡的詳細資訊，請參閱 在 Incident Manager 中建立和設定聯絡人。

1. 選擇建立聯絡人。
2. 在名稱中，輸入聯絡人的名稱。
3. 針對唯一別名，輸入別名以識別此聯絡人。
4. 在聯絡管道區段中，執行下列動作來定義在事件期間聯絡的參與方式：

   a. 針對類型，選擇電子郵件、簡訊或語音。

   b. 針對頻道名稱，輸入唯一的名稱，以協助您識別頻道。

   c. 針對詳細資訊，輸入聯絡人的電子郵件地址或電話號碼。

      電話號碼必須有 9 到 15 個字元，並以 開頭，+後面接著國碼和訂閱者號碼。

   d. 若要建立另一個聯絡管道，請選擇新增聯絡管道。我們建議為每個聯絡人定義至少兩個頻道。

5. 在業務開發計劃區域中，執行下列動作來定義通知聯絡人的管道，以及透過每個管道等待確認的時間。

   > **Note**
   >
   > 我們建議在參與計畫中定義至少兩個管道。

   a. 針對聯絡管道名稱，選擇您在聯絡管道區域中指定的管道。

   b. 針對參與時間 （分鐘），輸入參與聯絡管道之前要等待的分鐘數。

      我們建議您在互動開始時至少選取一個裝置來互動，並指定 **0**（零） 分鐘的等待時間。

   c. 若要將更多聯絡管道新增至參與計畫，請選擇新增參與。

6. （選用） 在標籤區域中，將一或多個標籤新增至聯絡人。標籤包含索引鍵和選擇性的值。

   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Incident Manager 中的標記資源。

7. 若要建立聯絡記錄並將啟用碼傳送至定義的聯絡管道，請選擇建立。
8. （選用）在聯絡管道啟用頁面中，輸入傳送至每個管道的啟用碼。

   如果您現在無法輸入代碼，稍後可以產生新的啟用代碼。
9. 若要新增其他聯絡人，請選擇建立聯絡人並重複上述步驟。

(準備期間選用）呈報計畫

1. 選擇建立呈報計畫。

   呈報計畫會在事件期間透過您的聯絡人呈報，確保 Incident Manager 在事件期間與正確的回應者互動。如需升級計劃的詳細資訊，請參閱 在 Incident Manager 中建立回應者參與的呈報計畫。
2. 在名稱中，輸入呈報計畫的唯一名稱。
3. 針對別名，輸入唯一的別名，以協助您識別呈報計畫。
4. 在階段 1 區域中，執行下列動作：

   a. 對於呈報管道，選擇要互動的聯絡管道。

   b. 如果您希望聯絡案例能夠停止升級計畫階段的進度，請選取確認停止計畫進度。

   c. 若要將更多頻道新增至階段，請選擇新增升級頻道。
5. 若要在升級計畫中建立新的階段，請選擇新增階段並新增其階段詳細資訊。
6. （選用）在標籤區域中，將一或多個標籤新增至呈報計畫。標籤包含索引鍵和選擇性的值。

   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Incident Manager 中的標記資源。
7. 選擇建立呈報計畫。

反應計劃

> **Note**
>
> 您可能需要返回 Incident Manager 開始頁面，然後選擇準備以繼續。

1. 選擇建立回應計畫。

   使用回應計劃來組合您建立的聯絡和呈報計劃。

在此入門精靈期間，下列各節是選用的，特別是如果您是第一次設定回應計劃：

- 聊天頻道
- 執行手冊
- 業務開發
- 第三方整合

如需稍後將這些元素新增至回應計畫的資訊，請參閱 在 Incident Manager 中準備事件。

2. 在名稱中，輸入回應計劃的唯一可識別名稱。名稱用於建立回應計畫 ARN，或在沒有顯示名稱的回應計畫中。
3. （選用）針對顯示名稱，輸入名稱，協助您在建立事件時識別此回應計劃。
4. 針對標題，輸入標題以協助識別與此回應計畫相關的事件類型。

   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。
5. 針對影響，選取您預期與此回應計畫相關的事件影響程度，例如 **`Critical`**或 **`Low`**。
6. （選用）針對摘要，輸入用於提供事件概觀的簡短描述。Incident Manager 會在事件期間自動將相關資訊填入摘要中。
7. （選用）針對 Dedupe 字串，輸入 dedupe 字串。Incident Manager 使用此字串來防止相同的根本原因在同一個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詞彙或片語。如果您指定重複資料刪除字串，則 Incident Manager 會在建立事件時，在 `dedupeString` 欄位中搜尋包含相同字串的開啟事件。如果偵測到重複，Incident Manager 會將較新的事件刪除重複到現有的事件中。

   > **Note**
   >
   > 根據預設，Incident Manager 會自動刪除由相同 Amazon CloudWatch 警示或 Amazon EventBridge 事件建立的多個事件。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的重複。

8. （選用）在事件標籤區域中，將一或多個標籤新增至回應計劃。標籤包含索引鍵和選擇性的值。

   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Incident Manager 中的標記資源。
9. 從業務開發下拉式清單中選取要套用至事件的聯絡人和呈報計劃。

10. 選擇建立回應計畫。

建立回應計劃之後，您可以將 Amazon CloudWatch 警示或 Amazon EventBridge 事件與回應計劃建立關聯。這會根據警示或事件自動建立事件。如需詳細資訊，請參閱在 Incident Manager 中自動或手動建立事件。

在 Incident Manager 中管理跨 AWS 帳戶 和 區域的事件

您可以設定 中的 Incident Manager 工具 AWS Systems Manager，以使用多個 AWS 區域 和 帳戶。本節說明跨區域和跨帳戶最佳實務、設定步驟和已知限制。

主題

- 跨區域事件管理
- 跨帳戶事件管理

跨區域事件管理

Incident Manager 支援在數個 AWS 區域中自動和手動建立事件。當您一開始使用 Get prepared 精靈加入 Incident Manager 時，您最多可以為複寫集指定三個 AWS 區域 。對於 Amazon CloudWatch 警示或 Amazon EventBridge 事件自動建立的事件，Avent Manager 會嘗試在與事件規則或警示相同的 中建立 AWS 區域 事件。如果 Incident Manager 在該區域中遇到中斷，則 CloudWatch 或 EventBridge 會自動在複寫資料所在的另一個區域中建立事件。

> **Important**
>
> 請注意以下重要詳細資訊。
>
> - 我們建議您 AWS 區域 在複寫集中至少指定兩個 。如果您未指定至少兩個區域，系統將無法在 Incident Manager 無法使用期間建立事件。
> - 跨區域容錯移轉建立的事件不會叫用回應計劃中指定的 Runbook。

如需使用 Incident Manager 加入和指定其他區域的詳細資訊，請參閱 Incident Manager 入門。

跨帳戶事件管理

Incident Manager 使用 AWS Resource Access Manager (AWS RAM) 跨管理和應用程式帳戶共用 Incident Manager 資源。本節說明跨帳戶最佳實務、如何為 Incident Manager 設定跨帳戶功能，以及 Incident Manager 中跨帳戶功能的已知限制。

管理帳戶是您執行操作管理的帳戶。在組織設定中，管理帳戶擁有回應計劃、聯絡人、呈報計劃、執行手冊和其他 AWS Systems Manager 資源。

應用程式帳戶是擁有組成您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 資料表，或您用來在 中建置應用程式的任何其他資源 AWS 雲端。應用程式帳戶也擁有在 Incident Manager 中建立事件的 Amazon CloudWatch 警示和 Amazon EventBridge 事件。

AWS RAM 使用資源共用在帳戶之間共用資源。您可以在 的帳戶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業務參與和事件互動。共用回應計劃會共用使用該回應計劃建立的所有過去和未來事件。共用聯絡人會共用聯絡人或回應計劃的所有過去和未來互動。

最佳實務

在跨帳戶共用您的 Incident Manager 資源時，請遵循以下最佳實務：

- 定期使用回應計劃和聯絡人更新資源共享。
- 定期檢閱資源共享主體。
- 在管理帳戶中設定 Incident Manager、Runbook 和聊天頻道。

設定跨帳戶事件管理

下列步驟說明如何設定和設定 Incident Manager 資源，並將其用於跨帳戶功能。您可能在過去已為跨帳戶功能設定了一些服務和資源。使用跨帳戶資源啟動第一個事件之前，請使用下列步驟做為需求檢查清單。

1. （選用）使用 建立組織和組織單位 AWS Organizations。請遵循 AWS Organizations 使用者指南中的教學課程：建立和設定組織。
2. （選用）使用 Quick Setup，這是其中的工具 AWS Systems Manager，可設定您在設定跨帳戶 Runbook 時使用的正確 AWS Identity and Access Management 角色。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 快速設定。
3. 請遵循 AWS Systems Manager 使用者指南中的在多個 AWS 區域 和 帳戶中執行自動化中列出的步驟，在 Systems Manager 自動化文件中建立 Runbook。Runbook 可由管理帳戶或您的其中一個應用程式帳戶執行。根據您的使用案例，您將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 Runbook。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 IDs。此角色會讓您的應

用程式帳戶從事件詳細資訊頁面讀取 Runbook 的狀態。應用程式帳戶必須安裝 AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 範本。事件詳細資訊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。此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. （選用）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 管理帳戶的帳戶 ID。此角色提供 Incident Manager 存取部署和 AWS CloudFormation 堆疊更新相關資訊 AWS CodeDeploy 所需的許可。如果啟用問題清單功能，則會將此資訊報告為事件的問題清單。如需詳細資訊，請參閱在 Incident Manager 中將來自其他服務的事件的潛在原因識別為「尋找」。
5. 若要設定和建立聯絡人、呈報計劃、聊天管道和回應計劃，請遵循 中詳述的步驟在 Incident Manager 中準備事件。
6. 將聯絡人和回應計劃資源新增至現有的資源共用或新的資源共用 AWS RAM。如需詳細資訊，請參閱「 AWS RAM使用者指南」中的 AWS RAM 入門。新增回應計劃， 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。新增聯絡人和呈報計劃， AWS RAM 讓應用程式帳戶能夠檢視參與，並從事件儀表板參與聯絡人。
7. 將跨帳戶跨區域功能新增至 CloudWatch 主控台。如需步驟和資訊，請參閱《Amazon CloudWatch 使用者指南》中的跨帳戶跨區域 CloudWatch 主控台。 Amazon CloudWatch 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. 建立跨帳戶 Amazon EventBridge 事件匯流排。如需步驟和資訊，請參閱AWS 在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來建立事件規則，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 Incident Manager 跨帳戶功能的已知限制：

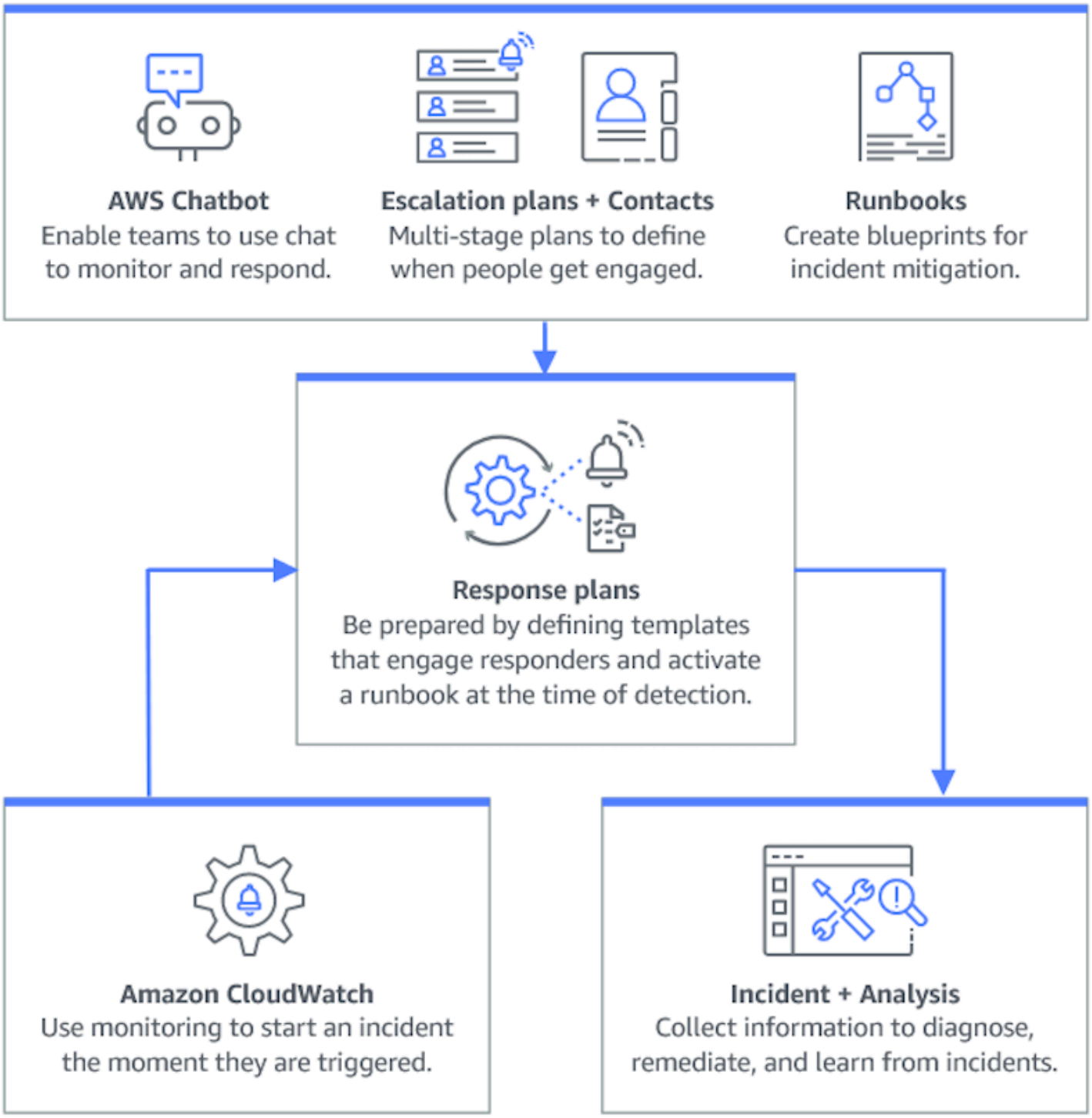
- 建立事後分析的帳戶是唯一可以檢視和變更的帳戶。如果您使用應用程式帳戶來建立事件後分析，則只有該帳戶的成員可以檢視和變更它。如果您使用管理帳戶來建立事件後分析，也是如此。

- 在應用程式帳戶中執行的自動化文件不會填入時間軸事件。在應用程式帳戶中執行的自動化文件更新，可見於事件的 Runbook 索引標籤。

- Amazon Simple Notification Service 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。
- 呈報計畫只能使用相同帳戶中的聯絡人建立。與您共用的聯絡人無法新增至您帳戶中的呈報計畫。
- 套用至回應計劃、事件記錄和聯絡人的標籤只能從資源擁有者帳戶檢視和修改。

在 Incident Manager 中準備事件

事件的規劃在事件生命週期之前很長的時間開始。如下圖所示，在開始回應事件之前，您可以透過設定聊天頻道、建立升級計畫、指定聯絡人，以及決定要在事件回應中使用的自動化 Runbook 來做好準備。然後，使用回應計畫來指定監控的發生方式，以及回應是否自動化。修復完成後，您可以分析事件和事件回應，以進一步完善未來事件的回應計劃。



主題

- 監控
- 在 Incident Manager 中設定複寫集和調查結果
- 在 Incident Manager 中建立和設定聯絡人

- 在 Incident Manager 中使用隨叫隨到排程管理回應者輪換
- 在 Incident Manager 中建立回應者參與的呈報計畫
- 在 Incident Manager 中為回應者建立和整合聊天頻道
- 將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件
- 在 Incident Manager 中建立和設定回應計劃
- 在 Incident Manager 中將來自其他服務的事件的潛在原因識別為「尋找」

監控

監控 AWS 託管應用程式的運作狀態是確保應用程式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有多重要。
- 失敗的常見性 – 系統失敗的頻率；需要頻繁介入的系統應受到密切監控。
- 延遲增加 – 完成任務的時間已增加或減少。
- 用戶端與伺服器端指標 – 如果用戶端與伺服器上的相關指標之間存在差異。
- 相依性失敗 – 您的團隊可以和應該準備的失敗。

建立回應計劃之後，您可以使用監控解決方案，在事件發生時自動追蹤事件。如需事件追蹤和建立的詳細資訊，請參閱 在 Incident Manager 主控台中檢視事件詳細資訊。

如需建構安全、高效能、彈性和高效基礎設施應用程式和工作負載的詳細資訊，請參閱 AWS Well-Architected。

在 Incident Manager 中設定複寫集和調查結果

完成 Incident Manager 準備精靈後，您可以在設定頁面上管理特定選項。這些選項包括複寫集、套用至複寫集的標籤，以及問題清單功能。

主題

- 設定 Incident Manager 複寫集
- 管理複寫集的標籤
- 管理問題清單功能

設定 Incident Manager 複寫集

Incident Manager 複寫集會將您的資料複寫至許多 ， AWS 區域 以執行下列動作：

- 增加跨區域備援
- 允許 Incident Manager 存取不同區域中的資源，並減少使用者的延遲。
- 使用 AWS 受管金鑰 或您自己的客戶受管金鑰來加密您的資料。

  預設會加密所有 Incident Manager 資源。若要進一步了解 資源的加密方式，請參閱 Incident Manager 中的資料保護。

若要開始使用 Incident Manager，請先使用 Get prepared 精靈建立複寫集。若要進一步了解如何在 Incident Manager 中做好準備，請參閱 準備精靈。

編輯複寫集

透過使用 Incident Manager 設定頁面，您可以編輯複寫集。您可以新增區域、刪除區域，以及啟用或停用複寫集刪除保護。您無法編輯用來加密資料的金鑰。若要變更金鑰，請刪除並重新建立複寫集。

新增區域

1. 開啟 Incident Manager 主控台，然後在左側導覽窗格中選擇設定。
2. 選擇新增區域。
3. 選取區域。
4. 選擇新增。

刪除區域

1. 開啟 Incident Manager 主控台，然後在左側導覽窗格中選擇設定。
2. 選取您要刪除的區域。
3. 選擇 刪除。
4. 在文字方塊中輸入 Delete，然後選擇 Delete。

刪除複寫集

刪除複寫集中的最後一個區域會刪除整個複寫集。在您可以刪除最後一個區域之前，請先關閉設定頁面上的刪除保護，以停用刪除保護。刪除複寫集後，您可以使用 Get prepared 精靈建立新的複寫集。

若要從複寫集刪除區域，請在建立區域後等待 24 小時。嘗試在建立複寫集後 24 小時內刪除區域會導致刪除失敗。

刪除複寫集會刪除所有 Incident Manager 資料。

刪除複寫集

1. 開啟 Incident Manager 主控台，然後在左側導覽窗格中選擇設定。
2. 選取複寫集中的最後一個區域。
3. 選擇 刪除。
4. 在文字方塊中輸入 Delete，然後選擇 Delete。

管理複寫集的標籤

標籤是您指派給資源的選用性中繼資料。使用標籤以不同方式分類資源，例如依用途、擁有者或環境。

管理複寫集的標籤

1. 開啟 Incident Manager 主控台，然後在左側導覽窗格中選擇設定。
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. 輸入標籤的索引鍵和選用值。
    c. 選擇儲存。
4. 若要刪除標籤，請執行下列動作：
    a. 在要刪除的標籤下，選擇移除。
    b. 選擇儲存。

管理問題清單功能

問題清單功能可協助組織中的回應者在事件開始後不久識別事件的潛在根本原因。Incident Manager 目前提供 AWS CodeDeploy 部署和 AWS CloudFormation 堆疊更新的調查結果。

若要跨帳戶支援問題清單，在啟用此功能之後，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 Incident Manager 建立服務角色，其中包含代表您存取資料所需的許可。

啟用問題清單功能

1. 開啟 Incident Manager 主控台，然後在左側導覽窗格中選擇設定。
2. 在問題清單區域中，選擇建立服務角色。
3. 檢閱要建立之服務角色的相關資訊，然後選擇建立。

停用問題清單功能

若要停止使用問題清單功能，請從每個建立問題清單的帳戶刪除`IncidentManagerIncidentAccessServiceRole`角色。

1. 前往 https://console.aws.amazon.com/iam/ 開啟 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 Incident Manager 中建立和設定聯絡人

AWS Systems Manager Incident Manager 聯絡人是事件的回應者。聯絡人可以有多個管道，而 Incident Manager 可以在事件期間與其互動。您可以定義聯絡人的參與計劃，描述 Incident Manager 如何和何時與聯絡人互動。

主題

- 聯絡管道
- 參與計劃
- 建立聯絡人
- 將聯絡人詳細資訊匯入您的通訊錄

聯絡管道

聯絡管道是 Incident Manager 用來與聯絡人互動的各種方法。

Incident Manager 支援下列聯絡管道：

- 電子郵件
- 簡訊服務 (SMS)
- 語音

聯絡管道啟用

為了保護您的隱私權和安全，Avent Manager 會在您建立聯絡人時傳送裝置啟用碼給您。若要在事件期間讓裝置參與，您必須先啟用裝置。若要這樣做，請在建立聯絡人頁面上輸入裝置啟用碼。

Incident Manager 的某些功能包括將通知傳送至聯絡管道的功能。使用這些功能，即表示您同意此服務將服務中斷或其他事件的相關通知傳送至指定工作流程中包含的聯絡管道。這包括在通話中排程輪換時傳送給聯絡人的通知。通知可以透過電子郵件、簡訊或語音通話傳送，如聯絡詳細資訊中所指定。您可以使用這些功能來確認您是否獲授權新增您提供給 Incident Manager 的聯絡管道。

選擇不接收

您可以隨時取消這些通知，方法是移除行動裝置做為聯絡管道。個別通知收件人也可以隨時取消通知，方法是從其聯絡人中移除裝置。

從聯絡人中移除聯絡管道

1. 導覽至 Incident Manager 主控台，然後從左側導覽中選擇聯絡人。
2. 選取您要移除之聯絡管道的聯絡人，然後選擇編輯。
3. 選擇您要移除的聯絡管道旁的移除。
4. 選擇更新。

聯絡管道停用

若要停用裝置，請回覆 UNSUBSCRIBE。回覆 UNSUBSCRIBE 會阻止 Incident Manager 與您的裝置建立信任。

聯絡管道重新啟用

1. 回覆來自 Incident Manager 的 START 訊息。
2. 導覽至 Incident Manager 主控台，然後從左側導覽中選擇聯絡人。
3. 選取您要移除之聯絡管道的聯絡人，然後選擇編輯。

4. 選擇啟用裝置。
5. 輸入 Incident Manager 傳送至裝置的啟用碼。
6. 選擇 Activate (啟用)。

參與計劃

參與計劃會定義 Incident Manager 何時參與聯絡管道。您可以從互動開始的不同階段多次互動聯絡管道。您可以在升級計劃或回應計劃中使用參與計劃。若要進一步了解升級計劃，請參閱在 Incident Manager 中建立回應者參與的呈報計畫。

建立聯絡人

若要建立聯絡人，請使用下列步驟。

1. 開啟 Incident Manager 主控台，然後從左側導覽中選擇聯絡人。
2. 選擇建立聯絡人。
3. 輸入聯絡人的完整名稱，並提供唯一且可識別身分的別名。
4. 定義聯絡管道。我們建議您擁有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. 輸入聯絡管道的可識別名稱。
   c. 提供聯絡管道詳細資訊，例如電子郵件：arosalez@example.com
5. 若要定義多個聯絡管道，請選擇新增聯絡管道。為每個新增的聯絡管道重複步驟 4。
6. 定義參與計劃。

> **Important**
> 若要與聯絡人互動，您必須定義互動計畫。

   a. 選擇聯絡管道名稱。
   b. 定義從互動開始要等待多少分鐘，直到 Incident Manager 與此聯絡管道互動為止。
   c. 若要新增另一個聯絡管道，請選擇新增參與。
7. 定義您的參與計劃之後，請選擇建立。Incident Manager 會將啟用碼傳送至每個定義的聯絡管道。
8. （選用）若要啟用聯絡管道，請輸入 Incident Manager 傳送至每個已定義聯絡管道的啟用代碼。

9. （選用）若要傳送新的啟用碼，請選擇傳送新的程式碼。
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。若要進一步了解升級計劃，請參閱在 Incident Manager 中建立回應者參與的呈報計畫。您可以將聯絡人新增至回應計劃以進行直接參與。若要進一步了解如何建立回應計劃，請參閱在 Incident Manager 中建立和設定回應計劃。

將聯絡人詳細資訊匯入您的通訊錄

建立事件時，Inventist Manager 可以使用語音或簡訊通知來通知回應者。為了確保回應者看到呼叫或簡訊通知來自 Incident Manager，我們建議所有回應者將 Incident Manager 虛擬卡格式 (.vcf) 檔案下載到行動裝置上的通訊錄。檔案託管在 Amazon CloudFront 中，並可在 AWS 商業分割區中使用。

下載 Incident Manager .vcf 檔案

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

在 Incident Manager 中使用隨叫隨到排程管理回應者輪換

Incident Manager 中的隨需排程會定義當發生需要操作員介入的事件時，會通知誰。隨需排程包含您為排程建立的一或多個輪換。每次輪換最多可包含 30 個聯絡人。

建立隨需排程之後，您可以將其納入升級計畫中做為升級。當發生與該升級計畫相關聯的事件時，Invent Manager 會根據排程通知正在呼叫的操作員（或操作員）。然後，此聯絡人可以確認參與。在您的升級計劃中，您可以在升級的多個階段中指定一或多個通話中排程，以及一或多個個別聯絡人。如需詳細資訊，請參閱在 Incident Manager 中建立回應者參與的呈報計畫。

> **Tip**
>
> 最佳實務是，建議在升級計畫中新增聯絡人和通話中排程做為升級管道。然後，您應該選擇升級計畫做為回應計畫中的參與。此方法為組織中的事件回應提供最完整的涵蓋範圍。

每個隨叫隨到排程最多支援八個輪換。輪換可以重疊或同時執行。這會增加事件發生時通知 回應的運算子數量。您也可以建立連續執行的輪換。這支援「追隨太陽」事件管理等案例，您在世界各地擁有支援相同服務的群組。

使用本節中的主題來協助您建立和管理事件回應操作的通話中排程。

主題

- 在 Incident Manager 中建立待命排程和輪換
- 在 Incident Manager 中管理現有的待命排程

在 Incident Manager 中建立待命排程和輪換

建立隨叫隨到排程，其中包含一或多個輪換聯絡案例，以在輪班期間回應事件。

開始之前

建立隨需排程之前，請確定您先前已建立要新增至排程中輪換的聯絡人。如需詳細資訊，請參閱 在 Incident Manager 中建立和設定聯絡人。

日光節約時間 (DST) 變更的會計

當您建立輪換時，您可以指定全域時區，做為您為此輪換指定的輪班涵蓋時間和日期的基礎。您可以使用網際網路指派號碼授權機構 (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需排程。不過，當每個輪換的回應者地理位置上位於不同的時區時，請記住每個輪換可能受到的任何 DST 變更。

例如， America/Los_Angeles和 Europe/Dublin 觀察不同的 DST 排程。因此，兩個區域之間的時間差可能從 6 到 8 小時不等，取決於一年中的時間。例如，follow-the-sun待命排程在America/Los_Angeles時區有一個輪換，在 有一個輪換Europe/Dublin。在此範例中，由於 DST 變更，排程可以包含一小時輪班間隔或一小時輪班重疊。

為了避免這些情況，我們建議採用下列方法：

1. 使用單一時區進行待命排程中的所有輪換。
2. 當您將回應者指派到該特定時區之外時，計算本機時間。

如果您決定將每個輪換指派給其當地時區，請在任何 DST 之前檢閱排程。然後，視需要調整輪換輪班時間，以確保您在進行任何 DST 變更生效之前，避免通話涵蓋範圍中的任何意外差距或重疊。

建立隨叫隨到排程

1. 開啟 Incident Manager 主控台。
2. 在左側導覽中，選擇待命排程。
3. 選擇建立通話中排程。
4. 針對排程名稱，輸入名稱以協助您識別排程，例如 **MyApp Primary On-call Schedule**。
5. 針對排程別名，輸入此排程的唯一別名 AWS 區域，例如 **my-app-primary-on-call-schedule**。
6. （選用）在標籤區域中，將一或多個標籤索引鍵名稱和值對套用至待命排程。

   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，以識別其執行的期間、其中包含的運算子類型，或其支援的升級計畫。如需標記 Incident Manager 資源的詳細資訊，請參閱Incident Manager 中的標記資源。
7. 繼續將一或多個輪換新增至隨需排程。

在 Incident Manager 中建立待命排程的輪換

待命排程中的輪換會指定輪班生效的時間。它也會指定轉移旋轉的聯絡人。您可以在單一通話排程中包含最多八個輪換。

您可以將您在 Incident Manager 中建立為聯絡人的任何個人新增至輪換。如需有關管理聯絡人的資訊，請參閱 在 Incident Manager 中建立和設定聯絡人。

當您設定輪換時，您可以查看整體排程在頁面右側的預覽行事曆中的外觀。

為隨需排程建立輪換

1. 在建立通話中排程頁面的輪換 1 區段中，針對輪換名稱輸入可識別輪換的名稱，例如 **00:00 - 7:59 Support**或 **Dublin Support Group**。
2. 對於開始日期，輸入此輪換變成作用中的日期，YYYY/MM/DD例如 2023/07/14。
3. 針對時區，選取做為您為此次輪換指定的輪班涵蓋時間和日期基礎的全域時區。

   您可以使用網際網路指派號碼授權機構 (IANA) 定義的任何時區。例如："America/Los_Angeles"、"UTC"、"Asia/Seoul"。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次輪換。不過，您選擇的時區中的任何日光節約時間變更都可能會影響預期的涵蓋時段。如需詳細資訊，請參閱本主題稍早的會計日光節約時間 (DST) 變更。

4. 對於輪換開始時間，輸入此輪換的輪班開始的時間，以 24 小時hh:mm格式，例如 16:00。

   請注意，時區中聯絡人的本機時間差異，與您指定的不同。例如，如果您選擇 America/Los_Angeles作為時區，而選擇 00:00作為輪換開始時間，則愛爾蘭都柏林的 08：00 和印度孟買的 13：30 等於 08：00。

5. 針對輪換結束時間，以 24 小時hh:mm格式輸入輪換結束的時間，例如 23:59。

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

6. （選用）若要將輪換長度設定為 24 小時，請選取 24 小時涵蓋範圍，然後在輪換開始時間欄位中輸入此輪換的開始時間。輪換結束時間值會自動更新。

   例如，如果您希望隨叫隨到的 24 小時涵蓋範圍與上午 11 點的輪班變更，請選擇 24 小時涵蓋範圍，然後輸入 **11:00**作為開始時間。

7. 對於作用中天數，選取此輪換作用中的一週天數。如果您的待命計劃排除週末涵蓋範圍，請選取星期日和星期六以外的所有天數。

8. 繼續將聯絡人新增至輪換。

在 Incident Manager 中的隨需排程中將聯絡人新增至輪換

對於隨需排程中的每個輪換，您可以新增一或多個聯絡人，最多共 30 個。您可以選擇在 Incident Manager 組態中設定的聯絡人。

當您將聯絡人新增至輪換時，該聯絡人可能會收到通知，做為他們待命職責的一部分。通知可以透過電子郵件、簡訊或語音通話傳送，如聯絡詳細資訊中所指定。

如需有關管理聯絡人和聯絡人通知選項的資訊，請參閱在 Incident Manager 中建立和設定聯絡人。

將聯絡人新增至通話中排程中的輪換

1. 在建立通話中排程頁面上，在輪換的聯絡人區段中，選擇新增或移除聯絡人。
2. 在新增或移除聯絡人對話方塊中，選取要包含在輪換中的聯絡人別名。

   您選取聯絡人的順序是它們在輪換排程中首先列出的順序。您可以在新增聯絡人之後變更順序。
3. 選擇確認。
4. 若要依順序變更聯絡人的位置，請選取該使用者的選項按鈕，然後使用向上
   ( )
   和向下
   ( )
   按鈕來更新聯絡人順序。
5. 繼續為輪換指定個別輪班循環和長度。

在 Incident Manager 中指定輪班週期和長度，並將標籤新增至輪換

輪換循環會指定輪換中的聯絡人輪換和輪換通話中的頻率。週期長度可以以天數、週數或月數來指定。

指定輪班週期和長度，並將標籤新增至輪換

1. 在建立通話中排程頁面上，於輪換的週期設定區段中，執行下列動作：
   - 針對輪班週期類型，從 、 `Weekly`和 選擇，指定每個待命輪班是否持續數天`Daily`、數週或數月`Monthly`。
   - 針對輪班長度，輸入輪班持續的天數、週數或月數。

     例如，如果您選擇`Daily`並輸入 **`1`**，每個聯絡人的待命輪班會持續一天。如果您選擇`Weekly`並輸入 **`3`**，每個聯絡人的通話中輪班會持續三週。
2. （選用）在標籤區域中，將一或多個標籤索引鍵名稱和值對套用至輪換。

   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，以識別指派給它的聯絡人位置、其要提供的涵蓋範圍類型，或是其將支援的升級計畫。如需標記 Incident Manager 資源的詳細資訊，請參閱Incident Manager 中的標記資源。
3. （建議）使用行事曆預覽，確保待命排程的涵蓋範圍沒有非預期的差距。
4. 選擇 Create (建立)。

您現在可以將隨需排程新增為升級計劃中的升級管道。如需相關資訊，請參閱 建立升級計畫。

在 Incident Manager 中管理現有的待命排程

使用本節中的內容，協助您處理已建立的隨需排程。

主題

- 檢視待命排程詳細資訊
- 編輯待命排程
- 複製待命排程
- 建立通話中排程輪換的覆寫
- 刪除待命排程

檢視待命排程詳細資訊

您可以在檢視通話中排程詳細資訊頁面上存取通話中排程的at-a-glance摘要。此頁面也包含有關目前通話中和接下來通話中對象的資訊。此頁面包含行事曆檢視，顯示哪些聯絡人在任何特定時間正在通話。

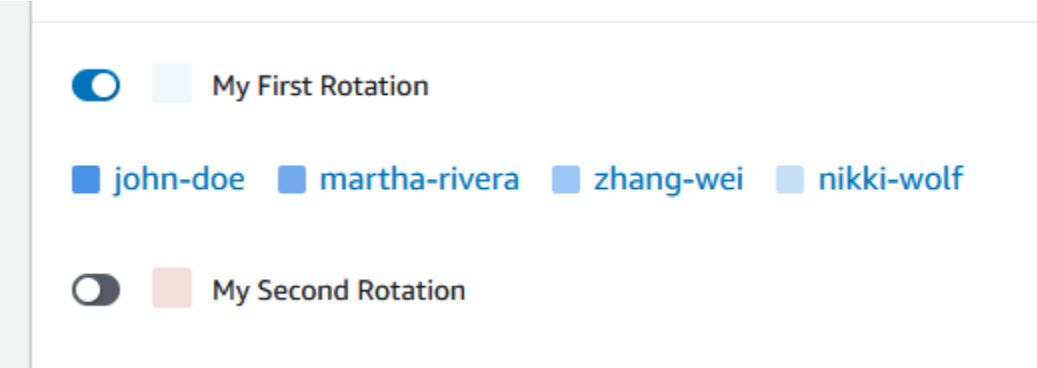
檢視待命排程詳細資訊

1. 開啟 Incident Manager 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列中，執行下列其中一項：
   - 若要開啟行事曆的摘要檢視，請選擇排程別名。

     -或-

     選取資料列的選項按鈕，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

     在行事曆檢視中，選擇排程中特定日期的聯絡人名稱，以查看指派輪班的詳細資訊或建立覆寫。
   - 若要開啟或關閉行事曆中特定輪換的顯示，請選擇輪換名稱旁的切換。



編輯待命排程

您可以更新待命排程及其輪換的組態，但下列詳細資訊除外：

- 排程別名
- 輪換名稱
- 輪換開始日期

若要使用現有行事曆做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。

編輯待命排程

1. 開啟 Incident Manager 主控台。
2. 在左側導覽中，選擇待命排程。
3. 執行以下任意一項：
   - 選取列中的選項按鈕，即可編輯待命排程，然後選擇編輯。
   - 選擇待命排程的排程別名，以開啟檢視待命排程詳細資訊頁面，然後選擇編輯。
4. 對待命排程及其輪換進行任何必要的修改。您可以變更輪換組態選項，例如開始和結束時間、聯絡人和循環。您可以視需要從排程新增或移除輪換。行事曆預覽會反映您在進行變更時所做的變更。

   如需使用頁面上選項的相關資訊，請參閱在 Incident Manager 中建立待命排程和輪換。
5. 選擇更新。

> **Important**
>
> 如果您編輯包含覆寫的排程，您的變更可能會影響覆寫。為了確保您的覆寫保持如預期設定，我們建議您在更新排程後仔細檢閱您的輪班覆寫。

複製待命排程

若要使用現有隨叫隨到排程的組態作為新排程的起點，您可以建立行事曆的副本並視需要修改。

複製隨傳隨到排程

1. 開啟 Incident Manager 主控台。
2. 在左側導覽中，選擇待命排程。
3. 選取 列中的選項按鈕，即可複製待命排程。
4. 請選擇 Copy (複製)。
5. 對行事曆及其輪換進行任何您需要的修改。您可以視需要變更、新增或移除輪換。

   > **Note**
   >
   > 複製現有的排程時，您必須為每個輪換指定新的開始日期。複製的排程不支援過去開始日期的輪換。

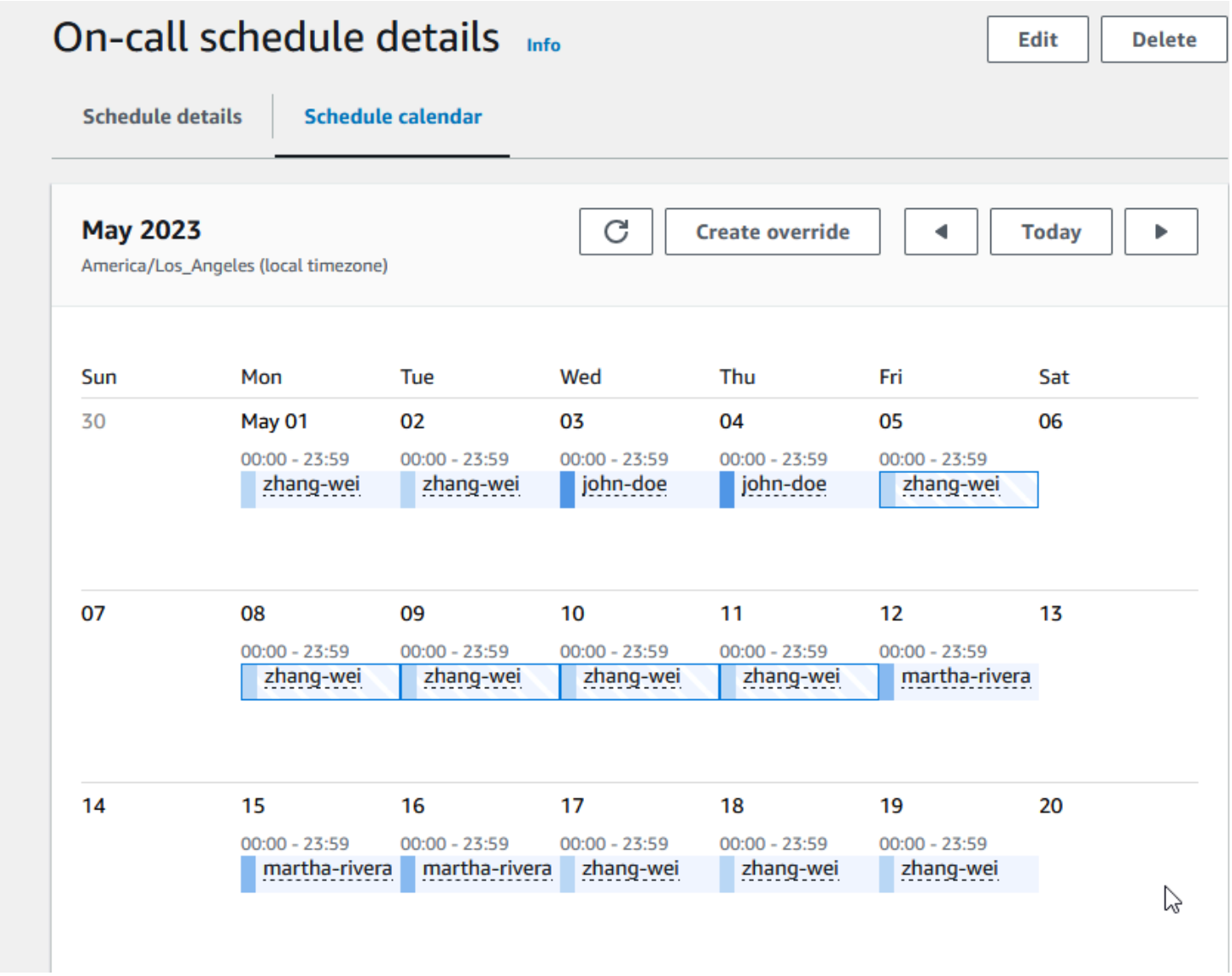
   如需使用頁面上選項的相關資訊，請參閱在 Incident Manager 中建立待命排程和輪換。
6. 選擇建立複本。

建立通話中排程輪換的覆寫

如果您需要對現有的輪換排程進行一次性變更，您可以建立覆寫。覆寫可讓您將聯絡人的全部或部分輪班取代為另一個聯絡人。您也可以建立跨多個輪班的覆寫。

您只能將聯絡人指派給已指派給輪換的覆寫。

在行事曆預覽中，覆寫的輪班會以條紋背景顯示，而非實心背景。下圖顯示名為 Zhang Wei 的聯絡人正在覆寫中通話。覆寫包含 John Doe 和 Martha Rivera 的部分輪班，從 5 月 5 日開始到 5 月 11 日結束。



建立待命排程的覆寫

1. 開啟 Incident Manager 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列中，執行下列其中一項：
   - 選擇排程別名，然後選擇排程行事曆索引標籤。
   - 選擇 檢視行事曆

     。
4. 執行以下任意一項：
   - 選擇建立覆寫。
   - 在行事曆預覽中選擇聯絡人的名稱，然後選擇覆寫輪班。

5. 在建立輪班覆寫對話方塊中，執行下列動作：

> **Note**
>
> 覆寫長度必須至少為 30 分鐘。您只能為未來六個月內發生的輪班指定覆寫。

   a. 針對選取輪換，選取輪換的名稱以建立覆寫。
   b. 針對開始日期，選取或輸入覆寫開始的日期。
   c. 針對開始時間，輸入覆寫開始的時間hh:mm，格式為 。
   d. 針對結束日期，選取或輸入覆寫結束的日期。
   e. 針對結束時間，以 hh:mm 格式輸入覆寫結束的時間。
   f. 針對選取覆寫聯絡人，選取覆寫期間正在通話的輪換聯絡人名稱。
6. 選擇建立覆寫。

建立覆寫之後，您可以依其分割背景來識別它。當您選擇覆寫輪班的聯絡人名稱時，資訊方塊會將其識別為覆寫輪班。您可以選擇刪除覆寫來移除它，並還原原始的通話中指派。

刪除待命排程

當您不再需要特定的待命排程時，您可以從 Incident Manager 刪除它。

如果任何升級計劃或回應計劃目前使用隨需排程作為升級管道，您應該在刪除排程之前將其從這些計劃中移除。

刪除待命排程

1. 開啟 Incident Manager 主控台。
2. 在左側導覽中，選擇待命排程。
3. 選取列中的選項按鈕，即可刪除待命排程。
4. 選擇 刪除 。
5. 在刪除通話中排程？對話方塊中，在文字方塊**confirm**中輸入 。
6. 選擇 Delete (刪除)。

在 Incident Manager 中建立回應者參與的呈報計畫

AWS Systems Manager Incident Manager 透過您定義的聯絡人或通話中排程提供呈報路徑，統稱為呈報管道。您可以同時將多個呈報管道提取到事件中。如果呈報管道中指定的聯絡人沒有回應，Inventist Manager 會呈報到下一組聯絡人。您也可以選擇計畫在使用者確認參與後是否停止呈報。您可以將升級計畫新增至回應計畫，以便升級在事件開始時自動開始。您也可以將升級計畫新增至作用中的事件。

主題

- 階段
- 建立升級計畫

階段

呈報計劃使用階段，其中每個階段會持續定義的分鐘數。每個階段都有以下資訊：

- 持續時間 – 計劃等待到開始下一個階段的時間。升級計劃的第一個階段會在互動開始時開始。
- 呈報管道 – 呈報管道是單一聯絡人或通話中排程，由多個聯絡人組成，這些聯絡人會依定義的排程輪換責任。呈報計畫使用其定義的參與計畫來吸引每個管道。您可以設定每個升級管道，在升級計畫繼續進入下一個階段之前停止升級計畫的進度。每個階段可以有多個升級頻道。

  如需設定個別聯絡人的資訊，請參閱 在 Incident Manager 中建立和設定聯絡人。如需建立隨叫隨到排程的詳細資訊，請參閱在 Incident Manager 中使用隨叫隨到排程管理回應者輪換。

建立升級計畫

1. 開啟 Incident Manager 主控台，然後從左側導覽中選擇升級計劃。
2. 選擇建立升級計畫。
3. 針對名稱，輸入升級計劃的唯一名稱，例如 **`My Escalation Plan`**。
4. 針對別名，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 Incident Manager 等待到繼續進入下一個階段的分鐘數。
6. 對於升級管道，選擇一或多個聯絡人或通話中排程，在此階段進行互動。
7. （選用）若要讓聯絡人在確認參與後停止升級計畫，請選取確認停止計畫進度。
8. 若要將另一個頻道新增至此階段，請選擇新增升級頻道。
9. 若要將另一個階段新增至升級計劃，請選擇新增階段。

10. 重複步驟 5 到 9，直到您完成新增您要用於此呈報計畫的呈報管道和階段為止。
11. （選用）在標籤區域中，將一或多個標籤索引鍵名稱和值對套用至升級計劃。

    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，您可以標記呈報計畫，以識別要使用的事故類型、其包含的呈報管道類型，或其支援的呈報計畫。如需標記 Incident Manager 資源的詳細資訊，請參閱Incident Manager 中的標記資源。
12. 選擇建立升級計畫。

在 Incident Manager 中為回應者建立和整合聊天頻道

Incident Manager 是 中的工具 AWS Systems Manager，可讓事件回應者在事件期間直接透過聊天管道進行通訊。聊天頻道是您在聊天應用程式中在 Amazon Q 開發人員中設定的聊天室。然後，您將此頻道連接到 Incident Manager 中的回應計劃。

在事件期間，回應者會使用聊天頻道來彼此溝通事件。Incident Manager 也會直接將有關事件的任何更新和通知推送至聊天頻道。它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。

聊天應用程式中的 Amazon Q Developer 和 Incident Manager 支援下列應用程式中的聊天管道：

- Slack
- Microsoft Teams
- Amazon Chime

設定聊天頻道以用於事件的程序包含三種不同 Amazon Web Services 服務中的任務。

任務

- 任務 1：建立或更新聊天頻道的 Amazon SNS 主題
- 任務 2：在聊天應用程式中建立 Amazon Q Developer 中的聊天頻道
- 任務 3：將聊天頻道新增至 Incident Manager 中的回應計劃
- 透過聊天管道互動

任務 1：建立或更新聊天頻道的 Amazon SNS 主題

Amazon SNS 是一種受管服務，提供從發佈者到訂閱者 （ 也稱為生產者和消費者) 的訊息傳遞。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。Incident Manager 會使用與回應計劃相關聯的一或多個主題，將事件的相關通知傳送給事件回應者。

在回應計劃中，您可以將一或多個 Amazon SNS 主題納入事件通知。最佳實務是，您應該 AWS 區域在已新增至複寫集的每個 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 Incident Manager 搭配使用。設定完成後，您就可以建立聊天頻道。

為您的聊天頻道建立或更新 Amazon SNS 主題

1. 請遵循 Amazon Simple Notification Service 開發人員指南中建立 Amazon SNS 主題中的步驟。

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

2. 選取您建立的主題，並以 等格式記下或複製主題的 Amazon Resource Name (ARN)`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`。
3. 選擇編輯，然後展開存取政策區段，以設定預設值以外的其他存取許可。
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 Resource Name (ARN)，格式為 `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`。
- *account-id* 是您正在使用之 AWS 帳戶 的 ID，例如 `111122223333`。

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

任務 2：在聊天應用程式中建立 Amazon Q Developer 中的聊天頻道

您可以在 Slack、 Microsoft Teams或 Amazon Chime 中建立聊天頻道。每個回應計劃只需要一個聊天頻道。

針對您的聊天頻道，我們建議您遵循最低權限的主體（不要提供使用者比完成其任務所需的更多許可）。您也應該在聊天應用程式聊天頻道中定期檢閱 Amazon Q 開發人員的成員資格。檢閱有助於檢查只有適當的回應者和其他利益相關者可以存取您的聊天頻道。

在聊天應用程式中在 Amazon Q Developer 中建立的Slack頻道和Microsoft Teams頻道中，事件回應者可以直接從 Slack或Microsoft Teams應用程式執行多個 Incident Manager CLI 命令。如需詳細資訊，請參閱透過聊天管道互動。

> **Important**
>
> 您新增至聊天頻道的使用者，必須與呈報或回應計劃中列出的聯絡人相同。您也可以將其他使用者新增至聊天頻道，例如利益相關者和事件觀察者。

如需聊天應用程式中 Amazon Q 開發人員的一般資訊，請參閱聊天應用程式中 Amazon Q 開發人員的什麼是聊天應用程式中的 Amazon Q 開發人員管理員指南。

從下列應用程式中選擇，在 中建立您的頻道：

Slack

此程序中的步驟提供建議的許可設定，以允許所有管道使用者搭配 Incident Manager 使用聊天命令。使用支援的聊天命令，您的事件回應者可以直接從Slack聊天管道更新並與事件互動。如需相關資訊，請參閱 透過聊天管道互動。

在 中建立聊天頻道 Slack

- 請遵循聊天應用程式管理員指南中的 Amazon Q 開發人員中的教學課程步驟：開始使用 Slack，並在您的組態中包含下列項目。
  - 在步驟 10 中，針對角色設定，選擇頻道角色。
  - 在步驟 10d 中，針對政策範本，選取 Incident Manager 許可。
  - 在步驟 11 中，針對頻道護欄政策，針對政策名稱，選擇 AWSIncidentManagerResolverAccess。
  - 在步驟 12 的 SNS 主題區段中，執行下列動作：
    - 針對區域 1，選取複寫集中包含 AWS 區域 的 。
    - 針對主題 1，選取您在該區域中建立的 SNS 主題，以用來傳送事件通知至聊天頻道。
    - 針對複寫集中的每個額外區域，選擇新增另一個區域，並新增其他區域和 SNS 主題。

Microsoft Teams

此程序中的步驟提供建議的許可設定，以允許所有管道使用者搭配 Incident Manager 使用聊天命令。您的事件回應者可以使用支援的聊天命令，直接從Microsoft Teams聊天管道更新並與事件互動。如需相關資訊，請參閱 透過聊天管道互動。

在 中建立聊天頻道 Microsoft Teams

- 遵循教學課程中的步驟：在聊天應用程式管理員指南Microsoft Teams中的 Amazon Q 開發人員中開始使用 ，並在您的組態中包含下列項目：
  - 在步驟 10 中，針對角色設定，選擇頻道角色。
  - 在步驟 10d 中，針對政策範本選取 Incident Manager 許可。
  - 在步驟 11 中，針對頻道護欄政策，針對政策名稱，選擇 AWSIncidentManagerResolverAccess。
  - 在步驟 12 的 SNS 主題區段中，執行下列動作：
    - 針對區域 1，選取複寫集中包含 AWS 區域 的 。

- 針對主題 1，選取您在該區域中建立的 SNS 主題，以用來傳送事件通知至聊天頻道。
- 針對複寫集中的每個額外區域，選擇新增另一個區域，並新增其他區域和 SNS 主題。

Amazon Chime

在 Amazon Chime 中建立聊天頻道

- 請遵循聊天應用程式管理員指南中的 Amazon Q 開發人員中的教學課程：開始使用 Amazon Chime，並在您的組態中包含下列項目：
  - 在步驟 11 中，針對政策範本選取 Incident Manager 許可。
  - 在步驟 12 的 SNS 主題區段中，選取將傳送通知至 Amazon Chime Webhook 的 SNS 主題：
    - 針對區域 1，選取複寫集中包含 AWS 區域 的 。
    - 針對主題 1，選取您在該區域中建立的 SNS 主題，以用來將事件通知傳送至聊天頻道。
    - 針對複寫集中的每個額外區域，選擇新增另一個區域，並新增其他區域和 SNS 主題。

> **Note**
>
> Amazon Chime 不支援在 Slack和 聊天頻道中使用哪些事件回應程式的Microsoft Teams聊天命令。

任務 3：將聊天頻道新增至 Incident Manager 中的回應計劃

當您建立或更新回應計劃時，您可以新增聊天頻道，讓回應者透過 進行通訊和接收更新。

遵循 中的步驟時建立回應計劃，針對 區段（選用）指定事件回應聊天頻道，選取您要用於與此回應計劃相關事件的頻道。

透過聊天管道互動

對於 Slack和 中的頻道Microsoft Teams，Invent Manager 可讓回應者使用下列`ssm-incidents`命令，直接從聊天頻道與事件互動：

- start-incident
- 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* 取代為命令要包含的任何選項。

```
@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
```

將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件

您可以使用 中的工具 AWS Systems Manager Automation 的 Runbook AWS Systems Manager，來自動化 AWS 雲端 環境中常見的應用程式和基礎設施任務。

每個 Runbook 都會定義 Runbook 工作流程，由 Systems Manager 在您的受管節點或其他 AWS 資源類型上執行的動作組成。您可以使用 Runbook 自動化資源 AWS 的維護、部署和修復。

在 Incident Manager 中， Runbook 會驅動事件回應和緩解，而您會指定 Runbook 做為回應計劃的一部分。

在您的回應計劃中，您可以從數十個預先設定的執行手冊中，為一般自動化任務進行選擇，也可以建立自訂執行手冊。當您在回應計劃定義中指定 Runbook 時，系統可在事件開始時自動啟動 Runbook。

> **Important**
>
> 跨區域容錯移轉建立的事件不會叫用回應計劃中指定的 Runbook。

如需 Systems Manager 自動化、執行手冊和搭配 Incident Manager 使用執行手冊的詳細資訊，請參閱下列主題：

- 若要將 Runbook 新增至回應計劃，請參閱 在 Incident Manager 中建立和設定回應計劃。
- 若要進一步了解 Runbook，請參閱 AWS Systems Manager 使用者指南中的AWS Systems Manager 自動化和 AWS Systems Manager Automation Runbook 參考。
- 如需使用 Runbook 的成本資訊，請參閱 Systems Manager 定價。
- 如需在 Amazon CloudWatch 警示或 Amazon EventBridge 事件建立事件時自動叫用 Runbook 的資訊，請參閱教學課程：搭配 Incident Manager 使用 Systems Manager Automation Runbook。

主題

- 啟動和執行 Runbook 工作流程所需的 IAM 許可
- 使用 Runbook 參數
- 定義 Runbook
- Incident Manager Runbook 範本

啟動和執行 Runbook 工作流程所需的 IAM 許可

Incident Manager 需要許可，才能在事件回應中執行 Runbook。若要提供這些許可，您可以使用 AWS Identity and Access Management (IAM) 角色、 Runbook 服務角色和 Automation `AssumeRole`。

Runbook 服務角色是必要的服務角色。此角色為 Incident Manager 提供存取和啟動 Runbook 工作流程所需的許可。

自動化AssumeRole提供執行 Runbook 中指定的個別命令所需的許可。

> **Note**
>
> 如果未指定AssumeRole任何 ，Systems Manager Automation 會嘗試針對個別命令使用 Runbook 服務角色。如果您未指定 AssumeRole，則必須將必要的許可新增至 Runbook 服務角色。如果沒有，則 Runbook 無法執行這些命令。
> 不過，根據安全最佳實務，我們建議您使用不同的 AssumeRole。使用單獨的 AssumeRole，您可以限制您必須新增至每個角色的必要許可。

如需自動化 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 （ 擔任角色 ） 存取。

您可以在 IAM 主控台中自行手動建立任一類型的角色。- 您也可以讓 Incident Manager 在建立或更新回應計劃時為您建立任一類型的角色。

Runbook 服務角色許可

Runbook 服務角色許可是透過類似下列的政策提供。

第一個陳述式可讓 Incident Manager 啟動 Systems Manager StartAutomationExecution操作。然後，此操作會在由三種 Amazon Resource Name (ARN) 格式表示的資源上執行。

第二個陳述式允許 Runbook 服務角色在受影響的帳戶中執行 Runbook 時，在另一個帳戶中擔任角色。如需詳細資訊，請參閱AWS Systems Manager 《 使用者指南》中的在多個 AWS 區域 和 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"
        }
      }
    }
  ]
}
```

Automation AssumeRole 許可

當您建立或更新回應計劃時，您可以從數個 AWS 受管政策中選擇連接到 Incident Manager 建立的 AssumeRole。這些政策提供許可，以執行在 Incident Manager Runbook 案例中使用的許多常見操作。您可以選擇一或多個這些受管政策來提供AssumeRole政策的許可。下表說明從 AssumeRole Incident Manager 主控台建立 時可以選擇的政策。

AWS 受管政策名稱	政策描述
AmazonSSMAutomationRole	准許 Systems Manager Automation 服務執行 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	准許使用者啟動、檢視和更新事件。您也可以使用它們在事件儀表板中建立客戶時間軸事件和相關項目。

您可以使用這些受管政策，授予許多常見事件回應案例的許可。不過，您需要的特定任務所需的許可可能會有所不同。在這些情況下，您需要為 提供額外的政策許可AssumeRole。如需詳細資訊，請參閱 AWS Systems Manager Automation Runbook 參考。

使用 Runbook 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。

關於相關聯的資源

Incident Manager 可以將 CloudWatch 警示、EventBridge 事件和手動建立的事件中指定的 AWS 資源 ARNs 填入 Runbook 參數值。本節說明在填入此參數時，Invent Manager 可以擷取 ARNs的不同類型的資源。

CloudWatch 警示

從 CloudWatch 警示動作建立事件時，Invent Manager 會自動從相關聯的指標擷取下列類型的資源。然後，它會將下列涉及的資源填入所選的參數：

AWS 服務	資源類型
Amazon DynamoDB	全域次要索引
	串流
	資料表

AWS 服務	資源類型
Amazon EC2	映像 執行個體
AWS Lambda	函數別名 函數版本 函數
Amazon Relational Database Service (Amazon RDS)	叢集 資料庫執行個體
Amazon Simple Storage Service (Amazon S3)	儲存貯體

EventBridge 規則

當系統從 EventBridge 事件建立事件時，Invent Manager 會在事件中將所選參數填入 `Resources` 屬性。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 StartIncident API 動作來建立事件時，Incident Manager 會使用 API 呼叫中的資訊填入選取的參數。具體而言，它會使用在 參數中傳遞的類型項目`INVOLVED_RESOURCE`來填入`relatedItems`參數。

> **Note**
>
> 該`INVOLVED_RESOURCES`值只能指派給類型 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 Runbook

建立 Runbook 時，您可以遵循此處提供的步驟，也可以遵循 Systems Manager 使用者指南中的使用 Runbook 一節所提供的更詳細指南。 如果您要建立多帳戶、多區域 Runbook，請參閱 Systems Manager 使用者指南中的在多個 AWS 區域 和 帳戶中執行自動化。

定義 Runbook

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 Systems Manager 主控台。
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 Runbook 的描述。
6. 為要擔任的自動化文件提供 IAM 角色。這可讓 Runbook 自動執行命令。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。
7. （選用）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。動態參數會使用 Runbook 啟動之事件中的值。靜態參數會使用您提供的值。
8. （選用）新增目標類型。
9. (選用) 新增標籤。
10. 填寫執行手冊執行時將採取的步驟。每個步驟都需要：
    - 名稱。
    - 步驟用途的描述。
    - 步驟期間要執行的動作。Runbook 使用暫停動作類型來描述手動步驟。
    - （選用）命令屬性。
11. 新增所有必要的 Runbook 步驟後，選擇建立自動化。

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

共用 Runbook

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 Systems Manager 主控台。
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訊。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，請選擇私有、輸入 AWS 帳戶 ID、選擇新增許可，然後選擇儲存。

Incident Manager Runbook 範本

Incident Manager 提供下列 Runbook 範本，以協助您的團隊開始在 Systems Manager 自動化中編寫 Runbook。您可以照原樣使用此範本，或對其進行編輯，以包含應用程式和資源的特定詳細資訊。

尋找 Incident Manager Runbook 範本

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 Systems Manager 主控台。
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 Incident Manager Runbook。

> **Tip**
>
> 輸入 **AWSIncidents-**做為任意文字，而不是使用文件名稱字首篩選條件選項。

使用範本

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 Systems Manager 主控台。
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

AWSIncidents-CriticalIncidentRunbookTemplate 是一個範本，可在手動步驟中提供 Incident Manager 事件生命週期。這些步驟非常通用，可用於大多數應用程式，但詳細程度足以讓回應者開始使用事件解決。

在 Incident Manager 中建立和設定回應計劃

回應計劃可讓您規劃如何回應影響使用者的事件。回應計劃可做為範本，其中包含要與誰互動、事件預期嚴重性、要啟動的自動 Runbook 以及要監控的指標等相關資訊。

最佳實務

當您事先規劃事件時，可以減少對團隊事件的影響。當您設計回應計畫時，團隊應考慮下列最佳實務。

- 簡化參與 – 識別最適合事件的團隊。如果您參與的分發清單太寬，或者您參與錯誤的團隊，可能會導致在事件期間混淆和浪費回應者時間。
- 可靠的呈報 – 對於您在回應計畫中的參與，我們建議您選擇參與計畫，而不是聯絡或通話排程。參與計畫應指定個別聯絡人或通話排程（包含多個輪換聯絡人），以便在事件期間進行互動。由於參與計畫中指定的回應者有時可能無法連線，因此您應該在回應計畫中設定備份回應者，以涵蓋這些案例。使用備份聯絡人時，如果主要和次要聯絡人無法使用，或涵蓋範圍有其他未規劃的差距，則 Incident Manager 仍會通知聯絡人有關事件。
- 執行手冊 – 使用執行手冊提供可重複、可理解的步驟，以減少回應者在事件期間遇到的壓力。
- 協同合作 – 使用聊天頻道來簡化事件期間的通訊。聊天頻道可協助回應者隨時掌握資訊。他們也可以透過這些管道與其他回應者共用資訊。

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。

建立回應計劃

1. 開啟 Incident Manager 主控台，然後在導覽窗格中選擇回應計劃。
2. 選擇建立回應計畫。
3. 在名稱中，輸入唯一且可識別的回應計劃名稱，用於回應計劃的 Amazon Resource Name (ARN)。
4. （選用）對於顯示名稱，輸入更人類可讀的名稱，以協助在建立事件時識別回應計畫。
5. 繼續指定事件記錄的預設值。

指定事件預設值

為了協助您更有效地管理事件，您可以指定預設值。Incident Manager 會將這些值套用至與回應計劃相關聯的所有事件。

指定事件預設值

1. 在標題中，輸入此事件的標題，以協助您在 Incident Manager 首頁上識別它。
2. 針對影響，請選擇影響層級，以指出從此回應計畫建立之事件的潛在範圍，例如嚴重或低。如需 Incident Manager 中影響評分的資訊，請參閱 分類。
3. （選用）針對摘要，輸入從此回應計畫建立的事件類型簡短摘要。
4. （選用）針對 Dedupe 字串，輸入 dedupe 字串。Incident Manager 使用此字串來防止相同的根本原因在同一個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詞彙或片語。如果您指定重複資料刪除字串，則 Incident Manager 會在建立事件時，在 `dedupeString` 欄位中搜尋包含相同字串的開啟事件。如果偵測到重複，Incident Manager 會將較新的事件刪除重複到現有的事件中。

   > **Note**
   >
   > 根據預設，Incident Manager 會自動刪除由相同 Amazon CloudWatch 警示或 Amazon EventBridge 事件建立的多個事件。您不需要輸入自己的重複資料刪除字串，以防止這些資源類型的重複。

5. （選用）在事件標籤下，新增標籤索引鍵和值，以指派給從此回應計畫建立的事件。

   您必須擁有事件記錄資源的`TagResource`許可，才能在回應計畫中設定事件標籤。
6. 繼續為解析程式指定選用的聊天頻道，以便彼此溝通事件。

（選用）指定事件回應聊天頻道

當您在回應計畫中包含聊天頻道時，回應者會透過頻道接收事件更新。他們可以使用聊天命令，直接從聊天頻道與事件互動。

在聊天應用程式中使用 Amazon Q Developer，您可以為 Slack、 Microsoft Teams或 建立頻道，讓 Amazon Chime 用於您的回應計劃。如需有關在聊天應用程式中在 Amazon Q Developer 中建立聊天頻道的資訊，請參閱聊天應用程式管理員指南中的 Amazon Q Developer。

> **Important**
>
> Incident Manager 必須具有發佈至聊天頻道 Amazon Simple Notification Service (Amazon SNS) 主題的許可。如果沒有發佈至該 SNS 主題的許可，則無法將其新增至回應計劃。Incident Manager 會將測試通知發佈至 SNS 主題，以驗證許可。

如需聊天頻道的詳細資訊，請參閱 在 Incident Manager 中為回應者建立和整合聊天頻道。

指定事件回應聊天頻道

1. 在聊天頻道中，選取聊天應用程式聊天頻道中的 Amazon Q Developer，回應者可以在事件期間進行通訊。

   > **Tip**
   >
   > 若要在聊天應用程式中的 Amazon Q Developer 中建立新的聊天頻道，請選擇設定新的聊天機器人用戶端。

2. 針對聊天頻道 SNS 主題，選擇要在事件期間發佈的其他 SNS 主題。在多個 中新增 SNS 主題 AWS 區域 會增加備援，以防發生事件時區域故障。
3. 繼續選擇在事件期間要參與的聯絡人、通話中排程和呈報計畫。

（選用）選取要參與事件回應的資源

務必在事件發生時識別最適合的回應者。最佳實務是建議您執行下列動作：

1. 在升級計畫中新增聯絡人和通話中排程作為升級管道。

   > **Note**
   >
   > 目前不支援將另一個帳戶共用的聯絡人新增至回應計劃。

2. 選擇呈報計畫作為回應計畫中的參與。

如需聯絡和呈報計劃的詳細資訊，請參閱 在 Incident Manager 中建立和設定聯絡人和 在 Incident Manager 中建立回應者參與的呈報計畫。

選取要參與事件回應的資源

1. 針對業務開發，選擇任意數量的呈報計畫、待命排程和個別聯絡人。
2. 繼續選擇性地指定 Runbook 做為事件緩解措施的一部分執行。

（選用）指定 Runbook 以緩解事件

您可以使用 AWS Systems Manager Automation 中的 Runbook，在 AWS 雲端 環境中 AWS Systems Manager自動化常見的應用程式和基礎設施任務。

每個 Runbook 都會定義 Runbook 工作流程。Runbook 工作流程包含 Systems Manager 在受管節點或其他 AWS 資源類型上執行的動作。在 Incident Manager 中，執行手冊會驅動事件回應和緩解。

如需在回應計劃中使用 Runbook 的詳細資訊，請參閱將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件。

若要指定事件緩解的 Runbook：

1. 針對 Runbook，執行下列其中一項：

   - 從範本中選擇複製 Runbook，以複製預設的 Incident Manager Runbook。針對 Runbook 名稱，輸入新 Runbook 的描述性名稱。
   - 選擇選取現有的 Runbook。選取要使用的擁有者、執行手冊和版本。

   > **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 將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件。

2. 在參數區域中，提供您所選 Runbook 請求的任何參數。

   可用的參數是由 Runbook 指定的參數。一個 Runbook 可能需要與另一個不同的參數。有些參數可能是必要的，有些則是選用的。

   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 IDs清單。您也可以讓 Incident Manager 提供事件動態產生的參數值。

3. （選用）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許可。

> **Note**
>
> 如果未指定AssumeRole任何 ，則 Incident Manager 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 AssumeRole 的 Amazon Resource Name (ARN)`arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`*。例如 **`arn:aws:iam::123456789012:role/MyAssumeRole`**。
- 使用現有的服務角色 – 從您帳戶中的現有角色清單中選擇具有所需許可的角色。
- 建立新的服務角色 – 從 AWS 受管政策中選擇以連接至 AssumeRole。選取此選項後，針對AWS 受管政策，從清單中選擇一或多個政策。

  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 Runbook 搭配使用。這是因為政策的資源區段不支援其他 Runbook。

4. 針對 Runbook 服務角色，指定要用來提供存取和啟動 Runbook 本身工作流程所需的許可的 IAM 角色。

   角色至少必須允許特定 Runbook 的 `ssm:StartAutomationExecution`動作。若要讓 Runbook 跨帳戶運作，該角色也必須允許您在 期間建立之`AWS-SystemsManager-AutomationExecutionRole`角色的 `sts:AssumeRole`動作在 Incident Manager 中管理跨 AWS 帳戶 和 區域的事件。

   請選擇下列項目：

   - 建立新的服務角色 – Incident Manager 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許可。

     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。建議您使用建議的名稱，或將 Runbook 的名稱保留在名稱中。這是因為新的 AssumeRole 與您選取的特定 Runbook 相關聯，且可能不會包含其他 Runbook 所需的許可。

- 使用現有的服務角色 – 您或 Incident Manager 先前建立的 IAM 角色會授予所需的許可。

  針對角色名稱，選取要使用之現有角色的名稱。

5. 展開其他選項，然後選擇下列其中一項，以指定執行手冊工作流程應執行 AWS 帳戶 的位置。

   - 回應計劃擁有者的帳戶 – 在 AWS 帳戶 建立它的 中啟動 Runbook 工作流程。
   - 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 Incident Manager，且 Runbook 需要存取受影響帳戶中的資源以修復它們時，請選擇受影響的帳戶。

6. 繼續選擇性將 PagerDuty 服務整合到回應計劃中。

（選用）將 PagerDuty 服務整合至回應計劃

將 PagerDuty 服務整合到回應計劃中

當您將 Incident Manager 與 PagerDuty 整合時，PagerDuty 會在 Incident Manager 建立事件時建立對應的事件。PagerDuty 中的事件會使用您在其中定義的分頁工作流程和升級政策，以及 Incident Manager 中的政策。PagerDuty 會將 Incident Manager 的時間軸事件附加為事件的備註。

1. 展開第三方整合，然後選擇啟用 PagerDuty 整合核取方塊。
2. 針對選取秘密，選取您存放登入資料以存取 PagerDuty 帳戶的秘密 AWS Secrets Manager 。

   如需將 PagerDuty 登入資料儲存在 Secrets Manager 秘密中的資訊，請參閱 將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中。
3. 對於 PagerDuty 服務，請從您要建立 PagerDuty 事件的 PagerDuty 帳戶選取服務。
4. 繼續新增選用標籤並建立回應計畫。

新增標籤並建立回應計劃

新增標籤並建立回應計劃

1. （選用）在標籤區域中，將一或多個標籤索引鍵名稱/值對套用至回應計劃。

   標籤是您指派給資源的選用性中繼資料。使用標籤，您可以用不同的方式分類資源，例如依用途、擁有者或環境。例如，您可能想要標記回應計畫，以識別其要緩解的事件類型、其包含的呈

報管道類型，或將與其相關聯的呈報計畫。如需標記 Incident Manager 資源的詳細資訊，請參閱 Incident Manager 中的標記資源。

2. 選擇建立回應計畫。

在 Incident Manager 中將來自其他服務的事件的潛在原因識別為「尋找」

在 Incident Manager 中，問題清單是與事件發生前後發生的 AWS CodeDeploy 部署或 AWS CloudFormation 堆疊更新有關的資訊，而這些部署或堆疊更新可能涉及與事件相關的一或多個資源。每個調查結果都可以檢查為事件的潛在原因。有關這些潛在原因的資訊會新增至事件的事件詳細資訊頁面。透過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。這可減少評估潛在原因所需的時間，這可以減少從事件復原的平均時間 (MTTR)。

目前，Invent Manager 支援從兩個 AWS 服務AWS CodeDeploy和 收集問題清單AWS CloudFormation。

調查結果是一項選擇加入功能。您可以在準備精靈中、初次加入 Incident Manager 時，或在設定頁面上稍後啟用它。

當您啟用問題清單功能時，Invent Manager 會為您建立服務角色。此服務角色包含從 CodeDeploy 和 CloudFormation 擷取問題清單所需的許可。

若要在跨帳戶案例中使用問題清單，請在管理帳戶中啟用 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，以協助您使用調查結果功能。

主題

- 啟用和建立問題清單的服務角色
- 設定跨帳戶調查結果支援的許可

啟用和建立問題清單的服務角色

當您啟用調查結果功能時，Invent Manager `IncidentManagerIncidentAccessServiceRole` 會代表您建立名為 的服務角色。此服務角色提供 Incident Manager 收集有關 CodeDeploy 部署和 CloudFormation 堆疊更新的資訊所需的許可，這些更新發生在事件建立時。

> **Note**
>
> 如果您將 Incident Manager 與組織搭配使用，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調查結果，必須在每個應用程式帳戶中建立服務角色。如需有關使用 CloudFormation 範本在您的應用程式帳戶中建立此角色的資訊，請參閱 中的步驟 4設定跨帳戶事件管理。

此服務角色與 AWS 受管政策相關聯。如需此政策中許可的相關資訊，請參閱 AWS 受管政策：AWSIncidentManagerIncidentAccessServiceRolePolicy。

如需在 Incident Manager 加入程序中啟用問題清單的資訊，請參閱 Incident Manager 入門。

如需有關在完成加入程序後啟用問題清單的資訊，請參閱 管理問題清單功能。

設定跨帳戶調查結果支援的許可

若要在 中設定組織的帳戶間使用調查結果功能 AWS RAM，每個應用程式帳戶都必須設定 Incident Manager 的許可，以代表其擔任管理帳戶的服務角色。

這些許可可以透過部署 AWS CloudFormation 由 提供的範本，在應用程式帳戶中設定 AWS，該範本會建立角色 `IncidentManagerIncidentAccessServiceRole`。

如需有關在應用程式帳戶中下載和部署此範本的資訊，請參閱 中的步驟 4在 Incident Manager 中管理跨 AWS 帳戶 和 區域的事件。

在 Incident Manager 中自動或手動建立事件

Incident Manager 是 中的工具 AWS Systems Manager，可協助您管理和快速回應事件。您可以設定 Amazon CloudWatch 和 Amazon EventBridge，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，或使用來自 AWS CLI 或 AWS SDK 的 StartIncident API 動作。Incident Manager 會將從相同 CloudWatch 警示或 EventBridge 事件建立的重複事件刪除為相同的事件。

對於 CloudWatch 警示或 EventBridge 事件自動建立的事件，Invent Manager 會嘗試在與事件規則或警示 AWS 區域 相同的 中建立事件。如果 Incident Manager 無法在 中使用 AWS 區域，CloudWatch 或 EventBridge 會自動在複寫集中指定的其中一個可用區域中建立事件。如需詳細資訊，請參閱在 Incident Manager 中管理跨 AWS 帳戶 和 區域的事件。

當系統建立事件時，Incident Manager 會自動收集事件所涉及 AWS 資源的相關資訊，並將此資訊新增至相關項目索引標籤。如果您在回應計劃中指定 Runbook，當系統建立事件時，Incident Manager 可以將事件所涉及 AWS 資源的相關資訊傳送至 Runbook。系統接著可以在啟動 Runbook 並嘗試修復問題時，以這些資源為目標。

當系統建立事件時，也會在 Systems Manager 的元件 OpsCenter 中建立父操作工作項目 (OpsItem)，並將其連結至事件做為相關項目。您可以使用此 OpsItem 來追蹤相關的工作和未來的事件分析。呼叫 OpsCenter 會產生成本。如需 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。
>
> - 如果 Incident Manager 無法使用，則只有在複寫集中已指定至少兩個區域 AWS 區域 時，系統才能容錯移轉並在其他 中建立事件。如需設定複寫集的資訊，請參閱 Incident Manager 入門。
> - 跨區域容錯移轉建立的事件不會叫用回應計劃中指定的 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 會與 Systems Manager 和 Incident Manager 搭配使用，從回應計劃範本建立事件。這需要下列先決條件：

- Incident Manager 已設定並已建立複寫集。此步驟會在您的帳戶中建立 Incident Manager 服務連結角色，並提供必要的許可。
- 已設定的 Incident Manager 回應計劃。若要了解如何設定 Incident Manager 回應計劃，請參閱本指南在 Incident Manager 中建立和設定回應計劃的事件準備一節。
- 監控應用程式的已設定 CloudWatch 指標。如需監控最佳實務，請參閱本指南監控事件準備一節中的 。

使用啟動事件動作建立警示

1. 在 CloudWatch 中建立警示。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示。
2. 選擇警示要執行的動作時，請選取新增 Systems Manager 動作。
3. 選擇建立事件，然後選取此事件的回應計畫。
4. 完成所選警示類型指南中的其餘步驟。

> **Tip**
>
> 您也可以將建立事件動作新增至任何現有的警示。

使用 EventBridge 事件自動建立事件

EventBridge 規則會監控事件模式。如果事件符合定義的模式，則 Incident Manager 會使用所選的回應計畫建立事件。

使用 SaaS 合作夥伴事件建立事件

您可以設定 EventBridge 從軟體即服務 (SaaS) 合作夥伴應用程式和服務接收事件，以允許第三方整合。設定 EventBridge 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來建立事件。若要查看第三方整合的清單，請參閱從 SaaS 合作夥伴接收事件。

設定 EventBridge 以接收來自 SaaS 整合的事件。

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中, 選擇合作夥伴事件來源。

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 Amazon AppFlow 使用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)。

建立從 SaaS 合作夥伴觸發事件的規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
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. 針對事件匯流排，選擇與此合作夥伴對應的事件匯流排。
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. 在事件來源欄位中，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. 針對事件來源，選擇 EventBridge 合作夥伴
11. 針對合作夥伴，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，請選擇編輯、進行變更，然後選擇儲存。
13. 選擇下一步。
14. 針對選取目標，選擇 Incident Manager 回應計畫，然後選擇回應計畫。

> **Note**
>
> 選取回應計劃時，您擁有並與您的帳戶共用的所有回應計劃都會出現在回應計劃下拉式清單中。

15. 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 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. 檢閱您的規則，然後選擇建立規則。

使用 AWS 服務事件建立事件

EventBridge 也會從支援服務的事件中 AWS 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，您可以為 AWS 服務設定規則。

建立從 AWS 服務觸發事件的規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
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. 在事件來源欄位中，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. 針對服務名稱，選擇監控事件的服務。
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，請選擇編輯、進行變更，然後選擇儲存。
13. 選擇下一步。
14. 針對選取目標，選擇 Incident Manager 回應計畫，然後選擇回應計畫。

> **Note**
>
> 選取回應計劃時，您擁有並與您的帳戶共用的所有回應計劃都會出現在回應計劃下拉式清單中。

15. 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 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. 檢閱您的規則，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畫，使用 Incident Manager 主控台手動追蹤事件。使用下列步驟來建立事件。

1. 開啟 Incident Manager 主控台。
2. 選擇開始事件。
3. 針對回應計畫，從清單中選擇回應計畫。
4. （選用）若要覆寫已定義回應計劃提供的標題，請輸入事件標題。
5. （選用）若要覆寫已定義回應計劃提供的影響，請輸入事件的影響。

手動啟動事件所需的 IAM 許可

若要手動啟動事件，使用者需要存取 Incident Manager 主控台、檢視回應計劃和啟動事件的許可。當使用者啟動事件時，Incident Manager 會使用轉送存取工作階段 (FAS) 來呼叫 `StartEngagement`。`StartIncident`

下列 IAM 政策提供手動啟動事件的必要許可、檢視可與其建立事件的回應計畫，以及在建立事件之後檢視和編輯事件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

此政策包含以下許可：

- ssm-incidents：StartIncident - 允許使用者使用主控台或 API 手動啟動事件。這會從回應計劃建立新的事件記錄。
- ssm-incidents：GetResponsePlan - 允許使用者擷取特定回應計劃的相關資訊。
- ssm-incidents：ListResponsePlans - 允許使用者列出其帳戶中的所有回應計劃。
- ssm-incidents：TagResource - 允許將標籤新增至 Incident Manager 資源，包括事件和回應計劃。
- ssm-incidents：GetIncidentRecord - 允許使用者擷取特定事件的詳細資訊。
- ssm-incidents：ListIncidentRecords - 允許使用者列出其帳戶中的所有事件。
- ssm-incidents：UpdateIncidentRecord - 允許使用者更新現有事件的詳細資訊。
- ssm-contacts：StartEngagement （有條件） - 允許 Incident Manager 開始與聯絡人互動。條件可確保只能透過 Incident Manager 呼叫。
- ssm：CreateOpsItem （有條件） - 允許 Incident Manager 在 OpsCenter 中建立 OpsItem。OpsCenter 條件可確保只能透過 Incident Manager 呼叫。

aws：CalledViaFirst 條件金鑰可確保只有在請求透過 Incident Manager 服務時，才能使用特定許可（例如 `StartEngagement`)。此方法使用 FAS 而非服務連結角色，可防止可能產生安全風險的潛在跨帳戶呼叫。

在 Incident Manager 主控台中檢視事件詳細資訊

AWS Systems Manager Incident Manager 會追蹤您的事件，從偵測到事件的那一刻到解決，以及透過事件後分析。您可以在 Incident Manager 主控台的事件清單頁面上找到所有事件，其中包含直接連結至事件詳細資訊的連結。

主題

- 在主控台中檢視事件清單
- 在主控台中檢視事件詳細資訊

在主控台中檢視事件清單

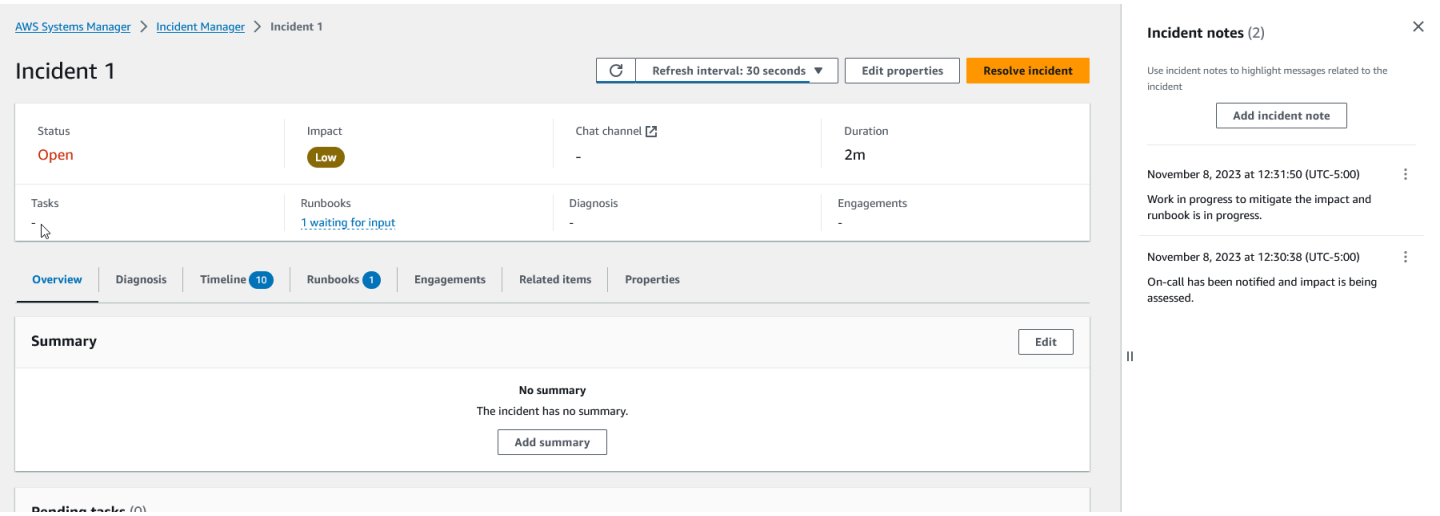
事件清單頁面包含三個區段：開啟事件、已解決的事件和分析。您可以手動追蹤新事件，並從此頁面建立分析。若要進一步了解手動追蹤事件，請參閱本指南手動建立事件的事件建立一節。若要了解事後分析，請參閱本指南的 在 Incident Manager 中執行事件後分析一節。

事件詳細資訊會以標題、影響、持續時間和該事件的聊天管道的圖磚顯示開啟事件。在您解決事件之後，它會移至已解決的事件清單。分析位於第二個索引標籤中。

在主控台中檢視事件詳細資訊

事件詳細資訊頁面提供詳細的洞見和工具，您可以用來管理事件。從此頁面，您可以啟動 Runbook 來緩解事件、新增事件備註、與其他解析程式互動，以及檢視事件詳細資訊，例如時間表、指標、屬性和相關資源。

如下圖所示，事件詳細資訊頁面包含數個區段：頂端橫幅、事件備註，以及包含其他資訊和資源的七個索引標籤。根據預設，頂端橫幅和事件備註區段會顯示在所有事件詳細資訊頁面上。



本主題說明事件詳細資訊頁面的元素，以及您可以從頁面執行的動作。

頂端橫幅

每個事件詳細資訊頁面上的頂端橫幅都包含下列資訊：

- 狀態 – 事件的目前狀態可以是開啟或解決。
- 影響 – 事件對您環境的影響。它可以是高、中和低。若要變更事件的影響，請選擇編輯屬性。
- 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經過的時間量。
- Runbooks – 與此事件相關聯的 Runbook 狀態。狀態可能正在等待輸入、成功或失敗。如果 Runbook 的狀態正在等待輸入，您可以選擇 Runbook 以檢視動作詳細資訊。您可以選擇失敗以檢視逾時、失敗或取消的 Runbook。
- 參與 – 參與總數和每個參與的狀態。當您建立參與時，其狀態為已參與。確認參與後，狀態會從 Engaged 變更為 Confirmd。Incident Manager 不支援第三方互動的確認。這類參與會維持在 Engaged 狀態。

您可以在橫幅的右上角選擇編輯，以編輯事件標題、影響和聊天頻道。

事件備註

畫面右側會顯示事件備註區段。使用備註，您可以與其他處理事件的使用者合作和通訊。您可以說明您套用的緩解措施、您識別的潛在根本原因，或事件的目前狀態。最佳實務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採取的動作。如果您需要即時與其他解析程式通訊，請使用 Incident Manager 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。備註可以包含事件狀態或任何其他相關資訊的更新，這些資訊可為其他使用者提供可見性。如有需要，您也可以編輯或刪除事件備註。

> **Note**
>
> 具有執行 `ssm-incidents:UpdateTimelineEvent`和 `ssm-incidents:DeleteTimelineEvent`動作的 IAM 許可的任何使用者都可以編輯和刪除備註。不過，當您與另一個帳戶共用事件時，資源政策不包含 `ssm-incidents:DeleteTimelineEvent`動作。這可防止與您共用事件的使用者刪除備註。您可以在 AWS CloudTrail 主控台中檢視 Incident Manager 事件中備註的稽核線索。

標籤

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

概觀

概觀索引標籤是回應者的登陸頁面。它包含事件摘要、最近的時間軸事件清單，以及目前的 Runbook 步驟。

回應者使用 摘要來掌握已採取的動作、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**
>
> 如果多個回應者同時編輯摘要欄位，則提交編輯的回應者最後會覆寫所有其他輸入。

最近時間軸事件區段包含由 Incident Manager 填入五個最近事件的時間軸。使用本節來了解事件的狀態，以及最近發生的情況。若要檢視完整的時間軸，請繼續前往時間軸索引標籤。

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

診斷索引標籤包含託管 AWS 應用程式和系統的重要資訊，包括指標和啟用後調查結果的相關資訊。

使用指標

Incident Manager 使用 Amazon CloudWatch 填入此索引標籤上的指標和警示圖表。若要進一步了解定義警示和指標的事件管理最佳實務，請參閱本使用者指南監控的事件規劃一節。

新增指標

- 選擇此標籤右上角的新增。
  - 若要從現有的 CloudWatch 儀表板新增指標，請選擇從現有的 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指標和警示。
    b. （選用）您也可以從儀表板選取指標以檢視特定指標。
  - 選取從 CloudWatch 並貼上指標來源，以新增單一指標。若要複製指標來源：
    a. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
    b. 在導覽窗格中，選擇指標。
    c. 在所有指標索引標籤上，在搜尋欄位中輸入搜尋字詞，例如指標名稱或資源名稱，然後選擇輸入。

       例如，如果您搜尋`CPUUtilization`指標，您會看到與此指標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. 選擇來源索引標籤並複製來源。

指標警示圖形只能透過相關回應計劃新增至事件詳細資訊，或在新增指標時選取從現有的 CloudWatch 儀表板。

若要移除指標，請選擇移除，然後從提供的指標下拉式清單中選擇您要移除的指標。

從 AWS CodeDeploy 和 檢視問題清單 AWS CloudFormation

啟用問題清單並設定所有必要的許可後，任何可能與特定事件相關的問題清單都會連接到事件。回應者可以在事件詳細資訊頁面上檢視這些調查結果的相關資訊。

從 CodeDeploy 和 CloudFormation 檢視問題清單

1. 開啟 Incident Manager 主控台。
2. 選擇要調查的事件名稱。

3. 在診斷索引標籤的調查結果區域中，比較任何報告調查結果的開始時間與事件的開始時間。
4. 若要檢視問題清單的詳細資訊，請在參考欄中選擇 CodeDeploy 或 CloudFormation 問題清單的連結。

時間表

使用時間軸索引標籤來追蹤事件發生期間的事件。Incident Manager 會自動填入時間軸事件，以識別事件發生期間的重要事件。回應者可以根據手動偵測到的發生情況來新增自訂事件。在事件後分析期間，時間軸索引標籤會提供寶貴的洞見，讓您了解如何在未來更好地準備和回應事件。如需事件後分析的詳細資訊，請參閱 在 Incident Manager 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。所有時間都會顯示在您的當地時區。提供時間軸中出現事件的簡短描述。

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。

執行手冊

事件詳細資訊頁面的 Runbooks 索引標籤可讓回應者檢視 Runbook 步驟並啟動新的 Runbook。

若要啟動新的 Runbook，請在 Runbooks 區段中選擇啟動 Runbook。使用搜尋欄位尋找您要啟動的 Runbook。提供啟動 Runbook 時要使用的任何必要參數和 Runbook 版本。從 Runbooks 索引標籤的事件期間啟動的 Runbook 會使用目前登入帳戶的許可。

若要導覽至 Systems Manager 中的 Runbook 定義，請在 Runbook 下選擇 Runbook 的標題。若要導覽至 Systems Manager 中執行中的 Runbook 執行個體，請選擇執行詳細資訊下的執行詳細資訊。這些頁面會顯示用來啟動 Runbook 的範本，以及目前執行中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 自動採取或回應者手動執行的步驟清單。這些步驟會隨著成為目前步驟而展開，顯示完成步驟所需的資訊，或步驟執行方式的詳細資訊。自動化完成後，自動 Runbook 步驟會解析。手動步驟需要回應者在每個步驟底部選擇下一步。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 Runbook。這將停止執行 Runbook，而不會完成 Runbook 中的任何進一步步驟。

參與

事件詳細資訊的參與索引標籤可推動回應者和團隊的參與。在此索引標籤中，您可以查看參與的人員、已回應的人員，以及哪些回應者將參與作為呈報計畫的一部分。回應者可以直接從此索引標籤與其他聯絡人互動。若要進一步了解如何建立聯絡人和呈報計畫，請參閱本指南的 在 Incident Manager 中建立和設定聯絡人和 在 Incident Manager 中建立回應者參與的呈報計畫章節。

您可以使用聯絡人和升級計劃來設定回應計劃，以在事件開始時自動開始參與。若要進一步了解如何設定回應計劃，請參閱本指南的 在 Incident Manager 中建立和設定回應計劃一節。

您可以在 資料表中找到每個聯絡人的相關資訊。此資料表包含下列資訊：

- 名稱 – 顯示其聯絡方式和參與計劃之聯絡詳細資訊頁面的連結。
- 呈報計畫 – 參與聯絡的呈報計畫連結。
- 聯絡來源 – 識別與此聯絡互動的服務，例如 AWS Systems Manager 或 PagerDuty。
- 已參與 – 顯示計畫何時與聯絡人互動，或何時與聯絡人互動，做為呈報計畫的一部分。
- 已確認 – 顯示聯絡人是否確認參與。

若要確認參與，回應者可以執行下列其中一項操作：

- 電話 – 出現提示**1**時輸入 。
- SMS – 使用提供的程式碼回覆訊息，或在事件的參與索引標籤中輸入提供的程式碼。
- 電子郵件 – 在事件的參與索引標籤中輸入提供的程式碼。

相關項目

相關項目標籤用於收集與事件緩解相關的資源。這些資源可以是 ARNs、外部資源的連結，或上傳至 Amazon S3 儲存貯體的檔案。資料表會顯示描述性標題和 ARN、連結或儲存貯體詳細資訊。使用 S3 儲存貯體之前，請參閱《Amazon S3 使用者指南》中的 Amazon S3 的安全最佳實務。 Amazon S3

將檔案上傳至 Amazon S3 儲存貯體時，版本控制會在該儲存貯體上啟用或停用。在儲存貯體上啟用版本控制時，與現有檔案同名上傳的檔案會新增為檔案的新版本。如果版本控制已暫停，上傳的檔案會與現有檔案名稱相同，以覆寫現有檔案。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。 Amazon S3

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。 Amazon S3

屬性

屬性索引標籤提供事件的下列詳細資訊。

在事件屬性區段中，您可以檢視下列項目：

- 狀態 – 說明事件的目前狀態。事件可以開啟或解決。
- 開始時間 – 在 Incident Manager 中建立事件的時間。
- 解決時間 – 在 Incident Manager 中解決事件的時間。
- Amazon Resource Name (ARN) – 事件的 ARN。從聊天或搭配 AWS Command Line Interface (AWS CLI) 命令參考事件時，請使用 ARN。
- 回應計畫 – 識別所選事件的回應計畫。選擇回應計劃會開啟回應計劃的詳細資訊頁面。
- Parent OpsItem – 識別建立為事件父項的 OpsItem。父 OpsItem 可以有多個相關事件和後續動作項目。選取父 OpsItem 會在 OpsCenter 中開啟 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。
- 擁有者 – 建立事件的帳戶。

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索引鍵和值。如需 Incident Manager 中標籤的詳細資訊，請參閱 Incident Manager 中的標記資源。

在 Incident Manager 中執行事件後分析

事件後分析會引導您識別事件回應的改進，包括偵測和緩解的時間。分析也可以協助您了解事件的根本原因。Incident Manager 會建立建議的動作項目，以改善您的事件回應。

事件後分析的優點

- 改善事件回應
- 了解問題的根本原因
- 使用可交付動作項目解決根本原因
- 分析事件的影響
- 在組織內擷取和共用學習

不對 使用分析的項目

分析是無責的，不會按名稱呼叫人員。

「無論我們發現什麼，我們了解並真心相信，考慮到每個人當時知道的、他們的技能和能力、可用的資源，以及手頭的情況，每個人都能做到最好的工作。」 - Norm Kerth，Project Retrospectives：團隊審核手冊

分析詳細資訊

分析詳細資訊頁面會引導您完成收集資訊、評估改善項目和建立動作項目。分析詳細資訊頁面類似於事件詳細資訊，其中包含一些關鍵差異，例如歷史指標、可編輯時間表和問題，以改善未來的事件。

概觀

概觀是事件的摘要。此摘要包括背景、發生的情況、發生原因、緩解方式、持續時間和關鍵動作項目，以防止再次發生事件。概觀是高階。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，在事件持續時間內視覺化應用程式中的關鍵指標。您可以在此處新增指標圖表，這些圖表具有相同圖表中描述的一或多個指標。事件期間使用的指標會自動填入此索引標籤。我們建議您在事件期間新增關鍵時間點的描述、標題和註釋。

分析指標圖表時，您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
- 警示時間
- 參與時間
- 緩解開始時間
- 事件解決時間

限制

- CloudWatch 警示和指標表達式不會從事件匯入。
- 位於 Incident Manager 不支援之區域中的指標不會從事件匯入。
- 應用程式帳戶中的指標需要先設定 ，`CloudWatch-CrossAccountSharingRole`才能建立分析。如需角色的詳細資訊，請參閱 CloudWatch 使用者指南中的跨帳戶跨區域 CloudWatch 主控台。CloudWatch

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。事件時間軸會自動填入此索引標籤。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。

使用時間軸索引標籤來回答您在問題索引標籤上找到有關事件回應的問題。

問題

使用 Incident Manager 問題來改善解決應用程式中事件的時間，並減少事件發生。當您回答問題時，請更新指標和時間軸索引標籤以確保準確性。這些問題著重於事件回應的這些關鍵層面：

- 偵測 – 您可以縮短偵測時間嗎？ 是否有指標和警示的更新，可以更快地檢測到事件？
- 診斷 – 您可以縮短診斷時間嗎？ 回應計劃或呈報計劃是否有更新，可以更快地吸引合適的回應方？
- 緩解 – 您可以縮短緩解時間嗎？ 是否有您可以新增或改善的 Runbook 步驟？
- 預防 – 您可以防止未來事件發生嗎？ 為了探索事件的根本原因，Amazon 使用 5-Whys方法進行問題調查。

動作

Incident Manager 會建立建議的動作項目，供您在完成問題時檢閱。您可以選擇從此索引標籤接受並完成這些動作，也可以關閉這些動作。您可以透過選擇已捨棄的動作項目來檢閱已捨棄的動作項目。動作項目是一種 OpsItem，連結至 OpsCenter 中的分析和事件。

檢查清單

關閉分析之前，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，動作旁的圖示會從橢圓變更為核取記號，表示動作已完成。如果您尚未完成檢查清單項目，則 Incident Manager 會顯示一則訊息，確認回應者想要關閉分析而不完成分析。

分析範本

分析範本提供一組問題，深入探討事件的根本原因。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

Incident Manager 根據 AWS 事件回應和問題分析最佳實務提供標準的問題範本，標題為 `AWSIncidents-PostIncidentAnalysisTemplate`。

建立分析範本

我們建議您使用預設`AWSIncidents-PostIncidentAnalysisTemplate`範本，並新增適用於您的使用案例的其他問題或區段。根據預設範本建立分析範本 使用此範本作為在管理帳戶中建立分析範本的起點。然後，您可以將分析範本複製到您啟用 Incident Manager 的每個區域。

建立分析範本

1. 呼叫 `GetDocument`動作，並使用其`Name`參數下載 `AWSIncidents-PostIncidentAnalysisTemplate`。如需`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。建議您在 `Incident questions` 區段中新增問題或區段。
3. 若要建立新的範本，請使用 `CreateDocument`操作搭配上一個步驟中更新的 JSON。您必須包含下列項目，其中 *`Analysis_Template_Name`*是範本的名稱，

   - `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 Create (建立)。

列印格式化的事件分析

您可以產生完整或不完整分析的副本，該分析已格式化為列印。您也可以將此副本儲存為 PDF。您可以一次列印一個分析。目前不支援批次列印多個分析。

列印格式化分析

1. 開啟 Incident Manager 主控台。
2. 選擇分析索引標籤。
3. 選擇您要列印的分析標題。
4. 在分析詳細資訊頁面的右上角，選擇列印。
5. 在列印事件分析對話方塊中，清除您不想要包含在列印版本中的分析區段。根據預設，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. 選擇您的列印目的地或格式。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**
>
> 本機列印控制項是指 Web 瀏覽器和裝置提供的使用者介面。
> 列印目的地是為您的裝置設定，且可從中存取的目的地。

Incident Manager 教學課程

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

主題

- 教學課程：搭配 Incident Manager 使用 Systems Manager Automation Runbook
- 教學課程：在 Incident Manager 中管理安全事件

教學課程：搭配 Incident Manager 使用 Systems Manager Automation Runbook

您可以使用 AWS Systems Manager Automation Runbook 來簡化 AWS 服務的常見維護、部署和修復任務。在本教學課程中，您將建立自訂 Runbook，以在 Incident Manager 中自動化事件回應。本教學課程的案例涉及指派給 Amazon EC2 指標的 Amazon CloudWatch 警示。 Amazon EC2 當執行個體進入觸發警示的狀態時，Invent Manager 會自動執行下列任務：

1. 在 Incident Manager 中建立事件。
2. 啟動 Runbook，嘗試修復問題。
3. 將 Runbook 結果發佈至 Incident Manager 中的事件詳細資訊頁面。

本教學中描述的程序也可以與 Amazon EventBridge 事件和其他類型的 AWS 資源搭配使用。透過自動化對警示和事件的修補回應，您可以降低事件對組織及其資源的影響。

本教學說明如何編輯指派給 Incident Manager 回應計劃的 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，建議您在開始之前設定這些資源。如需詳細資訊，請參閱下列主題：

- 《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示
- Amazon EC2 使用者指南中的 Amazon EC2 執行個體 Amazon EC2
- Amazon EC2 使用者指南中的 Amazon EC2 執行個體 Amazon EC2
- 在 Incident Manager 中建立和設定回應計劃

> **Important**
>
> 您將透過建立 AWS 資源和使用 Runbook 自動化步驟來產生成本。如需詳細資訊，請參閱 AWS 定價。

主題

- 任務 1：建立 Runbook
- 任務 2：建立 IAM 角色
- 任務 3：將 Runbook 連接到您的回應計劃
- 任務 4：將 CloudWatch 警示指派給您的回應計劃
- 任務 5：驗證結果

任務 1：建立 Runbook

使用下列程序在 Systems Manager 主控台中建立 Runbook。從 Incident Manager 事件調用時，執行手冊會重新啟動 Amazon EC2 執行個體，並使用執行手冊執行的相關資訊更新事件。開始之前，請確認您擁有建立 Runbook 的許可。如需詳細資訊，請參閱AWS Systems Manager 《 使用者指南》中的設定自動化。

> **Important**
>
> 檢閱下列有關建立本教學課程 Runbook 的重要詳細資訊：
>
> - Runbook 適用於從 CloudWatch 警示來源建立的事件。如果您將此 Runbook 用於其他類型的事件，例如手動建立的事件，則第一個 Runbook 步驟中的時間軸事件將無法找到，且系統會傳回錯誤。
> - Runbook 需要 CloudWatch 警示包含稱為 的維度`InstanceId`。Amazon EC2 執行個體指標的警示具有此維度。如果您將此 Runbook 與其他指標 （或其他事件來源，例如 EventBridge) 搭配使用，則必須變更`JsonDecode2`步驟以符合案例中擷取的資料。
> - Runbook 會嘗試透過重新啟動 Amazon EC2 執行個體來修復觸發警示的問題。對於真實事件，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修補動作來更新 Runbook。

如需建立 Runbook 的詳細資訊，請參閱AWS Systems Manager 《 使用者指南》中的使用 Runbook。

建立 Runbook

1. 在 https：//https://console.aws.amazon.com/systems-manager/ 開啟 AWS Systems Manager 主控台。
2. 在導覽窗格中，選擇 Documents (文件)。
3. 選擇自動化。
4. 針對名稱，輸入 Runbook 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)。

任務 2：建立 IAM 角色

使用下列教學課程來建立 AWS Identity and Access Management (IAM) 角色，提供 Incident Manager 啟動回應計劃中指定 Runbook 的許可。本教學課程中的 Runbook 會重新啟動 Amazon EC2 執行個體。當您將 Runbook 連接到回應計劃時，您將在下一個任務中指定此 IAM 角色。

建立從回應計劃啟動 Runbook 的 IAM 角色

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，選擇角色，然後選擇建立角色。
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，在其他 AWS 服務的使用案例欄位中輸入 **Incident Manager**。
5. 選擇 Incident Manager，然後選擇下一步。
6. 在新增許可頁面上，選擇建立政策。許可編輯器會在新的瀏覽器視窗或索引標籤中開啟。
7. 在編輯器中，選擇 JSON 索引標籤。
8. 將下列許可政策複製並貼到 JSON 編輯器。將 AWS 帳戶 *account_ID* 取代為您的 ID。

```
{
    "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. （選用）如有需要，請將標籤新增至您的政策。
11. 選擇下一步：檢閱。
12. 在名稱欄位中，輸入名稱，協助您將此角色識別為用於本教學課程。
13. （選用）在描述欄位中輸入描述。
14. 選擇 建立政策。
15. 導覽回您要建立之角色的瀏覽器視窗或索引標籤。隨即顯示新增許可頁面。
16. 選擇重新整理按鈕（位於建立政策按鈕旁），然後在篩選條件方塊中輸入您建立的滲透政策名稱。
17. 選擇您建立的許可政策，然後選擇下一步。
18. 在名稱、檢閱和建立頁面上，針對角色名稱輸入名稱，協助您將此角色識別為用於本教學課程。

19. （選用）在描述欄位中輸入描述。
20. 檢閱角色詳細資訊，視需要新增標籤，然後選擇建立角色。

任務 3：將 Runbook 連接到您的回應計劃

透過將 Runbook 連接到您的 Incident Manager 回應計劃，您可以確保一致、可重複且及時的緩解程序。Runbook 也可做為解析程式判斷下一個動作的起點。

將 Runbook 指派給您的回應計劃

1. 開啟 Incident Manager 主控台。
2. 選擇回應計劃。
3. 針對回應計劃，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來建立新的計劃。

   完成下列欄位：

   a. 在 Runbook 區段中，選擇選取現有的 Runbook。
   b. 對於擁有者，確認已選取我擁有的 。
   c. 針對 Runbook，選擇您在 中建立的 Runbook任務 1：建立 Runbook。
   d. 對於版本，請在執行時選擇預設。
   e. 在輸入區段中，針對 IncidentRecordArn 參數，選擇事件 ARN。
   f. 在執行許可區段中，選擇您在 中建立的 IAM 角色任務 2：建立 IAM 角色。
4. 儲存您的變更。

任務 4：將 CloudWatch 警示指派給您的回應計劃

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。

將 CloudWatch 警示指派給您的回應計劃

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中的警示下，選擇所有警示。
3. 選擇您要連線至回應計劃的 Amazon EC2 執行個體的警示。
4. 選擇動作，然後選擇編輯。確認指標具有稱為 的維度`InstanceId`。

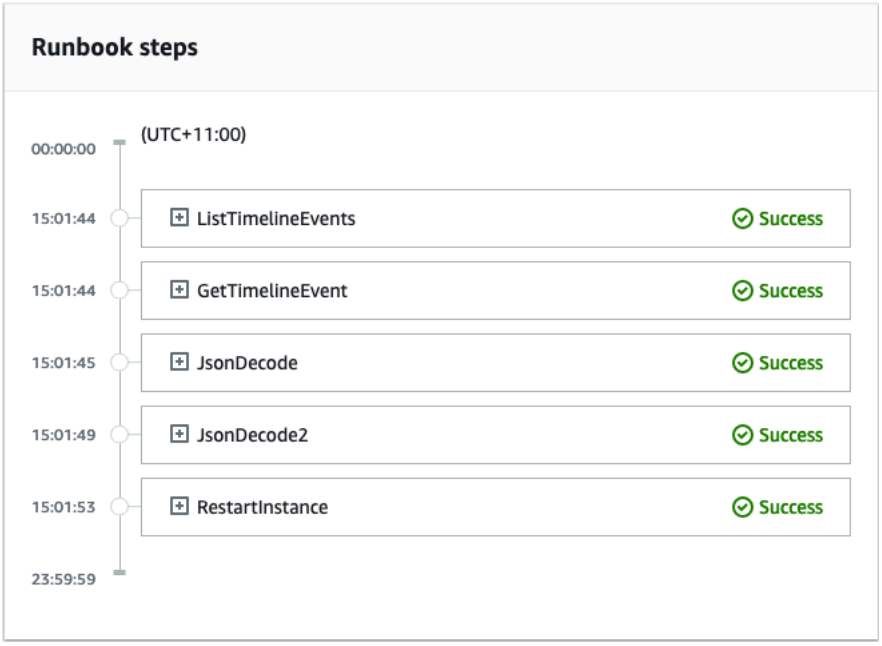
5. 選擇 Next (下一步)。
6. 針對設定動作精靈，選擇新增 Systems Manager 動作。
7. 選擇建立事件。
8. 選擇您在 中建立的回應計畫任務 3：將 Runbook 連接到您的回應計劃。
9. 選擇 Update alarm (更新警示)。

任務 5：驗證結果

若要驗證 CloudWatch 警示是否建立事件，然後處理回應計劃中指定的 Runbook，您必須觸發警示。觸發警示且 Runbook 完成處理後，您可以使用下列程序來驗證 Runbook 的結果。如需有關觸發警示的資訊，請參閱 AWS CLI 命令參考中的 set-alarm-state。

1. 開啟 Incident Manager 主控台。
2. 選擇 CloudWatch 警示建立的事件。
3. 選擇 Runbooks 索引標籤。
4. 在 Runbook 步驟區段中檢視在 Amazon EC2 執行個體上執行的動作。

   下圖示範如何在 主控台中報告您在本教學課程中建立的 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訊，請展開 JsonDecode2 步驟，然後展開輸出。

> **Important**
>
> 您必須清除您在本教學課程中實作的任何資源變更，而您不想保留這些變更。這包括對 Incident Manager 資源的變更，例如資源計劃和事件、CloudWatch 警示的變更，以及您在本教學課程中建立的 IAM 角色。

教學課程：在 Incident Manager 中管理安全事件

您可以同時使用 AWS Security Hub Amazon EventBridge 和 Incident Manager 來識別和管理 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 自動傳送的問題清單來建立事件。

> **Note**
>
> 本教學課程使用 EventBridge Security Hub。使用這些服務可能會產生費用。

先決條件

- 設定 Security Hub。如需詳細資訊，請參閱設定 AWS Security Hub。
- 在 Security Hub 中建立或更新問題清單。如需詳細資訊，請參閱 中的調查結果 AWS Security Hub。
- 設定回應計劃，Inventation Manager 會在建立您的安全事件時將其用作範本。如需詳細資訊，請參閱在 Incident Manager 中準備事件。

在此教學課程中，我們使用預先定義的模式來建立 EventBridge 規則。若要使用自訂模式建立規則，請參閱 AWS Security Hub 使用者指南中的使用自訂模式來建立規則。

建立 EventBridge 規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
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. 在事件來源欄位中，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. 針對AWS 服務，選擇 Security Hub。
12. 針對事件類型，選擇 Security Hub 調查結果 - 匯入。
13. 根據預設，EventBridge 會設定不含任何篩選條件值的事件模式。針對每個屬性，會選取任何**###**選項。更新這些篩選條件，根據最影響您環境的安全調查結果來建立事件。
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 Incident Manager 回應計劃。
17. 針對回應計劃，選擇要用作建立事件範本的回應計劃。
18. 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 Next (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調查結果將在 Incident Manager 中建立事件。您可以從這些事件中分類、管理、監控和建立事件後分析。

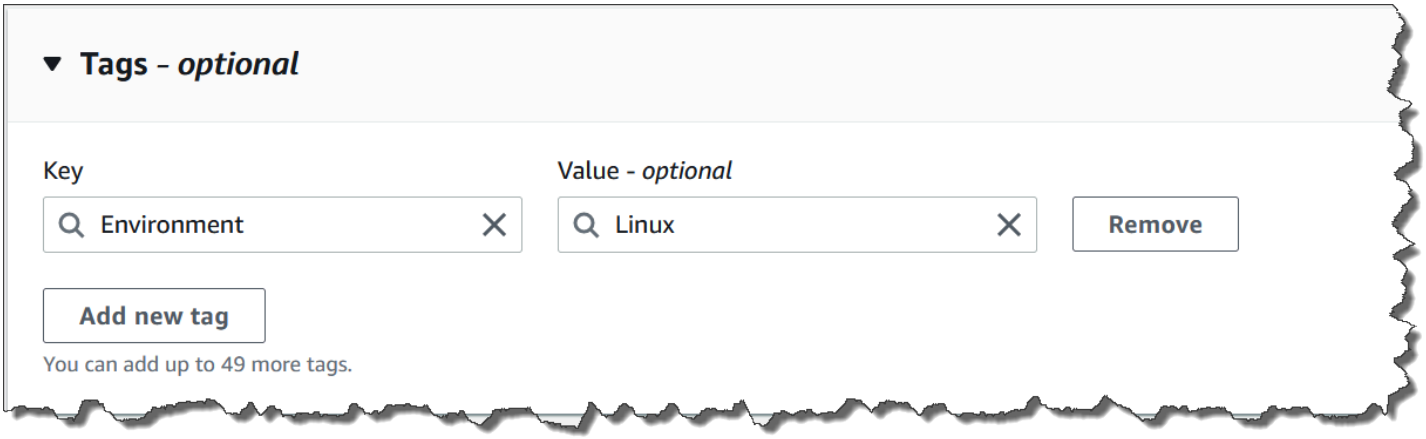
Incident Manager 中的標記資源

標籤是選用的中繼資料，您可以在複寫集中 AWS 區域 指定的 中將其指派給 Incident Manager 資源。您可以將標籤指派給回應計劃、事件記錄和聯絡人。您也可以將標籤新增至通話中排程和輪換。您也可以將標籤新增至複寫集本身。標籤可讓您以不同的方式分類和控制對這些資源的存取。每個標籤皆包含由您定義的一個金鑰與一個選用值。建議您設計一組標籤金鑰，以符合您對每個 Incident Manager 資源類型的需求。使用一組一致的標籤金鑰，可讓您更輕鬆地管理這些資源，以及管理對這些資源的存取。您可以根據標籤來搜尋和篩選資源。如需使用標籤控制對資源的存取的詳細資訊，請參閱《IAM 使用者指南》中的使用標籤控制對 AWS 資源的存取。

您可以在建立回應計劃時，在事件預設區段中指定標籤。當使用回應計劃建立事件時，這些標籤會套用至事件記錄。

> **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 Incident Manager 主控台新增或移除標籤。下列螢幕擷取畫面會顯示主控台頁面的標籤區域，其中包含用於新增標籤索引鍵和值的欄位，以及用於新增和移除標籤的按鈕。



若要以程式設計方式使用標籤，請使用下列 API 動作：

- TagResource
- UntagResource
- ListTagsForResource

Important

套用至回應計劃、事件記錄、聯絡人、待命排程和輪換的標籤，以及複寫集只能從資源擁有者帳戶檢視和修改。

中的安全性 AWS Systems Manager Incident Manager

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計劃中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計劃 AWS Systems Manager Incident Manager，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 Incident Manager 時套用共同責任模型。下列主題說明如何設定 Incident Manager 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務 來協助您監控和保護 Incident Manager 資源。

主題

- Incident Manager 中的資料保護
- 的 Identity and Access Management AWS Systems Manager Incident Manager
- 在 Incident Manager 中使用共用聯絡人和回應計劃
- 的合規驗證 AWS Systems Manager Incident Manager
- 中的彈性 AWS Systems Manager Incident Manager
- 中的基礎設施安全 AWS Systems Manager Incident Manager
- 使用 AWS Systems Manager Incident Manager 和界面 VPC 端點 (AWS PrivateLink)
- Incident Manager 中的組態和漏洞分析
- 中的安全最佳實務 AWS Systems Manager Incident Manager

Incident Manager 中的資料保護

AWS 共同責任模型適用於 中的資料保護 AWS Systems Manager Incident Manager。如此模型所述，AWS 負責保護執行所有 的全域基礎設施 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。如需資料隱私權的詳細資訊，請參閱資料隱

私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，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 Incident Manager 或使用 AWS 服務 主控台、API AWS CLI或其他 AWS SDKs 時。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。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

Incident Manager 預設會使用 SSL/TLS 加密傳輸中的資料。

資料加密

Incident Manager 使用 AWS Key Management Service (AWS KMS) 金鑰來加密您的 Incident Manager 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，以提供針對雲端擴展的金鑰管理系統。Incident Manager 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 Incident Manager，您必須設定複寫集，其中包括設定加密。Incident Manager 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寫集，也可以使用您在 中建立的自有客戶受管金鑰 AWS KMS 來加密複寫集中的區域。Incident Manager 僅支援對稱加密 AWS KMS 金鑰，以加密您在其中建立的資料 AWS KMS。Incident Manager 不支援具有匯入 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。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，並定義控制 Incident Manager 如何使用客戶受管金鑰的金鑰政策。當您使用客戶受管金鑰搭配 Incident Manager 進行加密時， AWS KMS 客戶受管金鑰必

須與資源位於相同的區域。若要進一步了解如何在 Incident Manager 中設定資料加密，請參閱 準備精靈。

使用 AWS KMS 客戶受管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》中的AWS KMS 概念 - KMS 金鑰和AWS KMS 定價。

> **Important**
>
> 如果您使用 a AWS KMS key (KMS 金鑰） 來加密複寫集和 Incident Manager 資料，但之後決定刪除複寫集，請務必先刪除複寫集，再停用或刪除 KMS 金鑰。

若要允許 Incident Manager 使用您的客戶受管金鑰來加密資料，您必須將下列政策陳述式新增至客戶受管金鑰的金鑰政策。若要進一步了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》中的在 中使用金鑰政策 AWS KMS。此政策提供下列許可：

- 允許 Incident Manager 執行唯讀操作，以尋找您帳戶中 Incident Manager AWS KMS key 的 。
- 允許 Incident Manager 使用 KMS 金鑰來建立授予和描述金鑰，但僅限於代表帳戶中有權使用 Incident Manager 的主體時。如果政策陳述式中指定的委託人沒有使用 KMS 金鑰和使用 Incident Manager 的許可，呼叫會失敗，即使它來自 Incident Manager 服務。

```
{
"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`值取代為建立複寫集的 IAM 主體。

Incident Manager 在所有對 的請求中使用加密內容 AWS KMS 進行密碼編譯操作。您可以使用此加密內容來識別 Incident Manager 使用您的 KMS 金鑰的 CloudTrail 日誌事件。Incident Manager 使用以下加密內容：

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

的 Identity and Access Management AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 Incident Manager 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS Systems Manager Incident Manager 如何使用 IAM
- AWS Systems Manager Incident Manager的身分型政策範例
- 的資源型政策範例 AWS Systems Manager Incident Manager
- Incident Manager 中的跨服務混淆代理人預防
- 針對 Incident Manager 使用服務連結角色
- AWS 的 受管政策 AWS Systems Manager Incident Manager
- 對 AWS Systems Manager Incident Manager 身分和存取進行故障診斷

目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在 Incident Manager 中執行的工作。

服務使用者 – 如果您使用 Incident Manager 服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 Incident Manager 功能來執行工作時，您可能需要額外的許可。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 Incident Manager 中的功能，請參閱對 AWS Systems Manager Incident Manager 身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責 Incident Manager 資源，您可能擁有 Incident Manager 的完整存取權。您的任務是判斷服務使用者應存取哪些 Incident Manager 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Incident Manager 使用 IAM，請參閱 AWS Systems Manager Incident Manager 如何使用 IAM。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解如何撰寫政策以管理 Incident Manager 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Incident Manager 身分型政策範例，請參閱 AWS Systems Manager Incident Manager的身分型政策範例。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 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。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

AWS 帳戶 根使用者

建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務 和 資源。此身分稱為 AWS 帳戶 Theroot 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。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務 來使用臨時憑證來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、Identity Center 目錄，或使用透過身分來源提供的 AWS 服務 登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

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，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。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 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色 （主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 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。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 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 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是一種連結至 的服務角色。 AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件， AWS 當與身分或資源相關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 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政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種服務，用於分組和集中管理您企業擁有 AWS 帳戶 的多個 。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。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 使用者指南中的工作階段政策。

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。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS Systems Manager Incident Manager 如何使用 IAM

在您使用 IAM 管理 Incident Manager 的存取權之前，請先了解哪些 IAM 功能可與 Incident Manager 搭配使用。

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

IAM 功能	Incident Manager 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
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要全面了解 Incident Manager 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

Incident Manager 不支援拒絕存取使用 共用之資源的政策 AWS RAM。

Incident Manager 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

Incident Manager 的身分型政策範例

若要檢視 Incident Manager 身分型政策的範例，請參閱 AWS Systems Manager Incident Manager的身分型政策範例。

Incident Manager 中的資源型政策

支援資源型政策：是

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 （使用者或角色） 存取資源的許可。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 使用者指南》中的 IAM 中的快帳戶資源存取。

Incident Manager 服務僅支援兩種類型的資源型政策，稱為使用 AWS RAM 主控台或 PutResourcePolicy 動作，此動作會連接到回應計劃或聯絡人。此政策定義哪些委託人可以對回應計劃、聯絡人、呈報計劃和事件執行動作。Incident Manager 使用資源型政策跨帳戶共用資源。

Incident Manager 不支援拒絕存取使用 共用之資源的政策 AWS RAM。

若要了解如何將資源型政策連接至回應計劃或聯絡人，請參閱 在 Incident Manager 中管理跨 AWS 帳戶 和 區域的事件。

Incident Manager 中的資源型政策範例

若要檢視 Incident Manager 資源型政策的範例，請參閱 的資源型政策範例 AWS Systems Manager Incident Manager。

Incident Manager 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。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 Incident Manager 動作的清單，請參閱《服務授權參考》中的 定義的動作 AWS Systems Manager Incident Manager。

Incident Manager 中的政策動作在動作之前使用以下字首：

```
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 Incident Manager 身分型政策的範例，請參閱 AWS Systems Manager Incident Manager的身分型政策範例。

Incident Manager 會在兩個不同的命名空間中使用動作：ssm-incidents 和 ssm-contacts。為 Incident Manager 建立政策時，請務必針對動作使用正確的命名空間。SSM-Incidents 用於回應計劃和事件相關動作。SSM-Contacts 用於與聯絡人和聯絡互動相關的動作。例如：

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

Incident Manager 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。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 Incident Manager 資源類型及其 ARNs的清單，請參閱《服務授權參考》中的 定義的資源 AWS Systems Manager Incident Manager。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Systems Manager Incident Manager定義的動作。

若要檢視 Incident Manager 身分型政策的範例，請參閱 AWS Systems Manager Incident Manager的身分型政策範例。

Incident Manager 資源可用來建立事件、在聊天頻道中進行協作、解決事件，以及與回應者互動。如果使用者有權存取回應計劃，則可以存取從中建立的所有事件。如果使用者可以存取聯絡人或呈報計畫，他們可以在呈報計畫中與聯絡人互動。

Incident Manager 的政策條件索引鍵

支援服務特定的政策條件索引鍵：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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， 會使用邏輯OR操作 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，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

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

Incident Manager 中的存取控制清單 (ACLs)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

使用 Incident Manager 的屬性型存取控制 (ABAC)

支援 ABAC （政策中的標籤）：否

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用屬性型存取控制 (ABAC)。

搭配 Incident Manager 使用臨時登入資料

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。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登入資料。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。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的從使用者切換至 IAM 角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。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 中的暫時性安全憑證。

Incident Manager 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

Incident Manager 的服務角色

支援服務角色：是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Incident Manager 功能。只有在 Incident Manager 提供指引時，才能編輯服務角色。

在 Incident Manager 中選擇 IAM 角色

當您在 Incident Manager 中建立回應計畫資源時，您必須選擇角色，以允許 Incident Manager 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 Incident

Manager 會為您提供可供選擇的角色清單。選擇允許存取以執行自動化文件執行個體的角色非常重要。如需詳細資訊，請參閱將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件。當您在聊天應用程式聊天頻道中建立要在事件期間使用的 Amazon Q Developer 時，您可以選擇允許您直接從聊天使用命令的服務角色。若要進一步了解如何建立事件協同合作的聊天頻道，請參閱 在 Incident Manager 中為回應者建立和整合聊天頻道。若要進一步了解聊天應用程式中 Amazon Q Developer 中的 IAM 政策，請參閱《聊天應用程式管理員指南》中的在聊天應用程式中使用 Amazon Q Developer 管理執行命令的許可。

Incident Manager 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 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Incident Manager 服務連結角色的資訊，請參閱 針對 Incident Manager 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 Incident Manager 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 Incident Manager 定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS Systems Manager Incident Manager。

主題

- 政策最佳實務
- 使用 Incident Manager 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

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Incident Manager 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 受管政策並轉向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Incident Manager 主控台

若要存取 AWS Systems Manager Incident Manager 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中有關 Incident Manager 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色可以使用 Incident Manager 主控台解決事件，也請將 Incident Manager `IncidentManagerResolverAccess` AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

```
IncidentManagerResolverAccess
```

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "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，您想要授予 Amazon Web Services 帳戶中的 IAM 使用者存取其中一個 Incident Manager 回應計畫 exampleplan。您也想要允許使用者新增、更新和刪除回應計劃。

政策會將 ssm-incidents:ListResponsePlans、 ssm-incidents:GetResponsePlanssm-incidents:UpdateResponsePlan和 ssm-incident:ListResponsePlan許可授予使用者。

```
{
   "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/*"
      }
   ]
}
```

的資源型政策範例 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 支援 Incident Manager 回應計劃和聯絡人的資源型許可政策。

Incident Manager 不支援拒絕存取使用 共用資源的資源型政策 AWS RAM。

若要了解如何建立回應計劃或聯絡人，請參閱 在 Incident Manager 中建立和設定回應計劃和 在 Incident Manager 中建立和設定聯絡人。

依組織限制 Incident Manager 回應計劃存取

下列範例使用組織 ID 將許可授予組織中的使用者： 以o-abc123def45回應使用回應計畫 建立的事件myplan。

Condition 區塊使用 StringEquals 條件和 aws:PrincipalOrgID 條件索引鍵，這是 AWS Organizations 特定的條件索引鍵。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 Incident Manager 聯絡人存取權給委託人

下列範例會授予許可給具有 ARN 的委託人`arn:aws:iam::999988887777:root`，以建立聯絡 的參與`mycontact`。

```
{
    "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/*"
            ]
        }
    ]
}
```

Incident Manager 中的跨服務混淆代理人預防

混淆代理人問題是當沒有執行動作許可的實體呼叫更特權的實體來執行動作時，發生的資訊安全問題。這可能會允許惡意執行者執行命令或修改他們沒有執行或存取許可的資源。

在 中 AWS，跨服務模擬可能會導致混淆代理人案例。跨服務模擬是指一個服務 (呼叫的服務) 呼叫另一個服務 (呼叫的服務)。惡意執行者可以使用呼叫服務，使用他們通常沒有的許可來修改其他服務中的資源。

AWS 為服務主體提供 帳戶中資源的受管存取權，以協助您保護資源的安全。我們建議您在資源政策中使用 aws:SourceArn和 aws:SourceAccount全域條件內容金鑰。這些金鑰會限制為該資源 AWS Systems Manager Incident Manager 提供其他服務的許可。如果您同時使用兩個全域條件內容索引鍵，則aws:SourceAccount值中參考aws:SourceArn的值和帳戶在相同政策陳述式中使用時，必須使用相同的帳戶 ID。

的值aws:SourceArn必須是受影響事件記錄的 ARN。如果您不知道資源的完整 ARN，或要指定多個資源，請將aws:SourceArn全域內容條件索引鍵與*萬用字元用於 ARN 的未知部分。例如，您可以將 aws:SourceArn 設定為 arn:aws:ssm-incidents::*111122223333*:*。

在下列信任政策範例中，我們使用 aws:SourceArn條件金鑰，根據事件記錄的 ARN 限制對服務角色的存取。只有從回應計畫建立的事件記錄myresponseplan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 Incident Manager 使用服務連結角色

AWS Systems Manager Incident Manager use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Incident Manager 的唯一 IAM 角色類型。服務連結角色由 Incident Manager 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Incident Manager，因為您不必手動新增必要的許可。Incident Manager 會定義其服務連結角色的許可，除非另有定義，否則只有 Incident Manager 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 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。這可保護您的 Incident Manager 資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (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。

Incident Manager 的服務連結角色許可

Incident Manager 使用名為 AWSServiceRoleforIncidentManager 的服務連結角色。此角色允許 Incident Manager 代表您管理 Incident Manager 事件記錄和相關資源。

AWSServiceRoleforIncidentManager 服務連結角色信任下列服務擔任該角色：

- `ssm-incidents.amazonaws.com`

角色許可政策`AWSIncidentManagerServiceRolePolicy`允許 Incident Manager 對指定的資源完成下列動作：

- 動作：`ssm-incidents:ListIncidentRecords`在與動作相關的所有資源上。
- 動作：`ssm-incidents:CreateTimelineEvent`在與動作相關的所有資源上。
- 動作：`ssm:CreateOpsItem`在與動作相關的所有資源上。
- 動作：`all resources related to the action.` 上的 `ssm:AssociateOpsItemRelatedItem`
- 動作：在與動作相關的所有資源`ssm-contacts:StartEngagement`上。
- 動作：`cloudwatch:PutMetricData`在 `AWS/IncidentManager`和 `AWS/Usage` 命名空間內的 CloudWatch 指標上

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 Incident Manager 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 AWS Management Console、 AWS CLI或 AWS API 中建立複寫集時，Invent Manager 會為您建立服務連結角色。

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。當您建立複寫集時，Incident Manager 會再次為您建立服務連結角色。

編輯 Incident Manager 的服務連結角色

Incident Manager 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。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Incident Manager 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，您必須先刪除複寫集。刪除複寫集會刪除在 Incident Manager 中建立和存放的所有資料，包括回應計畫、聯絡人和呈報計畫。您也將遺失先前建立的所有事件。指向已刪除回應計劃的任何警示和 EventBridge 規則將不再建立警示或規則比對的事件。若要刪除複寫集，您必須刪除集合中的每個區域。

> **Note**
>
> 如果 Incident Manager 服務在您嘗試刪除資源時使用角色，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 AWSServiceRoleforIncidentManager 所使用的複寫集中的區域

1. 開啟 Incident Manager 主控台，然後從左側導覽中選擇設定。
2. 在複寫集中選取區域。
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，直到您刪除複寫集中的所有區域為止。刪除最終區域時，主控台會通知您刪除具有該區域的複寫集。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleforIncidentManager 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Incident Manager 服務連結角色支援的 區域

Incident Manager 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 的 受管政策 AWS Systems Manager Incident Manager

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 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 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管政策：AWSIncidentManagerIncidentAccessServiceRolePolicy

您可以將 `AWSIncidentManagerIncidentAccessServiceRolePolicy` 連接到 IAM 實體。Incident Manager 也會將此政策連接至 Incident Manager 角色，以允許 Incident Manager 代表您執行動作。

此政策授予唯讀許可，允許 Incident Manager 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問題清單。

許可詳細資訊

此政策包含以下許可。

- `cloudformation` – 允許主體描述 AWS CloudFormation 堆疊。這對於 Incident Manager 識別與事件相關的 CloudFormation 事件和資源是必要的。
- `codedeploy` – 允許主體讀取 AWS CodeDeploy 部署。此為 Incident Manager 識別與事件相關的 CodeDeploy 部署和目標的必要項目。
- `autoscaling` – 允許主體判斷 Amazon Elastic Compute Cloud (EC2) 執行個體是否為 Auto Scaling 群組的一部分。這是必要的，因此 Incident Manager 可以為屬於 Auto Scaling 群組的 EC2 執行個體提供調查結果。

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

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南AWSIncidentManagerIncidentAccessServiceRolePolicy》中的 。

AWS 受管政策：**AWSIncidentManagerServiceRolePolicy**

您不得將 `AWSIncidentManagerServiceRolePolicy` 連接到 IAM 實體。此政策會連接到服務連結角色，允許 Incident Manager 代表您執行動作。如需詳細資訊，請參閱針對 Incident Manager 使用服務連結角色。

此政策授予 Incident Manager 許可，以列出事件、建立時間軸事件、建立 OpsItems、將相關項目與 OpsItems 建立關聯、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` – 允許主體列出事件並建立時間軸事件。這是必要的，因此回應者可以在事件儀表板上的事件期間協同合作。
- `ssm` – 允許主體建立 OpsItems 並關聯相關項目。這是在事件開始時建立父 OpsItem 的必要項目。
- `ssm-contacts` – 允許主體開始業務開發。這對於 Incident Manager 在事件期間與聯絡人互動是必要的。
- `cloudwatch` – 允許主體發佈 CloudWatch 指標。這對於 Incident Manager 發佈與事件和用量指標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",
                        "AWS/Usage"
                    ]
                }
            }
        }
    ]
}
```

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南AWSIncidentManagerServiceRolePolicy》中的 。

AWS 受管政策： **AWSIncidentManagerResolverAccess**

您可以AWSIncidentManagerResolverAccess連接到 IAM 實體，以允許它們啟動、檢視和更新事件。這也可以讓他們在事件儀表板中建立客戶時間軸事件和相關項目。您也可以將此政策連接到聊天應用程式服務角色中的 Amazon Q Developer，或直接連接到與用於事件協作的任何聊天管道相關聯的客戶受管角色。若要進一步了解聊天應用程式中 Amazon Q Developer 中的 IAM 政策，請參閱《聊天應用程式管理員指南》中的在聊天應用程式中使用 Amazon Q Developer 管理執行命令的許可。

許可詳細資訊

此政策包含以下許可。

- ssm-incidents – 可讓您啟動事件、列出回應計畫、列出事件、更新事件、列出時間軸事件、建立自訂時間軸事件、更新自訂時間軸事件、刪除自訂時間軸事件、列出相關項目、建立相關項目，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": "*"
        }
    ]
}
```

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南AWSIncidentManagerResolverAccess》中的 。

AWS 受管政策的 Incident Manager 更新

檢視自此服務開始追蹤這些變更以來，有關 Incident Manager AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Incident Manager 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSIncidentManagerServiceRolePolicy – 政策更新	Incident Manager 新增了新的許可，允許 Incident Manager 將AWS/Usage 命名空間內的指標發佈至您的帳戶。	2025 年 1 月 27 日
AWSIncidentManagerIncidentAccessServiceRolePolicy – 政策更新	Incident Manager 已將新的許可新增至 AWSIncidentManagerIncidentAccessServiceRolePolicy ，以支援問題清單功能，以允許它檢查 EC2 執行個體是否屬於 Auto Scaling 群組。	2024 年 2 月 20 日
AWSIncidentManagerIncidentAccessServiceRolePolicy – 新政策	Incident Manager 新增了新的政策，授予 Incident Manager 在管理事件時呼叫其他 AWS 服務 的許可。	2023 年 11 月 17 日
AWSIncidentManagerServiceRolePolicy – 政策更新	Incident Manager 新增了允許 Incident Manager 將指標發佈至您帳戶的新許可。	2022 年 12 月 16 日
AWSIncidentManagerResolverAccess – 新政策	Incident Manager 新增了新的政策，可讓您啟動事件、列出回應計畫、列出事件、更新事件、列出時間軸事件、建立自訂時間軸事件、更新自訂時間軸事件、刪除自訂時間軸事	2021 年 4 月 26 日

變更	描述	日期
	件、列出相關項目、建立相關項目，以及更新相關項目。	
AWSIncidentManagerServiceRolePolicy – 新政策	Incident Manager 新增了新的政策，以授予 Incident Manager 列出事件、建立時間軸事件、建立 OpsItems、將相關項目與 OpsItems 建立關聯，以及開始與事件相關的互動的許可。	2021 年 4 月 26 日
Incident Manager 開始追蹤變更	Incident Manager 開始追蹤其 AWS 受管政策的變更。	2021 年 4 月 26 日

對 AWS Systems Manager Incident Manager 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Incident Manager 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 Incident Manager 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 Amazon Web Services 帳戶以外的人員存取我的 Incident Manager 資源

我無權在 Incident Manager 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。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 ssm-incidents:*GetWidget* 許可時發生。

```
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。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞給 Incident Manager。

有些 AWS 服務 可讓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 IAM `marymajor` 使用者嘗試使用主控台在 Incident Manager 中執行動作時，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 Incident Manager 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。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Incident Manager 是否支援這些功能，請參閱 AWS Systems Manager Incident Manager 如何使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

在 Incident Manager 中使用共用聯絡人和回應計劃

透過聯絡人分享，身為聯絡人擁有者，您可以與其他 AWS 帳戶 或組織內的 AWS 聯絡人資訊、呈報計畫和業務開發分享。

透過回應計劃共用，身為回應計劃擁有者，您可以與其他 AWS 帳戶 或 AWS 組織內的 共用回應計劃和相關事件。

聯絡人或回應計畫擁有者可以與下列人員共用聯絡人和回應計畫：

- 中的特定組織 AWS 帳戶 內部或外部 AWS Organizations
- 中組織內部的組織單位 AWS Organizations
- 其在 中的整個組織 AWS Organizations

目錄

- 共用聯絡人和回應計畫的先決條件
- 相關服務
- 共用聯絡或回應計畫
- 停止共用聯絡人或回應計劃
- 識別共用聯絡人或回應計劃
- 共用聯絡和回應計畫許可
- 計費和計量
- 執行個體限制

共用聯絡人和回應計畫的先決條件

若要與 中的組織或組織單位共用聯絡或回應計畫 AWS Organizations：

- 您必須在 中擁有 資源 AWS 帳戶。您無法共用已與您共用的聯絡或回應計畫。
- 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

聯絡和回應計劃共用與 AWS Resource Access Manager (AWS RAM) 整合。您可以透過 AWS RAM AWS 帳戶 或 與 共用您的 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 中的個別、 AWS 帳戶組織單位或整個組織 AWS Organizations。

如需 的詳細資訊 AWS RAM，請參閱AWS RAM 《 使用者指南》 。

共用聯絡或回應計畫

在您共用回應計劃之後，消費者可以存取使用該回應計劃建立的所有過去、目前和未來事件。

在您共用聯絡人後，消費者可以存取事件期間發生的聯絡資訊、參與計劃、呈報計劃和參與。消費者也可以在事件期間參與聯絡或呈報計畫。

如果您屬於 中的組織， AWS Organizations 且已啟用組織內的共用，則組織中的消費者會自動獲得共用聯絡人或回應計劃的存取權。否則，消費者會收到加入資源共享的邀請，並在接受邀請後獲得共用聯絡人或回應計劃的存取權。

您可以使用 AWS RAM 主控台或 來共用您擁有的聯絡或回應計畫 AWS CLI。

> **Note**
>
> 目前，不支援將另一個帳戶共用的聯絡人新增至回應計劃。

使用 AWS RAM 主控台共用您擁有的聯絡或回應計畫

請參閱《AWS RAM 使用者指南》中的建立資源共享。

使用 共享您擁有的聯絡或回應計畫 AWS CLI

使用 create-resource-share 命令。

停止共用聯絡人或回應計劃

當資源擁有者停止與消費者共用聯絡或回應計畫時，聯絡、回應計畫、呈報計畫、業務開發和事件將不再出現在消費者的主控台中。

> **Note**
>
> 如果消費者在主控台中檢視聯絡人、回應計畫、呈報計畫、業務開發或事件，則繼續查看這些聯絡人、回應計畫、呈報計畫、業務開發或事件，直到重新整理頁面或離開頁面為止。

若要停止共用您擁有的共用聯絡人或回應計劃，您必須將其從資源共用中移除。您可以使用 AWS RAM 主控台或 來執行此操作 AWS CLI。

使用主控台停止共用您擁有的 AWS RAM 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。

使用 停止共用您擁有的聯絡人或回應計劃 AWS CLI

使用 disassociate-resource-share 命令。

識別共用聯絡人或回應計劃

擁有者和消費者可以使用 Incident Manager 主控台和 來識別共用聯絡人和回應計劃 AWS CLI。

使用 Incident Manager 主控台識別共用聯絡人或回應計劃

> **Note**
>
> 聯絡人、回應計畫、呈報計畫、業務開發和事件通常無法識別為 Incident Manager 主控台中的共用資源。在顯示 Amazon Resource Name (ARN) 的地方，ARN 會包含擁有者的帳戶 ID。

使用 識別共用聯絡人或回應計劃 AWS CLI

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

共用聯絡和回應計畫許可

擁有者的許可

擁有者可以更新、檢視、共用、停止共用，以及使用聯絡人和回應計劃。聯絡和回應計畫包括相關的業務開發和事件。

消費者的許可

消費者只能使用和檢視回應計畫和聯絡人。聯絡和回應計畫包括相關的業務開發和事件。

計費和計量

資源的擁有者會支付資源的費用。消費者不需要為與他們共用的資源付費。共用資源不會產生額外的成本。

執行個體限制

共用資源不會影響擁有者或消費者帳戶中資源的限制。只有擁有者的帳戶會用來計算資源的限制。

的合規驗證 AWS Systems Manager Incident Manager

在多個合規計畫 AWS Systems Manager Incident Manager 中，第三方稽核人員會評估 的安全與 AWS 合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構 （包括國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 保護 AWS 服務和映射指南至安全控制的最佳實務。
- 《 AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。

- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

中的彈性 AWS Systems Manager Incident Manager

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體分隔和隔離的可用區域，這些可用區域以低延遲、高輸送量和高備援聯網連接。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 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

Incident Manager 是全球區域服務，目前不支援可用區域。

除了 AWS 全球基礎設施之外，Incident Manager 還提供數種功能，以協助支援您的資料彈性和備份需求。在準備精靈期間，系統會要求您設定複寫集。此區域複寫集可確保您的資料和資源可從多個區域存取，使得跨雲端網路的事件管理更加易於管理。此複寫也可確保您的資料在其中一個區域故障時安全且可存取。

如需使用 Incident Manager 複寫集的詳細資訊，請參閱 設定 Incident Manager 複寫集。

中的基礎設施安全 AWS Systems Manager Incident Manager

作為受管服務， AWS Systems Manager Incident Manager 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Incident Manager。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。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 主體相關聯的私密存取金鑰來簽署。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 和界面 VPC 端點 (AWS PrivateLink)

您可以在 VPC 和 之間建立私有連線， AWS Systems Manager Incident Manager 方法是建立界面 VPC 端點。界面端點是採用 AWS PrivateLink技術。透過 AWS PrivateLink，您可以私下存取 Incident Manager API 操作，無需網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址，即可與 Incident Manager API 操作通訊。VPC 和 Incident Manager 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》中的界面 VPC 端點 (AWS PrivateLink)。

Incident Manager VPC 端點的考量事項

在您設定 Incident Manager 的介面 VPC 端點之前，請務必檢閱《Amazon VPC 使用者指南》中的介面端點屬性和限制和AWS PrivateLink 配額。

Incident Manager 支援從您的 VPC 呼叫其所有 API 動作。若要使用所有 Incident Manager，您必須建立兩個 VPC 端點：一個用於 `ssm-incidents`，另一個用於 `ssm-contacts`。

為 Incident Manager 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Incident Manager 建立 VPC 端點AWS CLI。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用您 中 Incident Manager 支援的服務名稱，為 Incident Manager 建立 VPC 端點 AWS 區域。下列範例顯示 IPv4 和雙堆疊端點的介面端點格式。

IPv4 端點格式

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

雙堆疊 (IPv4 和 IPv6) 端點格式

- `aws.api.region.ssm-incidents`

- aws.api.*region*.ssm-contacts

如需所有 區域的支援端點清單，請參閱《 AWS 一般參考指南》中的 AWS Systems Manager Incident Manager 端點和配額。

如果您為介面端點啟用私有 DNS，您可以使用其格式的預設區域 DNS 名稱向 Incident Manager 提出 API 請求。下列範例顯示預設的區域 DNS 名稱格式。

- ssm-incidents.*region*.amazonaws.com
- ssm-contacts.*region*.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 Incident Manager 建立 VPC 端點政策

您可以將端點政策連接至控制 Incident Manager 存取的 VPC 端點。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：適用於 Incident Manager 動作的 VPC 端點政策

以下是 Incident Manager 的端點政策範例。連接至端點時，此政策會授予所有資源上所有主體所列出的 Incident Manager 動作的存取權。

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

```
            "Resource":"*"
        }
    ]
}
```

Incident Manager 中的組態和漏洞分析

組態和 IT 控制是客戶 AWS 與您之間的共同責任。如需詳細資訊，請參閱 AWS 共同的責任模型。

中的安全最佳實務 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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

- Incident Manager 的預防性安全最佳實務
- Incident Manager 的 Detective 安全最佳實務

Incident Manager 的預防性安全最佳實務

實作最低權限存取

授予許可時，您可以決定誰要取得哪些 Incident Manager 資源的許可。您還需針對這些資源啟用允許執行的動作，因此， 只會授予執行任務所需的許可。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 實體的政策和許可界限控制對 AWS 資源的存取 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html
- 服務控制政策

建立和管理聯絡人

啟用聯絡人時，Incident Manager 會聯絡裝置以確認啟用。在啟用裝置之前，請確定裝置資訊正確無誤。這可減少 Incident Manager 在啟用期間聯絡錯誤裝置或人員的可能性。

定期檢閱您的聯絡人和呈報計劃，以確保只聯絡在事件期間需要聯絡的聯絡人。定期檢閱聯絡人以移除過時或不正確的資訊。如果事件發生時不應再通知聯絡人，請從相關的呈報計畫中移除聯絡人，或從 Incident Manager 中移除聯絡人。

將聊天頻道設為私有

您可以將事件聊天頻道設為私有，以實作最低權限存取。請考慮使用不同的聊天頻道，並為每個回應計畫範本提供縮小範圍的使用者清單。這可確保只會將正確的回應者提取至可能包含敏感資訊的聊天頻道。

Slack 在聊天應用程式中在 Amazon Q Developer 中建立的頻道會繼承用於在聊天應用程式中設定 Amazon Q Developer 的 IAM 角色許可。這可讓已啟用聊天應用程式的Slack頻道中 Amazon Q Developer 中的回應者呼叫任何允許列出的動作，例如 Incident Manager APIs 和擷取指標圖表。

將 AWS 工具保持在最新狀態

AWS 會定期發行您可以在 AWS 操作中使用的工具和外掛程式的更新版本。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) 是一種開放原始碼工具，可讓您使用命令列 shell 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。如需安裝命令的相關資訊，請參閱《 AWS 命令列界面使用者指南》中的安裝AWS 命令列界面。
- AWS Tools for Windows PowerShell – Tools for Windows PowerShell 是一組 PowerShell 模組，建置在適用於 .NET 的 AWS SDK 公開的功能上。適用於 Windows PowerShell 的工具可讓您從 PowerShell 命令列編寫 AWS 資源操作的指令碼。當 Tools for Windows PowerShell 的版本更新發佈時，您應定期更新於本機執行的版本。如需詳細資訊，請參閱在 Windows AWS Tools for Windows PowerShell 上更新 或在 Linux 或 macOS AWS Tools for Windows PowerShell 上更新 。

相關內容

Systems Manager 的安全最佳實務

Incident Manager 的 Detective 安全最佳實務

識別和稽核所有 Incident Manager 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，並對潛在弱點領域採取行動。為您的 Incident Manager 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 提供由使用者、角色或 Incident Manager 中的 AWS 服務所採取之動作的記錄。您可以使用 所收集的資訊 AWS CloudTrail，判斷向 Incident Manager 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，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 Trusted Advisor 中發佈的安全建議 AWS 帳戶。您也可以使用 describe-trusted-advisor-checks，以程式設計方式來執行此操作。

此外，請主動監控向每個 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絡，以了解可能會影響您的新安全問題。

AWS 具有廣泛影響的操作問題會張貼在AWS 服務運作狀態儀表板上。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 資源 AWS 時遵循安全最佳實務 (AWS 安全部落格)

IAM 最佳實務

中的安全最佳實務 AWS CloudTrail

在 Incident Manager 中監控

AWS Systems Manager Incident Manager 與下列 服務整合，提供監控和記錄功能：

CloudWatch 指標

使用 CloudWatch 指標擷取 AWS Systems Manager Incident Manager 操作資料點的統計資料，做為一組有序的時間序列資料，稱為指標。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，請參閱使用 Amazon CloudWatch 在 Incident Manager 中監控指標。

CloudTrail日誌

使用 AWS CloudTrail 擷取對 AWS APIs發出的呼叫詳細資訊。您可以在 Amazon Simple Storage Service 中將這些呼叫儲存為日誌檔案。您可以使用這些 CloudTrail 日誌來判斷進行了哪些呼叫、呼叫的來源 IP 地址、進行呼叫的人員以及進行呼叫的時間等資訊。CloudTrail 日誌包含有關針對 Incident Manager 呼叫 API 動作的資訊。IFor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，以提高效能、可靠性、安全性和成本效益。所有使用者皆可使用四個 Trusted Advisor 檢查；具有商業或企業支援計劃的使用者可使用超過 50 個檢查。對於 Incident Manager， 會 Trusted Advisor 檢查複寫集的組態是否使用多個 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 支援 使用者指南》中的 AWS Trusted Advisor。

使用 Amazon CloudWatch 在 Incident Manager 中監控指標

Incident Manager 提供您可以在 Amazon CloudWatch 中監控的彙總指標。您可以使用這些指標來識別事件和回應計畫趨勢。

這些指標包括：

- 在指定期間內建立的事件數量
- 回應和解決這些事件的時間
- 已解決的事件數量

您可以監控 Incident Manager 指標，以進一步了解您的營運運作狀態，並採取有意義的動作來推動事件回應的卓越營運。Incident Manager 指標適用於所有 Incident Manager 區域。您的指標將可在

Amazon CloudWatch 中檢視您在加入 Incident Manager 時在複寫集中指定的所有區域。您可以在事件採取動作的區域中檢視已發佈的指標。這些指標不收取額外費用。

在 CloudWatch 主控台上，您可以使用這些指標建置儀表板，以：

- 測量和檢閱您現有的事件負載
- 追蹤您的事件負載是否增加、減少或保持不變
- 更有效地使用 Incident Manager 來減少事件的頻率、持續時間和影響

此頁面說明 CloudWatch 主控台上可用的 Incident Manager 指標。

> **Important**
>
> 對於客戶產生的事件，如果 中的來源值`TriggerDetails`是使用非 ASCII 字元命名，則事件的指標將不會在 Amazon CloudWatch 指標中報告，而 不支援非 ASCII 文字。 `source` 只能以程式設計方式提供，例如使用 SDK 或 AWS CLI。

Incident Manager 會將下列指標傳送至 CloudWatch。

指標	描述
`NumberOfCreateIncidents`	建立的事件數量。 有效維度：【】（空維度）、【ResponseP lan 】、【Impact】、【Source】、【】、【ResponsePlan 、Impact】、【ResponseP lan 、Source】 單位：計數
`NumberOfResolveIncidents`	已解決的事件數量。 有效維度：【】（空維度）、【ResponseP lan 】、【Impact】、【Source】、【】、【ResponsePlan 、Impact】、【ResponseP lan 、Source】 單位：計數

指標	描述
TimeToFirstAcknowledgement	事件建立時間與第一次確認事件的時間差異。 有效維度：【】（空維度）、【ResponsePlan 】、【Impact】、【Source】、【】、【ResponsePlan 、Impact】、【ResponsePlan 、Source】 單位：秒
TimeToResolveIncident	事件建立和解決的時間差。 有效維度：】（空維度）、【ResponsePlan 】、【Impact】、【Source】、【】、【ResponsePlan 、Impact】、【ResponsePlan 、Source】 單位：秒

在 CloudWatch 主控台上檢視 Incident Manager 指標

在 CloudWatch 主控台中檢視 Incident Manager 指標

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇指標。
3. 选择 IncidentManager 命名空间。
4. 在指標索引標籤上，選擇維度，然後選擇指標。

如需使用 CloudWatch 指標的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的下列主題：

- 指標
- 使用 Amazon CloudWatch 指標

指標的維度

Incident Manager 指標使用 IncidentManager 命名空間，並提供下列維度的指標（以下維度）：

維度	描述
By Response Plan	依回應計劃檢視彙總指標。
By Impact Level	依嚴重性層級檢視彙總指標。
By Source	檢視由 CloudWatch 警示或 EventBridge 事件手動建立之事件的指標。
Across All Incidents	檢視目前 AWS 區域中所有事件的彙總指標。
Response Plan name and Source	檢視每個回應計劃和來源組合的彙總指標。
Response Plan Name and Impact Level	檢視每個回應計劃組合的彙總指標和嚴重性等級。

使用 記錄 AWS Systems Manager Incident Manager API 呼叫 AWS CloudTrail

AWS Systems Manager Incident Manager 已與 整合AWS CloudTrail，此服務提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 Incident Manager 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Incident Manager 主控台的呼叫，以及對 Incident Manager API 操作的程式碼呼叫。使用 CloudTrail 收集的資訊，您可以判斷對 Incident Manager 提出的請求、提出請求的 IP 地址、提出時間，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 Identity Center 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。

當您建立帳戶 AWS 帳戶 時CloudTrail 會在 中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、可搜尋、可下載且不可變的記錄。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄不會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立追蹤或 CloudTrail Lake 事件資料存放區。

CloudTrail 追蹤

線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有線索 AWS Management Console 都是多區域。您可以使用 AWS CLI建立單一或多區域追蹤。建議您建立多區域追蹤，因為您擷取 AWS 區域 帳戶中所有 的活動。如果您建立單一區域追蹤，您只能檢視追蹤 AWS 區域中記錄的事件。如需追蹤的詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的為您的 AWS 帳戶建立追蹤和為組織建立追蹤。

您可以透過建立追蹤，免費將持續管理事件的一個複本從 CloudTrail 傳遞至您的 Amazon S3 儲存貯體，但這樣做會產生 Amazon S3 儲存費用。如需 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 Lake 事件資料存放區

CloudTrail Lake 讓您能夠對事件執行 SQL 型查詢。CloudTrail Lake 會將分列式 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。如需 CloudTrail Lake 的詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 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 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

CloudTrail 中的 Incident Manager 管理事件

管理事件提供在 資源上執行的管理操作的相關資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

AWS Systems Manager Incident Manager 會將所有 Incident Manager 控制平面操作記錄為管理事件。如需 Incident Manager 記錄到 CloudTrail 的 AWS Systems Manager Incident Manager 控制平面操作清單，請參閱 AWS Systems Manager Incident Manager API 參考。

Incident Manager 事件範例

一個事件代表任何來源提出的單一請求，並包含請求 API 操作的相關資訊、操作的日期和時間、請求參數等。CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

以下範例顯示的是展示 `StartIncident` 動作的 CloudTrail 日誌項目。


```
{
    "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"
}
```

以下範例顯示的是展示 DeleteContactChannel 動作的 CloudTrail 日誌項目。

```
{
    "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"
}
```

如需有關 CloudTrail 記錄內容的資訊，請參閱《AWS CloudTrail 使用者指南》中的 CloudTrail record contents。

與 Incident Manager 的產品和服務整合

Incident Manager 是 中的工具 AWS Systems Manager，可與下列產品、服務和工具整合。

與 整合 AWS 服務

Incident Manager 會與下表所述的 AWS 服務 和 工具整合。

AWS CDK	AWS CDK 是使用程式碼來定義雲端基礎設施和使用 AWS CloudFormation 進行佈建的開發架構。 AWS CDK 支援多種程式設計語言，包括 TypeScript、JavaScript、Java、 Python和 C#/。淨額。 如需 AWS CDK 搭配 Incident Manager 使用 的相關資訊，請參閱 AWS CDK API 參考中的下列章節： • @aws-cdk/aws-ssmincidents 模組 • @aws-cdk/aws-ssmcontacts 模組
聊天應用程式中的 Amazon Q 開發人員	聊天應用程式中的 Amazon Q Developer 可讓 DevOps 和軟體開發團隊使用訊息程式聊天室來監控和回應其中的操作事件 AWS 雲端。 在具有 Incident Manager 的聊天應用程式中使用 Amazon Q Developer，您可以建立聊天管道，回應者可以使用這些管道來監控和回應事件。聊天應用程式中的 Amazon Q Developer 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，您也可以在 Amazon Simple Notification Service (Amazon SNS) 中建立主題。Amazon SNS 是一項受管服務，提供從發佈者到訂閱者的訊息傳遞。在事件回應計劃中，當您將已建立的聊天頻道與計劃建立關聯

	時，您也可以選擇與聊天頻道相關聯的一或多個主題。這些 SNS 主題用於將有關事件的通知傳送給事件回應者。 如需詳細資訊，請參閱在 Incident Manager 中為回應者建立和整合聊天頻道。
AWS CloudFormation	AWS CloudFormation 是一項服務，可用來建立範本，其中包含應用程式所需的所有資源，然後為您設定和佈建資源。它也會設定所有相依性，因此您可以更專注於應用程式，較少專注於管理資源。 如需 AWS CloudFormation 搭配 Incident Manager 使用 的相關資訊，請參閱 AWS CloudFormation 使用者指南中的下列主題： • Incident Manager 資源類型參考 • 聯絡資源類型參考資源類型參考
Amazon CloudWatch	CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以使用 CloudWatch 收集和追蹤指標，這些是您可以為您的資源和應用程式測量的變數。 您可以設定 CloudWatch 警示以在 Incident Manager 中建立事件。CloudWatch 會與 Systems Manager 和 Incident Manager 搭配使用，從回應計劃範本建立事件。 如需詳細資訊，請參閱使用 CloudWatch 警示自動建立事件。

Amazon Chime	Amazon Chime 是結合會議、聊天和商業通話的線上工作場所。您可以使用 Amazon Chime 在組織內外開會、聊天和撥打業務電話。 您可以在聊天應用程式中為 Amazon Q Developer 中建立 Amazon Chime 的聊天頻道，然後將該頻道新增至回應計劃，將 Amazon Chime 會議室整合到您的 Incident Manager 操作中。 如需詳細資訊，請參閱在 Incident Manager 中為回應者建立和整合聊天頻道。
Amazon EventBridge	EventBridge 是一種無伺服器服務，使用事件來連接應用程式元件，讓您更輕鬆地建置可擴展的事件驅動型應用程式。 您可以設定 EventBridge 規則來監控 AWS 資源中的事件模式，並在事件符合您定義的模式時，在 Incident Manager 中建立事件。您的規則可以監控數十個 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，請參閱使用 EventBridge 事件自動建立事件。
AWS Secrets Manager	Secrets Manager 可協助您管理、擷取和輪換資料庫憑證、應用程式憑證、OAuth 權杖、API 金鑰，以及在其生命週期內的其他秘密。 當您將 Incident Manager 與 PagerDuty 服務整合時，您可以在 Secrets Manager 中建立包含 PagerDuty 登入資料的秘密。 如需詳細資訊，請參閱將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中。

AWS Systems Manager	Systems Manager 是一個操作中樞，可用來檢視和控制您的應用程式基礎設施，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 工具會直接與 Incident Manager 整合： • 自動化 – Automation Runbook 會定義 Systems Manager 對 AWS 資源執行的動作。在 Incident Manager 中，執行手冊會定義一系列自動和手動步驟，用於解決您的事件。 如需建立 Automation Runbook 以搭配 Incident Manager 使用的詳細資訊，請參閱將 Systems Manager Automation Runbook 整合在 Incident Manager 中以修復事件。 • OpsCenter – OpsCenter 提供集中位置，讓營運工程師和 IT 專業人員可以管理與 AWS 資源相關的營運工作項目，稱為 OpsItems。您可以直接從事件後分析建立 OpsItems，以追蹤相關工作。 如需詳細資訊，請參閱在 Incident Manager 中執行事件後分析。
AWS Trusted Advisor	Trusted Advisor 是一項工具，可供具有基本或開發人員支援計劃 AWS 的客戶使用。 會 Trusted Advisor 檢查您的 AWS 環境，然後在存在節省成本、改善系統可用性和效能的機會時提出建議，或協助解決安全漏洞。 對於 Incident Manager， 會 Trusted Advisor 檢查複寫集的組態是否使用多個 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

您可以整合或使用 Incident Manager 與下表所述的第三方服務。

Jira Cloud	使用 AWS Service Management Connector，您可以將 Incident Manager 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 Incident Manager 中建立新的事件時，整合也會在 Jira Cloud 中建立事件。如果您在 Incident Manager 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 Incident Manager 或 Jira Cloud 中解決事件，整合會根據您設定的偏好設定來解決這兩個服務中的事件。 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)。
Jira 服務管理	您可以使用 AWS Service Management Connector將 Incident Manager 與第三方雲端工作流程平台 Jira Service Management 整合。 設定與 Jira Service Management 的整合後，當您在 Incident Manager 中建立新的事件時，整合也會在 Jira Service Management 中建立事件。如果您在 Incident Manager 中更新事件，則會在 Jira Service Management 中對對應的事件進行這些更新。如果您在 Incident Manager 或 Jira Service Management 中解決事件，整合會根據您設定的偏好設定來解決這兩個服務中的事件。 如需詳細資訊，請參閱 AWS Service Management Connector 管理員指南中的設定 Jira Service Management。
Microsoft Teams	Microsoft Teams 提供協作雲端工具，用於團隊傳訊、音訊和視訊會議，以及檔案共用。

	您可以在聊天應用程式中為 Amazon Q Developer Microsoft Team 建立聊天頻道，然後將該頻道新增至回應計劃，藉此將頻道整合Microsoft Teams到您的 Incident Manager 操作中。 https://docs.aws.amazon.com/chatbot/latest/adminguide/ 如需詳細資訊，請參閱在 Incident Manager 中為回應者建立和整合聊天頻道。
PagerDuty	PagerDuty 是一種事件回應工具，支援分頁工作流程和升級政策。 當您將 Incident Manager 與 PagerDuty 整合時，您可以將 PagerDuty 服務新增至您的回應計劃。之後，每當在 Incident Manager 中建立事件時，就會在 PagerDuty 中建立對應的事件。PagerDuty 中的事件會使用您在其中定義的分頁工作流程和升級政策，以及 Incident Manager 中的政策。PagerDuty 會將來自 Incident Manager 的時間軸事件附加為事件上的備註。 若要將 Incident Manager 與 PagerDuty 整合，您必須先在 中 AWS Secrets Manager 建立包含 PagerDuty 登入資料的秘密。 如需有關在 中將 PagerDuty REST API 金鑰和其他必要詳細資訊新增至秘密的資訊 AWS Secrets Manager，請參閱 將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中。 如需有關將 PagerDuty 服務從您的 PagerDuty 帳戶新增至 Incident Manager 中的回應計劃的資訊，請參閱主題 中將 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 Incident Manager 與第三方雲端工作流程平台 ServiceNow 整合。 在您設定與 ServiceNow 的整合後，當您在 Incident Manager 中建立新的事件時，整合也會在 ServiceNow 中建立事件。如果您在 Incident Manager 中更新事件，它會對 ServiceNow 中的對應事件進行這些更新。如果您在 Incident Manager 或 ServiceNow 中解決事件，整合會根據您設定的偏好設定來解決這兩個服務中的事件。 如需詳細資訊，請參閱 AWS Service Management Connector 管理員指南中的在 ServiceNow AWS Systems Manager Incident Manager 中整合。
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。 您可以在聊天應用程式中為 Amazon Q Developer Slack 建立聊天頻道，然後將該頻道新增至回應計劃，藉此將頻道整合Slack到您的 Incident Manager 操作中。 https://docs.aws.amazon.com/chatbot/latest/adminguide/ 如需詳細資訊，請參閱在 Incident Manager 中為回應者建立和整合聊天頻道。

Terraform	HashiCorp Terraform 是一種開放原始碼基礎設施即程式碼 (IaC) 軟體工具，可提供命令列介面 (CLI) 工作流程來管理各種雲端服務。對於 Incident Manager，您可以使用 Terraform 來管理或佈建下列項目： SSM Incident Manager 聯絡 資源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation SSM Contacts 資料來源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation SSM Incident Manager 資源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM Incident Manager 資料來源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中

開啟與回應計劃的 PagerDuty 整合後，Inventist Manager 會以下列方式使用 PagerDuty：

- 當您在 Incident Manager 中建立新事件時，Invent Manager 會在 PagerDuty 中建立對應的事件。

- 您在 PagerDuty 中建立的分頁工作流程和升級政策會用於 PagerDuty 環境。不過，Inventation Manager 不會匯入您的 PagerDuty 組態。
- Incident Manager 會將時間軸事件作為備註發佈至 PagerDuty 中的事件，最多 2，000 個備註。
- 當您在 Incident Manager 中解決相關事件時，您可以選擇自動解析 PagerDuty 事件。

若要將 Incident Manager 與 PagerDuty 整合，您必須先在 中建立包含 PagerDuty AWS Secrets Manager 登入資料的秘密。這些允許 Incident Manager 與您的 PagerDuty 服務通訊。然後，您可以在 Incident Manager 中建立的回應計劃中包含 PagerDuty 服務。

您在 Secrets Manager 中建立的此秘密必須包含適當的 JSON 格式如下：

- 來自您 PagerDuty 帳戶的 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。
- 來自您 PagerDuty 子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到相同的服務區域。

先決條件

在 Secrets Manager 中建立秘密之前，請確定您符合下列要求。

KMS 金鑰

您必須使用您在 AWS Key Management Service () 中建立的客戶受管金鑰來加密您建立的秘密 AWS KMS。當您建立存放您 PagerDuty 登入資料的秘密時，請指定此金鑰。

> **Important**
>
> Secrets Manager 提供使用 加密秘密的選項 AWS 受管金鑰，但不支援此加密模式。

客戶受管金鑰必須符合下列要求：

- 金鑰類型：選擇對稱。
- 金鑰用量：選擇加密和解密。

- 區域性：如果您想要將回應計劃複寫至多個 AWS 區域，請確定您選取多區域金鑰。

金鑰政策

設定回應計劃的使用者必須擁有金鑰資源型政策kms:Decrypt中 kms:GenerateDataKey和 的許可。ssm-incidents.amazonaws.com 服務主體必須擁有金鑰資源型政策kms:Decrypt中 kms:GenerateDataKey和 的許可。

下列政策示範這些許可。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": "*"
        }
    ]
}
```

如需有關建立新的客戶受管金鑰的資訊，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 金鑰的詳細資訊，請參閱 AWS KMS 概念。

如果現有的客戶受管金鑰符合所有先前的要求，您可以編輯其政策來新增這些許可。如需有關更新客戶受管金鑰中政策的資訊，請參閱《 AWS Key Management Service 開發人員指南》中的變更金鑰政策。

> **Tip**
>
> 您可以指定條件金鑰，進一步限制存取。例如，下列政策僅允許透過美國東部 （俄亥俄） 區域 (us-east-2) 的 Secrets Manager 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` 許可

建立回應計劃的 IAM 身分 （使用者、角色或群組） 必須具有 IAM 許可 `secretsmanager:GetSecretValue`。

在 AWS Secrets Manager 秘密中存放 PagerDuty 存取憑證

1. 請遵循 AWS Secrets Manager 使用者指南中建立 AWS Secrets Manager 秘密中的步驟 3a。
2. 對於步驟 3b，對於鍵/值對，請執行下列動作：
   - 選擇純文字索引標籤。
   - 將方塊的預設內容取代為下列 JSON 結構：

```
{
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
}
```

   - 在您貼上的 JSON 範例中，取代*#####*，如下所示：
     - *pagerduty-token*：從您的 PagerDuty 帳戶取得的一般存取 REST API 金鑰或使用者權杖 REST API 金鑰的值。

       如需相關資訊，請參閱 PagerDuty 知識庫中的 API 存取金鑰。
     - *pagerduty-region*：託管 PagerDuty 子網域的 PagerDuty 資料中心的服務區域。

       如需相關資訊，請參閱 PagerDuty 知識庫中的服務區域。
     - *pagerduty-email*：屬於您 PagerDuty 子網域之使用者的有效電子郵件地址。

       如需相關資訊，請參閱 PagerDuty 知識庫中的管理使用者。

     下列範例顯示已完成的 JSON 秘密，其中包含必要的 PagerDuty 登入資料：

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. 在步驟 3c 中，針對加密金鑰，選擇您建立的客戶受管金鑰，其符合先前先決條件章節中列出的要求。
4. 在步驟 4c 中，針對資源許可執行下列動作：
   - 展開資源許可。

- 選擇編輯許可。
- 將政策方塊的預設內容取代為下列 JSON 結構：

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- 選擇 Save (儲存)。

5. 在步驟 4d 中，對於複寫秘密，如果您將回應計劃複寫到多個回應計劃，請執行下列動作 AWS 區域：
   - 展開複寫秘密。
   - 針對 AWS 區域，選取您複寫回應計劃的區域。
   - 針對加密金鑰，選擇您在此區域中建立或複寫的客戶受管金鑰，以符合先決條件區段下列出的要求。
   - 針對每個額外的項目 AWS 區域，選擇新增區域，然後選取區域名稱和客戶受管金鑰。
6. 完成 AWS Secrets Manager 使用者指南中建立 AWS Secrets Manager 秘密中的其餘步驟。

如需有關如何將 PagerDuty 服務新增至 Incident Manager 事件工作流程的資訊，請參閱主題 中的將 PagerDuty 服務整合到回應計劃中建立回應計劃。

相關資訊

如何使用 PagerDuty 和（操作和遷移部落格） 自動化事件回應 AWS Systems Manager Incident ManagerAWS 雲端

AWS Secrets Manager 使用者指南中的 中的秘密加密 AWS Secrets Manager

Systems AWS Manager Incident Manager 故障診斷

如果您在使用 AWS Systems Manager Incident Manager 時遇到問題，您可以根據我們的最佳實務使用下列資訊來解決這些問題。如果您遇到的問題超出下列資訊的範圍，或在您嘗試解決這些問題後仍持續存在，請聯絡 AWS 支援。

主題

- 錯誤訊息： ValidationException – We were unable to validate the AWS Secrets Manager secret
- 其他疑難排解問題

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 （使用者、角色或群組）沒有 IAM `secretsmanager:GetSecretValue` 許可。IAM 身分必須具有此許可，才能驗證 Secrets Manager 秘密。

- 解決方案：將缺少的`secretsmanager:GetSecretValue`許可新增至建立回應計劃的 IAM 身分的 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） 或新增 IAM 政策 (AWS CLI)。

問題 2：秘密未連接資源型政策，允許 IAM 身分執行`GetSecretValue`動作，或資源型政策拒絕身分的許可。

- 解決方案：建立陳述式或將`Allow`陳述式新增至秘密的資源型政策，以授予 IAM 身分`secrets:GetSecretValue`的 許可。或者，如果您使用的`Deny`陳述式包含 IAM 身分，請更新政策，讓身分可以執行動作。如需詳細資訊，請參閱AWS Secrets Manager 《 使用者指南》中的將許可政策連接至 AWS Secrets Manager 秘密。

問題 3：秘密未連接資源型政策，允許存取 Incident Manager 服務主體 `ssm-incidents.amazonaws.com`。

- 解決方案：建立或更新秘密的資源型政策，並包含下列許可：

```
{
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

問題 4： AWS KMS key 選取要加密秘密的 不是客戶受管金鑰，或選取的客戶受管金鑰未提供 IAM 許可`kms:Decrypt`和`kms:GenerateDataKey*` Incident Manager 服務主體。或者，建立回應計畫的 IAM 身分可能沒有 IAM 許可 `GetSecretValue`。

- 解決方案：確保您符合主題 中先決條件中所述的要求將 PagerDuty 存取憑證存放在 AWS Secrets Manager 秘密中。

問題 5：包含一般存取 REST API 金鑰或使用者權杖 REST API 金鑰的秘密 ID 無效。

- 解決方案：確保您準確輸入 Secrets Manager 秘密的 ID，沒有尾端空格。您必須在存放要使用之秘密 AWS 區域 的相同 中工作。您無法使用已刪除的秘密。

問題 6：在極少數情況下，Secrets Manager 服務可能會遇到問題，或者 Incident Manager 可能無法與其通訊。

- 解決方案：等待幾分鐘，然後再試一次。檢查 AWS Health Dashboard 是否有任何可能影響任一服務的問題。

其他疑難排解問題

如果上述步驟無法解決您的問題，您可以從下列資源找到其他協助：

- 如需存取 Incident Manager 主控台時 Incident Manager 特有的 IAM 問題，請參閱對 AWS Systems Manager Incident Manager 身分和存取進行故障診斷。
- 如需存取 時的一般身分驗證和授權問題 AWS Management Console，請參閱《IAM 使用者指南》中的對 IAM 進行故障診斷

Incident Manager 的文件歷史記錄

變更	描述	日期
變更手動建立事件的許可要求	使用者手動建立事件所需的 IAM 許可已變更，不再使用服務連結角色。Incident Manager 現在會使用轉送存取工作階段 (FAS) `ssm-contacts:StartEngagement` 做為 的一部分呼叫 `ssm-incidents:StartIncident` 。如需詳細資訊，請參閱手動啟動事件所需的 IAM 許可。	2025 年 6 月 10 日
受管政策的更新 AWSServiceRoleforIncidentManagerPolicy	Incident Manager 已將新的許可新增至 `AWSServiceRoleforIncidentManagerPolicy` ，允許 Incident Manager 將`AWS/Usage` 命名空間內的指標發佈至您的帳戶。如需詳細資訊，請參閱 Incident Manager 對 AWS 受管政策的更新。	2025 年 1 月 28 日
受管政策的更新 AWSIncidentManagerIncidentAccessServiceRolePolicy	Incident Manager 已將新的許可新增至 `AWSIncidentManagerIncidentAccessServiceRolePolicy` ，以支援問題清單功能，以允許它檢查 EC2 執行個體是否為 Auto Scaling 群組的一部分。如需詳細資訊，請參閱 Incident Manager 對 AWS 受管政策的更新。	2024 年 2 月 20 日

其他 HashiCorp Terraform 支援：待命輪換	Terraform 已新增至對 Incident Manager 的支援。您現在可以使用 Terraform 佈建或管理 Incident Manager 待命資源。如需有關此 和其他第三方與 Incident Manager 整合的資訊，請參閱與其他 產品和服務整合。	2024 年 2 月 2 日

新功能：其他 的調查結果 AWS 服務	問題清單可提供您在 Incident Manager 中建立事件時，大約同時發生之 AWS CloudFormation 堆疊和 AWS CodeDeploy 部署相關變更的相關資訊。在 Incident Manager 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 CodeDeploy 主控台的連結，以取得變更的完整詳細資訊。調查結果可減少評估事件潛在原因所需的時間。它們也會降低回應者存取錯誤帳戶或主控台以調查事件原因的機會。此功能也會引進新的 受管政策 `AWSIncidentManagerIncidentAccessServiceRolePolicy` ，這可讓 Incident Manager 讀取其他 中的資源 AWS 服務 ，以識別與事件相關的問題清單。如需詳細資訊，請參閱下列主題： • 使用問題清單 • AWS 受管政策：AWSIncidentManagerIncidentAccessServiceRolePolicy	2023 年 11 月 15 日
已更新與 Incident Manager 整合的清單	與 Incident Manager 的產品和服務整合主題已擴展，以列出並描述所有 AWS 服務 和第三方工具，您可以將這些工具與 Incident Manager 整合到您的事件偵測和回應操作中。	2023 年 6 月 9 日

與 整合 AWS Trusted Advisor	Trusted Advisor 現在會檢查複寫集的組態是否使用多個 AWS 區域 來支援區域容錯移轉和回應。對於 CloudWatch 警示或 EventBridge 事件建立的事件，Invent Manager 會在 AWS 區域 與警示或事件規則相同的 中建立事件。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。為了協助避免這種情況， 只會針對一個區域設定複寫集時 Trusted Advisor 報告 。如需使用 的詳細資訊 Trusted Advisor，請參閱AWS 支援 《 使用者指南AWS Trusted Advisor》中的 。	2023 年 4 月 28 日

在回應計畫中使用 Microsoft Teams做為聊天頻道	透過與聊天應用程式中的Microsoft Teams和 Amazon Q Developer 整合，您現在可以將 Microsoft Teams 用於回應計劃中的聊天頻道。這是對Slack和 Amazon Chime 聊天頻道的支援。在事件期間，Incident Manager 會直接將狀態通知傳送至聊天頻道，讓所有回應者隨時收到通知。回應者也可以在Microsoft Teams應用程式中互相通訊和與事件相關的AWS CLI 命令，以更新並與事件互動。如需詳細資訊，請參閱 Incident Manager 中的使用聊天頻道。	2023 年 4 月 4 日
新功能：待命排程	Incident Manager 中的待命排程會定義發生需要操作員介入的事件時，誰會收到通知。隨需排程包含您為排程建立的一或多個輪換。每次輪換最多可包含 30 個聯絡人。建立隨需排程之後，您可以將其做為呈報計畫中的呈報。當與該呈報計畫相關聯的事件發生時，Incident Manager 會根據排程通知正在呼叫的操作員（或操作員）。如需詳細資訊，請參閱 Incident Manager 中的使用待命排程。	2023 年 3 月 28 日

列印格式化的事件分析或儲存為 PDF	事件分析頁面現在包含列印按鈕，可產生用於列印的分析版本。使用為您的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： Incident Manager 現在會將事件時間軸事件複製到 PagerDuty 事件	當您在回應計畫中開啟與 PagerDuty 的整合時，Incident Manager 會將從該計畫建立的時間軸事件新增至 PagerDuty 中對應的事件記錄。PagerDuty 會將時間軸事件新增為事件上的備註，最多 2，000 筆備註。若要進一步了解這些變更，請參閱下列主題： • 在 AWS Secrets Manager 秘密中存放 PagerDuty 存取憑證 • 將 PagerDuty 服務整合至回應計劃	2022 年 12 月 15 日
Incident Manager 與 CloudWatch 指標整合。	您現在可以在 CloudWatch 中發佈事件相關指標。如需詳細資訊，請參閱 CloudWatch 指標。 AWSIncidentManagerServiceRolePolicy 包含額外的許可，允許我們的服務代表您發佈指標。	2022 年 12 月 15 日

已啟動事件備註並更新事件詳細資訊畫面	您可以使用事件備註，與其他處理事件的使用者進行協作和通訊。此外，您可以從事件詳細資訊畫面檢視 Runbook 和參與狀態。如需詳細資訊，請參閱事件詳細資訊。	2022 年 11 月 16 日
將 PagerDuty 呈報計畫和分頁工作流程整合至 Incident Manager 回應計畫	您現在可以將 Incident Manager 與 PagerDuty 整合，並將 PagerDuty 服務新增至回應計劃。設定整合之後，Invent Manager 可以在 PagerDuty 中為在 Incident Manager 中建立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升級政策。 如需詳細資訊，請參閱下列主題： • 與 Incident Manager 的產品和服務整合 • 在 AWS Secrets Manager 秘密中存放 PagerDuty 存取憑證 • 將 PagerDuty 服務整合至 主題中的回應計劃 建立回應計劃 • 疑難排解	2022 年 11 月 16 日
已啟動事件備註並更新事件詳細資訊畫面。	您可以使用事件備註，與其他處理事件的使用者進行協作和通訊。此外，您可以從事件詳細資訊畫面檢視 Runbook 和參與狀態。如需詳細資訊，請參閱事件詳細資訊。	2022 年 11 月 16 日

複寫集的標記支援	您現在可以將標籤指派給 中的複寫集 AWS Systems Manager Incident Manager。這會新增現有支援，以將標籤指派給複寫集中 AWS 區域 指定的 中的回應計劃、事件記錄和聯絡人。如需詳細資訊，請參閱以下主題： • 準備好精靈 • 標記 Incident Manager 資源	2022 年 11 月 2 日
Incident Manager 與 Atlassian Jira Service Management 整合	您可以使用 AWS Service Management Connector for Jira Service Management，將 Incident Manager 與 Jira Service Management 整合。設定整合之後，在 Incident Manager 中建立的新事件會在 Jira 中建立對應的事件。如果您在 Incident Manager 中更新事件，則更新會新增至 Jira 中對應的事件。如果您在 Incident Manager 或 Jira 中解決事件，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《Service Management Connector 管理員指南》中的設定 Jira AWS Service Management。	2022 年 10 月 6 日

增強型標記支援	Incident Manager 支援在複寫集中 AWS 區域 指定的 中，將標籤指派給回應計畫、事件記錄和聯絡人。Incident Manager 也支援自動將標籤指派給從回應計劃建立的事件。如需詳細資訊，請參閱標記 Incident Manager 資源。	2022 年 6 月 28 日
Incident Manager 與 ServiceNow 整合	您可以使用 AWS Service Management Connector for ServiceNow，將 Incident Manager 與 ServiceNow 整合。在您設定整合之後，在 Incident Manager 中建立的新事件會在 ServiceNow 中建立對應的事件。如果您在 Incident Manager 中更新事件，則更新會新增至 ServiceNow 中對應的事件。如果您在 Incident Manager 或 ServiceNow 中解決事件，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，請參閱在 ServiceNow 中整合 AWS Systems Manager Incident Manager。	2022 年 6 月 9 日

匯入聯絡人詳細資訊	建立事件時，Incident Manager 可以使用語音或簡訊通知來通知回應者。為了確保回應者看到呼叫或簡訊通知來自 Incident Manager，我們建議所有回應者將 Incident Manager 虛擬卡格式 (.vcf) 檔案下載到行動裝置上的通訊錄。如需詳細資訊，請參閱將聯絡人詳細資訊匯入您的通訊錄。	2022 年 5 月 18 日

多項功能改進，以增強事件建立和修復	Incident Manager 推出下列功能改進，以增強事件建立和修復： • 自動在其他 中建立事件 AWS 區域：如果當 Amazon CloudWatch 或 Amazon EventBridge 建立事件 AWS 區域 時， 中無法使用 Incident Manager，這些服務現在會自動在複寫集中指定的其中一個可用區域中建立事件。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 Incident Manager 從事件中收集 AWS 資源的相關資訊。然後 Incident Manager 可以將收集的資訊填入 Runbook 參數。如需詳細資訊，請參閱教學課程：搭配 Incident Manager 使用 Systems Manager Automation Runbook。 • 自動收集 AWS 資源資訊：當系統建立事件時，Invent Manager 現在會自動收集事件所涉及 AWS 資源的相關資訊。Incident Manager 接著會將此資訊新增至相關項目索引標籤。	2022 年 5 月 17 日
多執行手冊支援	Incident Manager 現在支援在事件詳細資訊頁面的事件期間執行多個 Runbook。	2022 年 1 月 14 日

在新的 中啟動的 Incident Manager AWS 區域	Incident Manager 現已在下列新區域提供：us-west-1、sa-east-1、ap-northeast-2、ap-south-1、ca-central-1、eu-west-2 和 eu-west-3。如需 Incident Manager 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 Incident Manager 主控台確認參與。	2021 年 8 月 5 日
屬性索引標籤	Incident Manager 將屬性索引標籤引入事件詳細資訊頁面，提供有關事件、父項 OpsItem 和相關事件後分析的詳細資訊。	2021 年 8 月 3 日
Incident Manager 啟動	Incident Manager 是一種事件管理主控台，旨在協助使用者緩解影響其 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。