aws

用户指南

Incident Manager

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Incident Manager: 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS Systems Manager Incident Manager？

Incident Manager 是 AWS Systems Manager 的一项功能，可帮助您减轻影响 AWS 托管应用程序的事件并从中恢复。

就 AWS 而言，事件是指可能对业务运营产生重大影响的任何意外中断或服务质量下降。因此，组织必须制定应对策略，以有效缓解并从中恢复过来，采取措施防止将来发生事件。

Incident Manager 通过以下方式帮助缩短解决事件的时间：

- 提供自动化计划，让负责响应事件的人员高效进行互动。
- 提供相关的故障排除数据。
- 使用预定义的自动化运行手册，启用自动响应操作。
- 提供与所有利益相关者合作和沟通的方法。

Incident Manager 内置的特征和工作流程基于 Amazon 自成立以来一直在开发的事件响应最佳实践。Incident Manager 与 Amazon CloudWatch、AWS CloudTrail、AWS Systems Manager 和 Amazon EventBridge 等 AWS 服务 集成。

主要组件和特征

该部分介绍 Incident Manager 中用于设置事件响应计划的特征。

响应计划

响应计划作为模板，用于定义事件发生时必须采取的措施。它包括以下信息：

- 事件发生时谁需要做出响应。
- 为缓解事件而建立的自动化响应。
- 响应者必须使用用于沟通和接收有关事件的自动通知的协作工具。

事件检测

您可以配置 Amazon CloudWatch 警报和 Amazon EventBridge 事件，以便在检测到影响 AWS 资源的条件或变化时创建事件。

运行手册自动化支持

您可以从 Incident Manager 中启动自动化运行手册，自动对事件做出关键响应，并为第一响应者提供详细的步骤。

互动和上报

互动计划规定了每个独特事件都要通知所有人。您可以指定已添加到 Incident Manager 的单个联系人，也可以指定在 Incident Manager 中创建的待命时间表。互动计划还规定了上报路径，以帮助确保在事件响应过程中利益相关者的可见性和积极参与。

待命时间表

Incident Manager 中的待命时间表由您为该计划创建的一个或多个轮换组成。每次轮换最多可包括 30 个联系人。在上报计划或响应计划中加入待命时间表后，就能确定在发生需要响应者干预的事件时，谁会收到通知。待命时间表有助于确保您根据事件响应的需要获得全面、冗余的全天候服务。

积极协作

事件响应者通过与 AWS Chatbot 客户端集成，积极应对事件。AWS Chatbot 支持为 Incident Manager 创建使用 Slack、Microsoft Teams 或 Amazon Chime 的聊天渠道。响应者可以直接相互通信，接收有关事件的自动通知，并在 Slack 和 Microsoft Teams 中直接运行一些 Incident Manager 命令行界面 (CLI) 操作。

事件诊断

事件发生期间，响应者可以在 Incident Manager 控制台中查看最新信息。然后，响应者可以根据信息的变化创建后续项目，并使用自动化运行手册对其进行补救。

其他服务的调查发现

为了支持响应者的事件诊断，您可以在 Incident Manager 中启用调查发现特征。调查发现是有关在事件发生前后发生的 AWS CodeDeploy 部署和 AWS CloudFormation 堆栈更新的信息，这些信息涉及一个或多个可能与事件相关的资源。掌握这些信息可以减少评估潜在原因所需的时间，从而缩短从事件中恢复的平均时间 (MTTR)。

事件后分析

在事件解决后，您可以使用事件后分析来确定事件响应的改进措施，包括检测和缓解时间。分析还可以帮助您了解事件的根本原因。Incident Manager 会创建建议的后续行动项目，您可以利用这些项目改进事件响应。

使用 Incident Manager 的好处

了解在事件检测和响应操作中使用 Incident Manager 的好处。

该部分介绍在实施 Incident Manager 响应计划时，您的组织可以获得的优势。

即时有效地诊断问题

当出现意外中断或服务质量下降时，您配置的 Amazon CloudWatch 警报和 Amazon EventBridge 事件可自动创建事件。

当指标或表达式的值在多个时间段内相对于阈值发生变化时，CloudWatch 警报会进行检测和报告。EventBridge 事件是由于您在 EventBridge 规则中指定的环境、应用程序或服务发生变化而创建的。创建警报或事件时，可以指定在 Incident Manager 中创建事件的操作以及适当的响应计划，以促进事件的互动、上报和缓解。

通过使用 CloudWatch 指标，Incident Manager 能够自动收集和跟踪与事件相关的指标。除了通过 CloudWatch 警报创建事件时自动生成的指标外，您还可以实时手动添加指标，为事件响应者提供更多的上下文和数据。

使用 Incident Manager 事件时间轴按时间顺序显示关注点。响应者还可以使用时间轴添加自定义事件，以描述他们所做的事情或发生的事情。自动关注点包括：

- CloudWatch 警报或 EventBridge 规则会创建事件。
- 事件指标将报告给 Incident Manager。
- 响应者进行互动。
- 运行手册步骤成功完成。

有效互动

Incident Manager 通过使用联系人、待命时间表、上报计划和聊天渠道将事件响应者聚集在一起。您可以直接在 Incident Manager 中定义单个联系人，并指定联系人首选项（电子邮件、短信或语音）。您可以将联系人添加到待命时间表轮换中，以确定在特定时间段内由谁处理事件。使用已定义的联系人和待命时间表，您可以制定上报计划，以便在事件发生期间的正确时间与必要的响应者互动。

实时协作

事件期间的沟通是更快解决问题的关键。通过使用 Slack、Microsoft Teams 或 Amazon Chime 设置 AWS Chatbot 客户端，您可以将响应者聚集到他们首选的联网聊天频道中，让他们可以直接与事件以及彼此互动。Incident Manager 还会在聊天频道中显示事件响应者的实时行动，为其他人提供上下文信息。

自动恢复服务

Incident Manager 通过使用自动化运行手册，使您的响应者能够专注于解决事件所需的关键任务。在 Incident Manager 中，运行手册是为解决事件而预定义的一系列操作。它们根据需要将自动任务的强大功能与手动步骤相结合，使响应者有更多时间进行分析和应对影响。

防止未来事件

通过使用 Incident Manager 进行事件后分析，您的团队可以制定更强大的响应计划，并在整个应用程序中进行更改，以防止未来发生事件和停机。事后分析还有助于迭代学习和改进运行手册、响应计划和指标。

相关服务

Incident Manager 与其他一些 AWS 服务 和第三方服务及工具集成，可帮助您检测和解决事件，并间接与其 API 操作进行交互和管理基础设施。有关信息，请参阅 产品和服务与 Incident Manager 集成。

访问 Incident Manager

您可以使用以下任一方式访问 Incident Manager：

- Incident Manager 控制台
- AWS CLI——有关一般信息，请参阅《AWS Command Line Interface 用户指南》中的开始使用 AWS CLI。有关 Incident Manager 的 CLI 命令的信息，请参阅AWS CLI 命令参考中的 ssm-incidents 和 ssm-contacts。
- Incident Manager API – 有关更多信息，请参阅 AWS Systems Manager Incident Manager API 参考。
- AWS SDK – 有关更多信息，请参阅用于在 AWS 上进行构建的工具。

Incident Manager 区域和配额

Systems Manager 支持的所有 AWS 区域 均不支持 Incident Manager。

要查看有关 Incident Manager 区域和配额的信息，请参阅 Amazon Web Services 一般参考 中的AWS Systems Manager Incident Manager 端点和配额。

Incident Manager 的定价

使用 Incident Manager 需要付费。有关更多信息，请参阅 AWS Systems Manager 的定价。

> **Note**
>
> 与该服务相关的其他 AWS 服务、AWS 内容和第三方内容可能需要单独收费，并受其他条款约束。

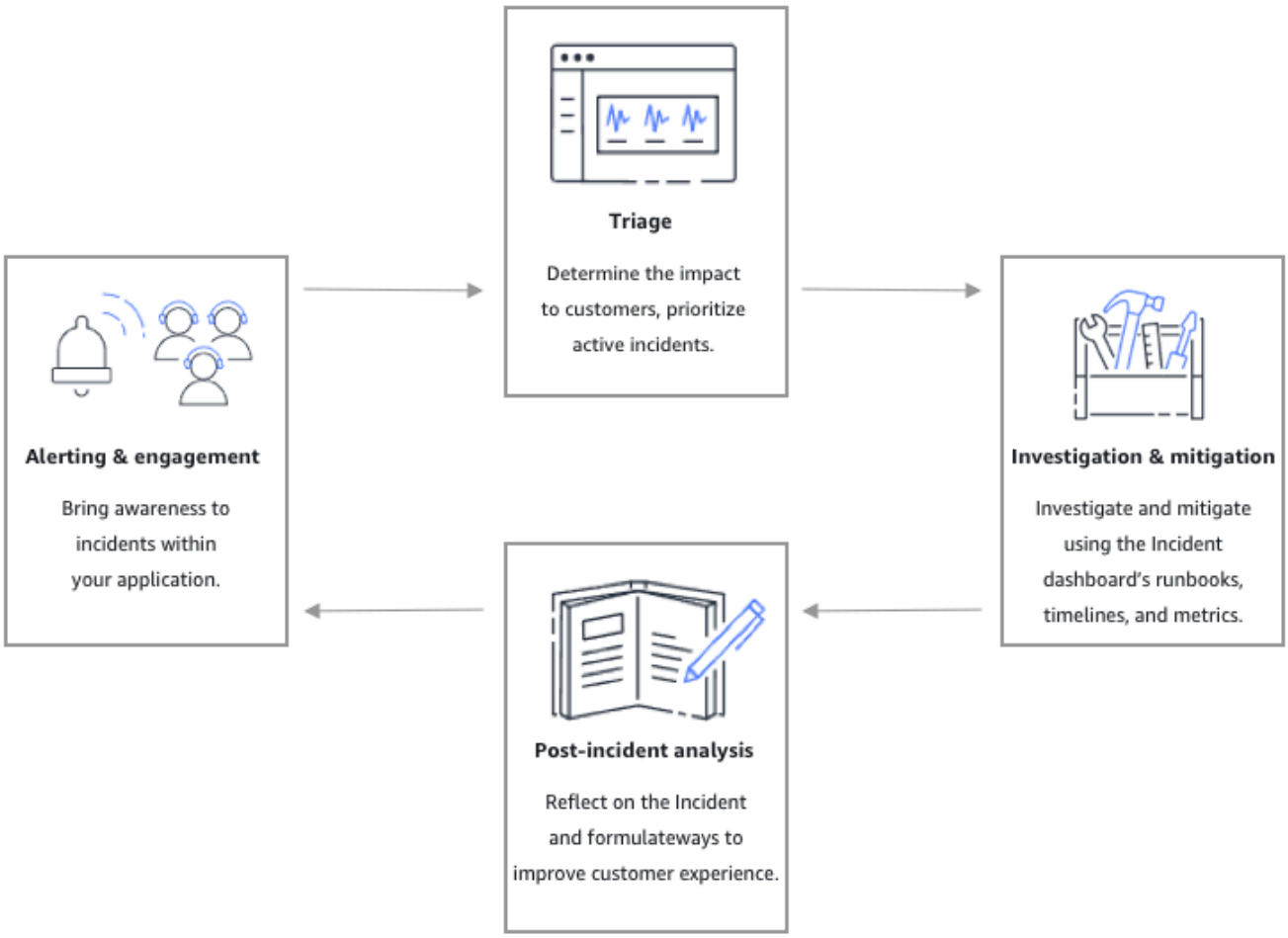
Trusted Advisor 服务可帮助您优化 AWS 环境的成本、安全性和性能，如需了解该服务的概述，请参阅《AWS Support 用户指南》中的 AWS Trusted Advisor。

Incident Manager 中的事件生命周期

AWS Systems Manager Incident Manager 提供了一个基于最佳实践的分步框架，用于识别和应对服务中断或安全威胁等事件。Incident Manager 主要侧重于通过完整的事件生命周期管理解决方案，帮助受影响的服务或应用程序尽快恢复正常。

Incident Manager 为事件生命周期的每个阶段提供工具和最佳实践：

- 警报和互动
- 分类
- 调查和缓解
- 事件后分析



警报和互动

事件生命周期的警报和互动阶段侧重于提高对应用程序和服务中事件的认识。该阶段在检测到事件之前就开始了，需要对您的应用程序有深入的了解。您可以使用 Amazon CloudWatch 指标来监控有关应用程序性能的数据，也可以利用 Amazon EventBridge 来汇总来自不同来源、应用程序和服务的警报。为应用程序设置监控后，您就可以开始对偏离历史标准的指标发出警报。要了解有关监控最佳实践的更多信息，请参阅 监控。

为了支持响应者的事件诊断，您可以在 Incident Manager 中启用调查发现特征。调查发现是有关在事件发生前后发生的 AWS CodeDeploy 部署和 AWS CloudFormation 堆栈更新的信息。掌握这些信息可以减少评估潜在原因所需的时间，从而缩短从事件中恢复的平均时间 (MTTR)。

现在，您可以监控应用程序中的事件，并定义在事件发生期间使用的事件响应计划。要了解有关制定响应计划的更多信息，请参阅 在 Incident Manager 中使用响应计划。Amazon EventBridge 事件或

CloudWatch 警报可使用响应计划作为模板自动创建事件。要了解有关事件创建的更多信息，请参阅 在 Incident Manager 中创建事件。

响应计划启动相关的上报计划和互动计划，以便让第一响应者参与到事件中来。有关设置上报计划的更多信息，请参阅 制定上报计划。同时，AWS Chatbot 使用聊天渠道通知响应者，将他们引导到事件详细信息页面。使用聊天渠道和事件详细信息，团队可以对事件进行沟通和分类。有关在 Incident Manager 中设置聊天渠道的更多信息，请参阅 任务 2：在 AWS Chatbot 中创建聊频道。

分类

分类是指第一响应者试图确定对客户的影响。Incident Manager 控制台中的事件详细信息视图为响应者提供了时间轴和指标，以帮助他们评估事件。评估事件的影响还可以为事件的响应时间、解决方案和沟通奠定基础。响应者根据从 1（严重）到 5（无影响）的影响评级来确定事件的优先级。

您的组织可以自行定义每个影响评级的确切范围。下表举例说明了每个影响等级通常是如何定义的。

影响代码	影响名称	示例定义范围
1	Critical	影响大多数客户的全面应用程序故障。
2	High	影响部分客户的全面应用程序故障。
3	Medium	对客户造成影响的部分应用程序故障。
4	Low	对客户影响有限的间歇性故障。
5	No Impact	客户目前没有受到影响，但需要采取紧急行动以避免影响。

调查和缓解

事件详细信息视图为您的团队提供了运行手册、时间轴和指标。要了解如何处理事件，请参阅 事件详细信息。

运行手册通常提供调查步骤，可以自动提取数据或尝试常用的解决方案。运行手册还提供了清晰、可重复的步骤，您的团队认为这些步骤有助于缓解事件。运行手册选项卡侧重于当前的运行手册步骤，并显示过去和未来的步骤。

Incident Manager 与 Systems Manager Automation 集成以构建运行手册。使用运行手册，执行以下任一操作：

- 管理实例和 AWS 资源
- 自动运行脚本
- 管理 AWS CloudFormation 资源

有关支持的操作类型的更多信息，请参阅《AWS Systems Manager 用户指南》https://docs.aws.amazon.com/systems-manager/latest/userguide/automation-actions.html中的 Systems Manager Automation 操作参考。

时间轴选项卡显示已采取的操作。时间轴会记录每个时间戳和自动创建的详细信息。要向时间轴添加自定义事件，请参阅本用户指南事件详细信息页面中的 时间轴 部分。

诊断选项卡显示自动填充的指标和手动添加的指标。此视图提供了有关事件期间应用程序活动的重要信息。

互动选项卡允许您向事件添加其他联系人，并帮助为互动的联系人提供资源，以便在参与事件后快速上手。通过定义的上报计划或个人互动计划与联系人互动。

使用聊天渠道，您可以直接与您的事件和团队中的其他响应者互动。使用 AWS Chatbot，您可以在 Slack、Microsoft Teams 和 Amazon Chime 中配置聊天渠道。在 Slack 和 Microsoft Teams 渠道中，响应者可以使用多种 `ssm-incidents` 命令直接从聊天渠道与事件互动。有关更多信息，请参阅 通过聊天频道进行互动。

事件后分析

Incident Manager 提供了一个框架，用于对事件进行反思，采取必要步骤防止事件在未来再次发生，并从整体上改进事件响应活动。改进功能可能包括：

- 更改事件中涉及的应用程序。您的团队可以利用这段时间改进系统，提高容错能力。
- 更改事件响应计划。花时间总结经验教训。
- 更改运行手册。您的团队可以深入研究解决问题所需的步骤以及您可以自动执行的步骤。

- 更改警报。事件发生后，您的团队可能已经注意到了指标中的关键点，您可以利用这些关键点来提醒团队更早地注意到事件。

Incident Manager 通过在事件时间轴旁边使用一组事后分析问题和行动项目来促进这些潜在的改进。要了解有关通过分析进行改进的更多信息，请参阅 在 Incident Manager 中执行事件后分析。

设置 AWS Systems Manager 事件管理器

我们建议在用于管理运营的账户中设置 S AWS ystems Manager 事件管理器。首次使用 Incident Manager 前，请完成以下任务：

主题

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

授权以编程方式访问

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关 AWS 软件开发工具包、工具和 AWS API，请参阅《软件开发工具包和AWS工具参考指南》中的 IAM 身份中心身份验证。
IAM	使用临时证书签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI、 AWS 软件开发工具包或 AWS API 发出的编程请求。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDK 和工具，请参阅 S AWS DK 和工具参

哪个用户需要编程式访问权限？	目的	方式
		考指南中的使用长期凭证进行身份验证。 • 有关 AWS API，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

Incident Manager 设置所需的角色

在开始之前，您的账户必须为 IAM 权限 `iam:CreateServiceLinkedRole`。Incident Manager 使用此权限在您的账户 `AWSServiceRoleforIncidentManager` 中创建。有关更多信息，请参阅 使用 Incident Manager 的服务相关角色。

开始使用 Incident Manager

该部分介绍在 Incident Manager 控制台中做准备。您需要先在控制台中完成做准备，然后才能将其用于事件管理。该向导会引导您设置复制集、至少一个联系人和一个上报计划以及您的第一个响应计划。以下指南将帮助您了解 Incident Manager 和事件生命周期：

- 什么是 AWS Systems Manager Incident Manager？
- Incident Manager 中的事件生命周期

先决条件

如果您第一次使用 Incident Manager，请参阅 设置 AWS Systems Manager 事件管理器。我们建议您在用于管理操作的账户中设置 Incident Manager。

我们建议您在开始 Incident Manager 做准备向导之前完成 Systems Manager 快速设置功能。使用 Systems Manager 快速设置功能以配置常用的 AWS 服务和特征，并提供建议的最佳实践。Incident Manager 使用 Systems Manager 特征来管理与 AWS 账户 相关的事件，并从首先配置的 Systems Manager 中受益。

准备向导

首次使用 Incident Manager 时，您可以从 Incident Manager 服务主页访问做准备向导。要在首次完成设置后访问做准备向导，请在事件列表页面上选择做准备。

1. 打开 Incident Manager 控制台。
2. 在 Incident Manager 服务主页上，选择做准备。

常规设置

1. 在常规设置下，选择设置。
2. 通读条款和条件。如果您同意 Incident Manager 的条款和条件，请选择我已阅读并同意 Incident Manager 的条款和条件，然后选择下一步。
3. 在区域区域中，您的当前 AWS 区域 显示为复制集中的第一个区域。要向您的复制集添加更多区域，请从区域列表中进行选择。

我们建议包括至少两个区域。如果其中一个区域暂时不可用，与事件有关的活动仍可转到另一个区域。

> **Note**
>
> 创建复制集可在账户中创建 `AWSServiceRoleforIncidentManager` 服务相关角色。要了解有关该角色的更多信息，请参阅 使用 Incident Manager 的服务相关角色。

4. 要为您的复制集设置加密，请执行以下操作之一：

> **Note**
>
> 所有 Incident Manager 资源均加密。要了解有关您的数据如何加密的更多信息，请参阅 Incident Manager 中的数据保护。有关 Incident Manager 复制集的更多信息，请参阅 使用 Incident Manager 复制集。

- 要使用 AWS 自有密钥，请选择使用 AWS 自有密钥。
- 要使用自己的 AWS KMS 密钥，请选择选择现有 AWS KMS key。对于您在步骤 3 中选择的每个区域，请选择 AWS KMS 密钥或输入 AWS KMS Amazon 资源名称（ARN）。

> **Tip**
>
> 如果您没有可用的 AWS KMS key，请选择创建 AWS KMS key。

5. （可选）在标签区域，向复制集添加一个或多个标签。标签包括密钥和可选的值。

标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。有关更多信息，请参阅 在 Incident Manager 中标记资源。

6. （可选）在服务访问权限区域中，要激活调查发现特征，请选择为该帐户中的调查发现创建服务角色复选框。

调查发现是指与事件创建时间相近的代码部署或基础设施变更的相关信息。可以将调查发现视为事件的潜在原因进行审查。有关这些潜在原因的信息已添加到事件的事件详细信息页面。由于有关这些部署和变更的信息随时可用，响应者无需手动搜索这些信息。

> **Tip**
>
> 要查看有关要创建的角色的信息，请选择查看权限。

7. 选择创建。

   要了解有关复制集和故障恢复能力的更多信息，请参阅 韧性在 AWS Systems Manager Incident Manager。

联系人（可选）

1. 选择创建联系人。

   Incident Manager 在事件期间与联系人互动。有关联系人的更多信息，请参阅 在 Incident Manager 中使用联系人。

2. 对于姓名，输入联系人的姓名。
3. 对于唯一别名，输入别名以识别该联系人。
4. 在联系人渠道部分，请执行以下操作以定义事件期间与联系人的互动方式：

   a. 对于类型，选择电子邮件、短信或语音。

   b. 对于渠道名称，输入有助于标识该渠道的唯一名称。

   c. 对于详细信息，输入联系人的电子邮件地址或电话号码。

      电话号码必须包含 9-15 个字符，并以 + 开头，然后是国家/地区代码和订阅用户号码。

   d. 要创建其他联系人渠道，请选择添加新的联系人渠道。我们建议为每位联系人至少定义两个渠道。

5. 在互动计划区域，请执行以下操作以定义通过哪些渠道通知联系人，以及通过每个渠道等待确认需要多长时间。选择用于在事件发生期间与联系人互动的联系人渠道。

> **Note**
>
> 我们建议在互动计划中至少定义两个设备。

   a. 对于联系人渠道名称，选择您在联系人渠道区域中指定的渠道。

   b. 对于互动时间（分钟），输入与联系人渠道互动之前要等待的分钟数。

我们建议您在互动开始时至少选择一个设备进行互动，并指定 **0**（零）分钟的等待时间。

c. 要在互动计划中添加更多联系人渠道，请选择添加互动。

6. （可选）在标签区域，向联系人添加一个或多个标签。标签包括密钥和可选的值。

   标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。有关更多信息，请参阅 在 Incident Manager 中标记资源。

7. 要创建联系人记录并向定义的联系人渠道发送激活码，请选择下一步。

8. （可选）在联系人渠道激活页面中，输入发送到每个渠道的激活码。

   如果您现在无法输入代码，则可以稍后再生成新的激活码。

9. 重复第四步，直到将所有联系人添加到 Incident Manager。

10. 输入所有联系人后，选择完成。

（可选）上报计划

1. 选择创建上报计划。

   事件发生期间，上报计划会通过您的联系人进行上报，从而确保 Incident Manager 在事件发生期间与正确的响应者互动。有关上报计划的更多信息，请参阅 在 Incident Manager 中使用上报计划。

2. 对于名称，输入上报计划的唯一名称。

3. 对于别名，输入唯一别名以帮助您识别上报计划。

4. 在第 1 阶段区域，执行以下操作：

   a. 对于上报渠道，请选择要互动的联系人渠道。

   b. 如果您希望联系人能够停止上报计划各阶段的进展，请选择确认停止计划进展。

   c. 要向一个阶段添加更多渠道，请选择添加上报渠道。

5. 要在上报计划中创建新阶段，请选择添加阶段并添加其阶段详细信息。

6. （可选）在标签区域，向上报计划添加一个或多个标签。标签包括密钥和可选的值。

   标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。有关更多信息，请参阅 在 Incident Manager 中标记资源。

7. 选择创建上报计划。

响应计划

1. 选择创建响应计划。使用响应计划整理您创建的联系人和上报计划。在该开始使用向导中，以下部分为可选部分，特别是如果您是第一次制定响应计划：

   - 聊天通道
   - 运行手册
   - 互动
   - 第三方集成

   有关稍后将这些要素添加到响应计划的信息，请参阅 在 Incident Manager 中为事件做准备。
2. 对于名称，输入响应计划输入的唯一、可识别的名称。该名称用于创建响应计划 ARN 或在没有显示名称的响应计划中。
3. （可选）对于显示名称，输入名称，以帮助您在创建事件时识别该响应计划。
4. 对于标题，输入标题，以帮助识别与该响应计划相关的事件类型。您指定的值将包含在每个事件的标题中。标题中还会添加引发事件的警报或事件。
5. 对于影响，选择您预期与该响应计划有关的事件的影响级别，例如 **`Critical`** 或 **`Low`**。
6. （可选）对于摘要，输入用于概述事件的简要说明。Incident Manager 会在事件发生期间自动将相关信息填入摘要中。
7. （可选）对于重复数据删除字符串，输入重复数据删除字符串。Incident Manager 使用此字符串来防止相同的根本原因在同一个账户中创建多个事件。

   重复数据删除字符串是系统用来检查重复事件的术语或短语。如果您指定重复数据删除字符串，Incident Manager 会在创建事件时在 `dedupeString` 字段中搜索包含相同字符串的未解决事件。如果检测到重复事件，Incident Manager 会删除较新事件的重复数据到现有事件中。

   > **Note**
   >
   > 默认情况下，Incident Manager 会自动删除由同一 Amazon CloudWatch 警报或 Amazon EventBridge 事件创建的多个事件的重复数据。您无需输入自己的重复数据删除字符串即可防止这些资源类型出现重复。
8. （可选）在标签区域，向响应计划添加一个或多个标签。标签包括密钥和可选的值。

   标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。有关更多信息，请参阅 在 Incident Manager 中标记资源。

9. 从互动下拉列表中选择要应用于事件的联系人和上报计划。
10. 选择创建响应计划。

创建响应计划后，您可以将 Amazon CloudWatch 警报或 Amazon EventBridge 事件与响应计划相关联。这将根据警报或事件自动创建事件。有关更多信息，请参阅 在 Incident Manager 中创建事件。

Incident Manager 中的跨区域和跨账户事件管理

您可以将 Incident Manager（AWS Systems Manager 的功能）配置为使用多个 AWS 区域 和帐户。该部分介绍跨区域和跨账户的最佳实践、设置步骤和已知限制。

主题

跨区域事件管理

Incident Manager 支持在多个 AWS 区域 中自动和手动创建事件。当您使用做准备向导初次使用 Incident Manager 时，最多可为复制集指定三个 AWS 区域。对于 Amazon CloudWatch 警报或 Amazon EventBridge 事件自动创建的事件，Incident Manager 会尝试在与事件规则或警报相同的 AWS 区域 中创建事件。如果在 AWS 区域 中没有 Incident Manager，CloudWatch 或 EventBridge 会自动在复制集中指定的可用区域中创建事件。

> **Important**
>
> 请注意以下重要详细信息。
>
> - 我们建议您在复制集中至少指定两个 AWS 区域。如果您未指定至少两个区域，系统将无法在 Incident Manager 不可用期间创建事件。
> - 跨区域失效转移创建的事件不会调用响应计划中指定的运行手册。

有关使用 Incident Manager 和指定其他区域的更多信息，请参阅 开始使用 Incident Manager。

跨账户事件管理

Incident Manager 使用 AWS Resource Access Manager (AWS RAM) 在管理和应用程序帐户之间共享 Incident Manager 资源。该部分介绍跨账户最佳实践、如何为 Incident Manager 设置跨账户功能以及 Incident Manager 中跨账户功能的已知限制。

管理账户是您用来执行操作管理的账户。在组织设置中，管理账户拥有响应计划、联系人、上报计划、运行手册和其他 AWS Systems Manager 资源。

应用程序账户是拥有构成应用程序的资源的账户。这些资源可以是 Amazon EC2 实例、Amazon DynamoDB 表或您用于在 AWS Cloud 中构建应用程序的任何其他资源。应用程序账户还拥有在 Incident Manager 中创建事件的 Amazon CloudWatch 警报和 Amazon EventBridge 事件。

AWS RAM 使用资源共享在账户之间共享资源。您可以在 AWS RAM 账户之间共享响应计划和联系人资源。通过共享这些资源，应用程序账户和管理账户可以与互动和事件进行互动。共享响应计划可共享使用该响应计划创建的所有过去和未来事件。共享联系人会共享该联系人或响应计划过去和未来的所有互动。

最佳实践

在跨账户共享 Incident Manager 资源时，请遵循以下最佳实践：

- 定期更新资源共享中的响应计划和联系人。
- 定期审查资源共享原则。
- 在您的管理账户中设置 Incident Manager、运行手册和聊天频道。

设置和配置跨账户事件管理

以下步骤介绍了如何设置和配置 Incident Manager 资源并将其用于跨账户功能。您过去可能已经为跨账户功能配置了一些服务和资源。在使用跨账户资源开始您的第一次事件之前，请将这些步骤作为需求清单。

1. （可选）使用 AWS Organizations 创建组织和组织单位。请按照《AWS Organizations 用户指南》中的教程：创建和配置组织中的步骤。
2. （可选）使用 Systems Manager 快速设置功能来设置正确的 AWS Identity and Access Management 角色，供您在配置跨账户运行手册时使用。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的快速设置功能。
3. 按照《AWS Systems Manager 用户指南》中在多个 AWS 区域 和账户中运行自动化中列出的步骤，在 Systems Manager Automation 文档中创建运行手册。运行手册既可以由管理账户运行，也可以由应用程序账户运行。根据您的用例，您需要为在事件期间创建和查看运行手册所需的角色安装相应的 AWS CloudFormation 模板。
    - 在管理账户中运行运行手册。管理账户必须下载并安装 AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 模板。安装 AWS-SystemsManager-AutomationReadOnlyRole 时，请指定所有应用程序帐户的帐户 ID。该角色将允许您的应用程序帐户从事件详细信息页面读取运行手册的状态。应用程序账户必须安装 AWS-

SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 模板。事件详细信息页面使用该角色从管理账户获取自动化状态。

- 在应用程序帐户中运行运行手册。管理账户必须下载并安装 AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 模板。该角色允许管理账户读取应用程序账户中运行手册的状态。应用程序账户必须下载并安装 AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 模板。安装 AWS-SystemsManager-AutomationReadOnlyRole 时，请指定管理账户和其他应用程序账户的账户 ID。管理账户和其他应用程序账户代入该角色，以读取运行手册的状态。

4. （可选）在组织中的每个应用程序帐户中，下载并安装 AWS-SystemsManager-IncidentManagerIncidentAccessServiceRoleCloudFormation 模板。安装 AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole 时，请指定管理账户的账户 ID。该角色提供 Incident Manager 访问 AWS CodeDeploy 部署和 AWS CloudFormation 堆栈更新信息所需的权限。如果启用了调查发现特征，则会将此信息报告为事件的调查发现。有关更多信息，请参阅 在 Incident Manager 中处理调查发现。
5. 要设置和创建联系人、上报计划、聊天渠道和响应计划，请按照 在 Incident Manager 中为事件做准备 中的详细步骤操作。
6. 将您的联系人和响应计划资源添加到您的现有资源共享或 AWS RAM 中的新资源共享。有关更多信息，请参阅《AWS RAM 用户指南》中的开始使用 AWS RAM。将响应计划添加到 AWS RAM 可使应用程序账户访问使用响应计划创建的事件和事件控制面板。应用程序账户还能将 CloudWatch 警报和 EventBridge 事件与响应计划相关联。将联系人和上报计划添加到 AWS RAM 中后，应用程序账户就可以从事件控制面板中查看互动情况并与联系人互动。
7. 向 CloudWatch 控制台添加跨账户跨区域功能。有关步骤和信息，请参阅《Amazon CloudWatch 用户指南》https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Cross-Account-Cross-Region.html中的跨账户跨区域 CloudWatch 控制台。添加该功能可确保您创建的应用程序账户和管理账户能够查看和编辑事件和分析控制面板中的指标。
8. 创建跨账户的 Amazon EventBridge 事件总线。有关步骤和信息，请参阅在 AWS 账户之间发送和接收 Amazon EventBridge 事件。然后，您可以使用该事件总线创建事件规则，以检测应用程序账户中的事件并在管理账户中创建事件。

限制

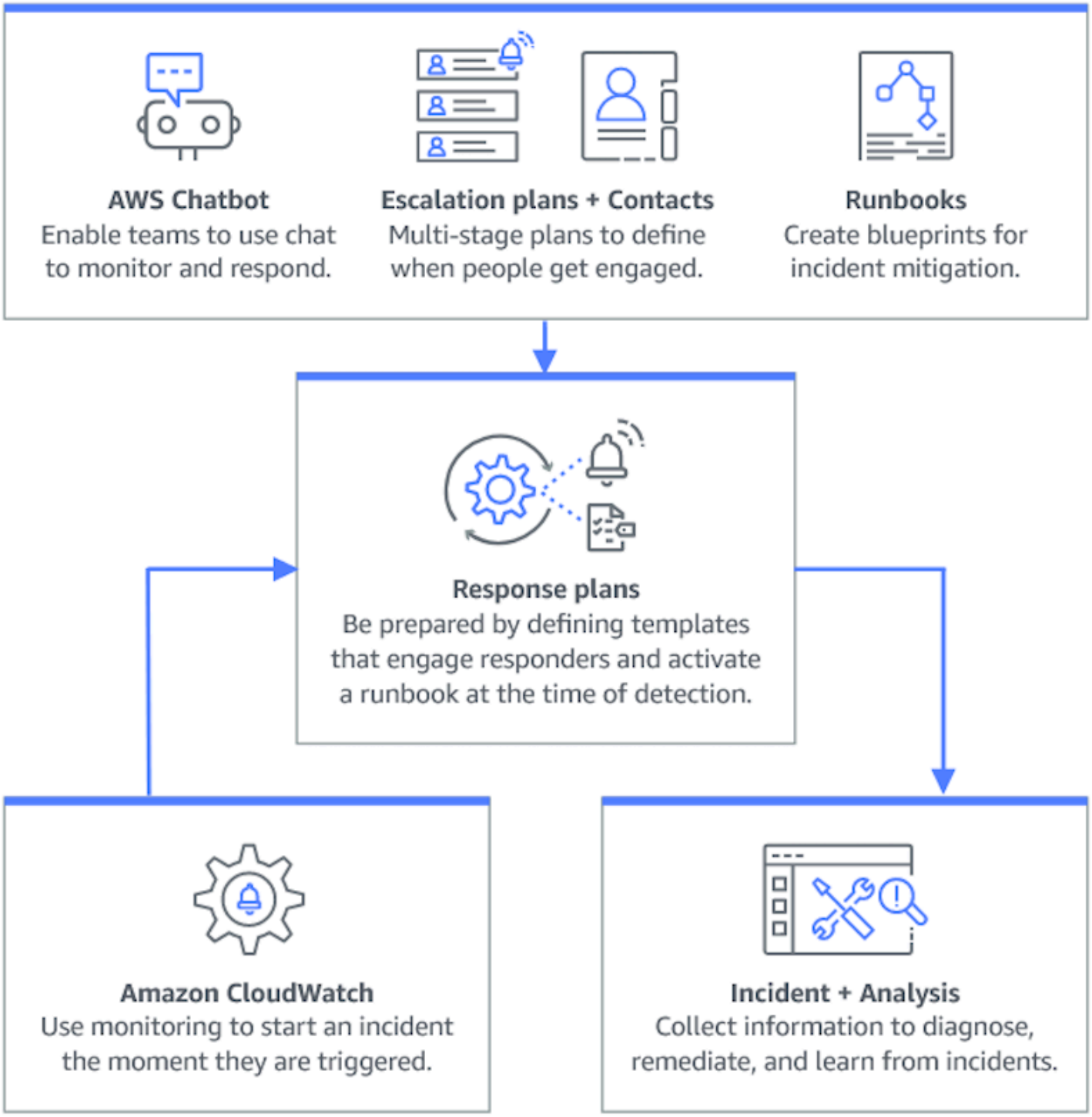
以下是 Incident Manager 跨账户功能的已知限制：

- 创建事后分析的帐户是唯一可以查看和更改该分析的帐户。如果您使用应用程序帐户创建事件后分析，则只有该帐户的成员才能查看和更改。如果使用管理账户创建事故后分析，也会发生同样的情况。
- 在应用程序账户中运行的自动化文档不会弹出时间轴事件。在应用程序帐户中运行的自动化文档的更新可在事件的运行手册 选项卡中查看。

- Amazon Simple Notification Service 主题不能跨账户使用。Amazon SNS 主题必须与其使用的响应计划在相同的区域和账户中创建。我们建议使用管理账户创建所有 SNS 主题和响应计划。
- 上报计划只能使用同一账户中的联系人创建。已与您共享的联系人无法添加到您账户的上报计划中。
- 应用于响应计划、事件记录和联系人的标签只能通过资源所有者账户查看和修改。

在 Incident Manager 中为事件做准备

事件规划早在事件生命周期之前就已开始。要为事件做好准备，请在制定响应计划之前考虑以下每个主题。使用监控、联系人、上报计划、聊天频道和运行手册来制定自动响应的响应计划。



主题

监控

监控 AWS 托管应用程序的运行状况是确保应用程序正常运行时间和性能的关键。在确定监控解决方案时，请注意以下事项：

- 特征的严重性——如果系统发生故障，对下游用户的影响将有多严重。
- 故障的共同性——系统发生故障的频率；需要经常干预的系统应受到密切监控。
- 延迟时间增加——完成一项任务的时间增加或减少了多少。
- 客户端指标与服务器端指标——如果客户端和服务器上的相关指标之间存在差异。
- 依赖性故障——您的团队可以而且应该做好准备的故障。

创建响应计划后，您可以使用监控解决方案在环境中发生事件时自动跟踪事件。有关事件跟踪和创建的更多信息，请参阅 在 Incident Manager 中跟踪事件。

有关构建安全、高性能、弹性和高效基础设施应用程序和工作负载的更多信息，请参阅 AWS Well-Architected 白皮书。

使用常规设置

完成 Incident Manager 入门向导后，您可以在设置页面上管理某些选项。这些选项包括您的复制集、应用于复制集的标签以及调查发现特征。

主题

使用 Incident Manager 复制集

Incident Manager 复制集可将数据复制到多个 AWS 区域，以增加跨区域冗余，允许 Incident Manager 访问不同区域的资源，并减少用户的延迟。复制集还用于使用 AWS 托管式密钥 或您自己的客户托管式密钥对数据进行加密。默认情况下，所有 Incident Manager 资源均加密。要了解有关您的资源如何加密的更多信息，请参阅 Incident Manager 中的数据保护。要开始使用 Incident Manager，请先使用做准备向导创建您的复制集。要了解有关在 Incident Manager 中做准备的更多信息，请参阅 准备向导。

编辑复制集

通过使用 Incident Manager 设置页面，您可以编辑您的复制集。您可以添加区域、删除区域以及启用或禁用复制集删除保护。您无法编辑用于加密数据的密钥。要更改密钥，请删除并重新创建复制集。

添加区域

1. 打开 Incident Manager 控制台，然后从左侧导航窗格中选择设置。
2. 选择添加区域。
3. 选择区域。
4. 选择添加。

删除区域

1. 打开 Incident Manager 控制台，然后从左侧导航窗格中选择设置。
2. 选择要删除的区域。
3. 选择删除。
4. 在文本框中输入删除，然后选择删除。

删除复制集

删除复制集中的最后一个区域会删除整个复制集。在删除最后一个区域之前，请通过在设置页面上切换删除保护来禁用删除保护。删除复制集后，您可以使用做准备向导创建新的复制集。

要从复制集中删除区域，请在创建该区域后等待 24 小时。在创建后 24 小时内尝试从复制集删除区域会导致删除失败。

删除复制集会删除所有 Incident Manager 数据。

删除复制集

1. 打开 Incident Manager 控制台，然后从左侧导航窗格中选择设置。
2. 在复制集中选择最后一个区域。
3. 选择删除。
4. 在文本框中输入删除，然后选择删除。

管理复制集的标签

标签是您分配给资源的可选元数据。使用标签按不同的方式（如用途、拥有者或环境）对资源进行分类。

要管理复制集的标签

1. 打开 Incident Manager 控制台，然后从左侧导航窗格中选择设置。
2. 在标签 部分中，选择编辑。
3. 要添加标签，请执行以下操作：
   a. 选择添加新标签。
   b. 输入标签的密钥和可选值。
   c. 选择保存。
4. 要删除标签，请执行以下操作：
   a. 在要删除的标签的下面，选择删除。
   b. 选择保存。

管理调查发现特征

调查发现特征可帮助组织中的响应者在事件开始后立即识别事件的潜在根本原因。目前，Incident Manager 提供 AWS CodeDeploy 部署和 AWS CloudFormation 堆栈更新的调查发现。

对于跨账户支持调查发现，在启用该特征后，您必须在组织中的每个应用程序账户中完成额外的设置步骤。

要使用该特征，您可以让 Incident Manager 创建一个服务角色，该角色包含代表您访问数据所需的权限。

要启用调查发现特征

1. 打开 Incident Manager 控制台，然后从左侧导航窗格中选择设置。
2. 在调查发现区域中，选择创建服务角色。
3. 查看要创建的服务角色的相关信息，然后选择创建。

要禁用调查发现特征

要停止使用调查发现特征，请从创建 `IncidentManagerIncidentAccessServiceRole` 角色的每个账户中删除该角色。

1. 访问：https://console.aws.amazon.com/iam/，打开 IAM 控制台。
2. 在左侧导航窗格中，选择角色。
3. 在搜索框中，输入 **`IncidentManagerIncidentAccessServiceRole`**。
4. 选择角色的名称，然后选择删除。
5. 在对话框中输入角色的名称，确认要删除角色，然后选择删除。

在 Incident Manager 中使用联系人

AWS Systems Manager Incident Manager 联系人是事件的响应者。Incident Manager 在事件发生期间可以通过多个渠道与联系人互动。您可以定义联系人的互动计划，描述 Incident Manager 与联系人互动的方式和时间。

主题

- 联系人渠道
- 互动计划
- 创建联系人
- 将联系人详细信息导入您的通讯录

联系人渠道

联系渠道是 Incident Manager 用于与联系人互动的各种方法。

Incident Manager 支持以下联系渠道：

- 电子邮件
- 短信服务 (SMS)
- 语音

联系人渠道激活

为了保护您的隐私和安全，Incident Manager 会在您创建联系人时向您发送设备激活码。要在事件发生期间使用您的设备，必须先将其激活。为此，请在创建联系人页面输入设备激活码。

Incident Manager 的某些特征包括向联系人渠道发送通知的功能。使用这些特征，即表示您同意本服务向指定工作流程中的联系人渠道发送有关服务中断或其他事件的通知。这包括作为待命时间表轮换的一部分发送给联系人的通知。通知可根据联系人的详细信息，通过电子邮件、短信或语音电话发送。通过使用这些特征，您确认自己有权将您提供的联系人渠道添加到Incident Manager 中。

选择退出

您可以随时取消这些通知，方法是删除移动设备作为联系人渠道。个人通知收件人也可以随时从联系人中删除设备，从而取消通知。

要从联系人中删除联系人渠道

1. 导航到 Incident Manager 控制台，然后从左侧导航栏中选择联系人。
2. 选择要删除的联系人渠道的联系人，然后选择编辑。
3. 选择您要删除的联系人渠道旁边的删除。
4. 选择更新。

联系人渠道停用

要停用设备，请回复取消订阅。回复取消订阅会阻止 Incident Manager 使用您的设备。

联系人渠道重新激活

1. 对来自 Incident Manager 的消息回复开始。

2. 导航到 Incident Manager 控制台，然后从左侧导航栏中选择联系人。
3. 选择要删除的联系人渠道的联系人，然后选择编辑。
4. 选择激活服务。
5. 输入 Incident Manager 发送到设备的激活码。
6. 选择激活。

互动计划

互动计划定义了 Incident Manager 何时与联系人渠道互动。您可以在互动开始的不同阶段多次与联系人渠道互动。您可以在上报计划或响应计划中使用互动计划。要了解有关上报计划的更多信息，请参阅在 Incident Manager 中使用上报计划。

创建联系人

创建联系人的步骤如下。

1. 打开 Incident Manager 控制台，然后从左侧导航栏中选择联系人。
2. 选择创建联系人。
3. 键入联系人的全名，并提供唯一且可识别的别名。
4. 定义联系人渠道。我们建议拥有两种或两种以上不同类型的联系人渠道。
   a. 选择类型：电子邮件、短信或语音。
   b. 为联系人渠道输入一个可识别的名称。
   c. 提供联系人渠道的详细信息，例如电子邮件：arosalez@example.com
5. 要定义多个联系人渠道，请选择添加联系人渠道。每添加一个新的联系人渠道，就重复步骤 4。
6. 定义互动计划。

> **Important**
> 要与联系人互动，您必须定义互动计划。

   a. 选择联系人渠道名称。
   b. 定义从互动开始到 Incident Manager 与该联系人渠道互动的等待时间。

c. 要添加其他联系人渠道，请选择添加互动。

7. 定义互动计划后，选择创建。Incident Manager 向每个定义的联系人渠道发送激活码。
8. （可选）要激活联系人渠道，请输入 Incident Manager 发送给每个定义的联系人渠道的激活码。
9. （可选）要发送新的激活码，请选择发送新的激活码。
10. 选择结束。

定义联系人并激活其联系人渠道后，您可以将联系人添加到上报计划中以形成上报链。要了解有关上报计划的更多信息，请参阅 在 Incident Manager 中使用上报计划。您可以将联系人添加到响应计划中以进行直接互动。要了解有关制定响应计划的更多信息，请参阅 在 Incident Manager 中使用响应计划。

将联系人详细信息导入您的通讯录

创建事件后，Incident Manager 可以使用语音或短信通知来通知响应者。为确保响应者看到来电或短信通知来自 Incident Manager，我们建议所有响应者将 Incident Manager 虚拟卡片格式 (.vcf) 文件下载到其移动设备上的通讯录中。该文件托管在 Amazon CloudFront 中，可在 AWS 商业分区中使用。

要下载 Incident Manager .vcf 文件

1. 在您的移动设备上，选择或输入以下网址：https://d26vhuvd5b89k2.cloudfront.net/aws-incident-manager.vcf。
2. 将文件保存或导入到移动设备上的通讯录。

在 Incident Manager 中使用待命时间表

Incident Manager 中的待命时间表定义了当发生需要操作员干预的事件时，谁会收到通知。待命时间表由您为该时间表创建的一个或多个轮换组成。每次轮换最多可包括 30 个联系人。

创建待命时间表后，您可以将其作为上报纳入上报计划中。当发生与该上报计划相关的事件时，Incident Manager 会根据时间表通知待命的操作员（或多名操作员）。然后，该联系人可以确认互动。在上报计划中，您可以在多个上报阶段指定一个或多个待命时间表，以及一个或多个联系人。有关更多信息，请参阅 在 Incident Manager 中使用上报计划。

> **Tip**
>
> 作为最佳实践，我们建议在上报计划中添加联系人和待命时间表作为上报渠道。然后，您应选择上报计划作为响应计划的互动方式。这种方法可以最大限度地覆盖您的组织中的事件响应。

每个待命时间表最多支持八次轮换。轮换可以重叠或同时运行。这增加了在事件发生时被通知做出响应的操作员数量。您也可以创建连续运行的轮换。这支持诸如“全天候式”事件管理之类的场景，在这种场景中，世界各地都有支持相同服务的群组。

该部分中的主题可帮助您创建和管理事件响应操作的待命时间表。

主题

- 在 Incident Manager 中创建待命时间表和轮换
- 在 Incident Manager 中管理现有的待命时间表

在 Incident Manager 中创建待命时间表和轮换

制定待命时间表，让一个或多个联系人轮换互动，以处理轮班期间发生的事件。

开始之前

在创建待命时间表之前，请确保您之前创建了要添加到时间表轮换中的联系人。有关信息，请参阅 在 Incident Manager 中使用联系人。

考虑夏令时（DST）的变化

创建轮换时，您可以指定全球时区，该时区作为轮班覆盖时间和日期的基础。您可以使用互联网编号分配机构 (IANA) 定义的任何时区。例如：America/Los_Angeles、UTC 和 Asia/Seoul。您可以在待命时间表中添加多个轮换。但是，当每次轮换的响应者在地理位置上位于不同的时区时，请注意每次轮换可能会发生的任何夏令时变化。

例如，America/Los_Angeles 并 Europe/Dublin 遵守不同的 DST 时间表。因此，根据一年中的不同时间，两个区域之间的时差可能相差 6 到 8 个小时。例如，全天候式待命时间表在 America/Los_Angeles 时区轮换一次，在 Europe/Dublin 轮换一次。在该示例中，由于 DST 的变化，时间表可能包含一小时的轮班间隔或一小时的轮班重叠。

为避免出现这些情况，建议您使用以下方法：

1. 在待命时间表中，所有轮换都使用单一时区。
2. 在指定特定时区以外的响应者时，请计算当地时间。

如果您决定将每次轮换分配到其当地时区，请在任何 DST 之前查看时间表。然后，根据需要调整轮班时间，以确保在 DST 变化生效之前，避免待命覆盖范围出现任何意外间隙或重叠。

要创建待命时间表

1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 选择创建待命时间表。
4. 对于时间表名称，输入名称以帮助您识别时间表，例如 **MyApp Primary On-call Schedule**。
5. 在时间表别名中，为该时间表输入在当前 AWS 区域 中唯一的别名，例如 **my-app-primary-on-call-schedule**。
6. （可选）在标签区域，将一个或多个标签密钥名称和值对应用到待命时间表。

   标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。例如，您可以标记时间表，以确定其运行的时间段、包含的操作员类型或支持的上报计划。有关标记 Incident Manager 资源的更多信息，请参阅 在 Incident Manager 中标记资源。
7. 继续在待命时间表中添加一个或多个轮换。

在 Incident Manager 中为待命时间表创建轮班

待命时间表中的轮班规定了轮班的生效时间。它还指定了轮班轮换的联系人。您最多可以在单个待命时间表中包括八次轮换。

您可以将在 Incident Manager 中创建为联系人的任何个人添加到轮换中。有关管理联系人的信息，请参阅 在 Incident Manager 中使用联系人。

在配置轮换时，您可以在页面右侧的预览日历中看到整个时间表的外观。

要创建待命时间表的轮班

1. 在创建待命时间表页面的轮换 1部分，在轮换名称中，输入标识轮换的名称，例如 **00:00 - 7:59 Support** 或 **Dublin Support Group**。
2. 对于开始日期，以 YYYY/MM/DD 格式输入该轮换开始生效的日期，例如 2023/07/14。
3. 对于时区，选择全球时区，该时区作为您为该轮换指定的轮班覆盖时间和日期的基础。

   您可以使用互联网编号分配机构 (IANA) 定义的任何时区。例如：“America/Los_Angeles”、“UTC”或“Asia/Seoul”。有关更多信息，请参阅 IANA 网站上的时区数据库。

> **Warning**
>
> 您可以根据自己的时区进行每次轮换。但是，您所选择时区的夏令时变化可能会影响您的预期覆盖窗口。有关更多信息，请参阅本主题前面的考虑夏令时 (DST) 的变化。

4. 对于轮换开始时间，以 24 小时 hh:mm 格式输入该轮换的轮班开始的时间，例如 16:00。

   请注意，与您指定的时区不同的联系人的当地时间差异。例如，如果您选择 America/Los_Angeles 为时区，00:00 为轮换开始时间，这相当于爱尔兰都柏林的 08:00，印度孟买的 13:30。

5. 对于轮换结束时间，以 24 小时 hh:mm 格式输入该轮换的轮班结束的时间，例如 23:59。

> **Note**
>
> 轮换开始和结束之间的间隔时间必须至少为 30 分钟。

6. （可选）要将轮换长度设置为 24 小时，请选择 24 小时覆盖，然后在轮换开始时间字段中输入该轮换的开始时间。轮换结束时间值会自动更新。

   例如，如果您希望待命时间为 24 小时，而轮班在上午 11 点更换，请选择 24 小时覆盖，然后输入 **11:00** 作为开始时间。

7. 对于活跃天数，选择该轮换在一周中的处于活动状态的天数。例如，如果您的待命计划不包括周末，请选择除周日和周六之外的所有天数。

8. 继续将联系人添加到轮换中。

在 Incident Manager 的待命时间表中将联系人添加到轮换中

在您的待命时间表中，每次轮换都可以添加一个或多个联系人，最多可添加 30 个。您可以从 Incident Manager 配置中设置的联系人中进行选择。

当您将联系人添加到轮换中时，该联系人可能会收到通知，作为其待命职责的一部分。通知可根据联系人的详细信息，通过电子邮件、短信或语音电话发送。

有关管理联系人和联系人通知选项的信息，请参阅 在 Incident Manager 中使用联系人。

要将联系人添加到待命时间表的轮换中

1. 在创建待命时间表页面上，在轮换的联系人部分，选择添加或删除联系人。

2. 在添加或删除联系人对话框中，选择要包含在轮换中的联系人的别名。

   您选择联系人的顺序就是这些联系人在轮换时间表中首次列出的顺序。您可以在添加联系人后更改顺序。

3. 选择确认。

4. 要更改联系人在顺序中的位置，请选择该用户的单选按钮，然后使用向上
   ()
   和向下
   ()
   按钮更新联系人顺序。

5. 继续指定轮换的个别轮班周期和时长。

在 Incident Manager 中指定轮班周期和时长，并向轮换添加标签

轮班周期规定了轮换中的联系人轮换进入和退出待命的频率。周期时长可以按天数、周数或月数指定。

要指定轮班周期和时长，并向轮换添加标签

1. 在创建待命时间表页面上，在轮换的周期设置部分，请执行以下操作：

   - 对于轮班周期类型，请从 `Daily`、`Weekly` 和 `Monthly` 中进行选择，指定每个待命轮班是持续多少天、几周还是几个月。
   - 对于轮班时长，输入轮班持续多少天、几周还是几个月。

     例如，如果您选择 `Daily` 并输入 **1**，则每位联系人的待命轮班将持续一天。如果您选择 `Weekly` 并输入 **3**，则每位联系人的待命轮班将持续三周。

2. （可选）在标签 区域，将一个或多个标签密钥名称和值对应用到轮换。

   标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。例如，您可以标记轮换，以确定分配给该轮换的联系人的位置、其本应提供的轮换覆盖类型或其支持的上报计划。有关标记 Incident Manager 资源的更多信息，请参阅 在 Incident Manager 中标记资源。

3. （推荐）使用日历预览，确保待命时间表的覆盖范围不会出现意外间隙。

4. 选择创建。

现在，您可以在上报计划中将待命时间表添加为上报渠道。有关信息，请参阅 制定上报计划。

在 Incident Manager 中管理现有的待命时间表

使用本部分中的内容可帮助您处理已创建的待命时间表。

主题

查看待命时间表详细信息

您可以在查看待命时间表详细信息页面上查看待命时间表的概要信息。该页面还包含当前待命人员和下一个待命人员的信息。该页面包含一个日历视图，显示在任何特定时间哪些联系人待命。

要查看待命时间表详细信息

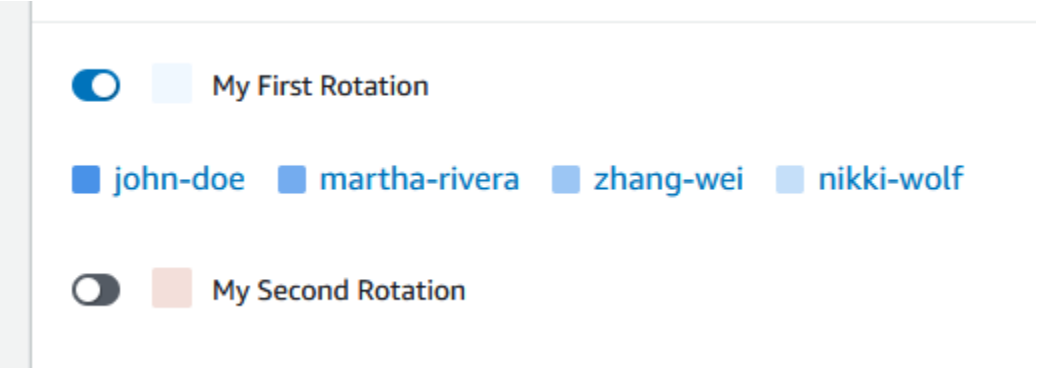
1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 在要查看的待命时间表行中，请执行以下操作之一：

   - 要打开日历摘要视图，请选择时间表别名。

     –或者–

     选择该行的单选按钮，然后选择查看。
   - 要打开时间表的日历视图，请选择查看日历

     在日历视图中，选择时间表中特定日期的联系人姓名，查看有关分配轮班的详细信息或创建替换。
   - 要打开或关闭日历中特定轮换的显示，请选择轮换名称旁边的开关。



编辑待命时间表

您可以更新待命时间表及其轮换的配置，但以下详细信息除外：

- 时间表别名
- 轮换名称
- 轮换开始日期

要使用现有日历作为能够更改这些值的新日历的基础，您可以改为复制该日历。有关信息，请参阅 复制待命时间表。

要编辑待命时间表

1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 请执行下列操作之一：
   - 选择要编辑的待命时间表行中的单选按钮，然后选择编辑。
   - 选择待命时间表的时间表别名，打开查看待命时间表详细信息页面，然后选择编辑。
4. 对待命时间表及其轮换进行必要的修改。您可以更改轮换配置选项，例如开始和结束时间、联系人和周期。您可以根据需要从时间表中添加或删除轮换。日历预览会反映您所做的更改。

   有关使用页面选项的信息，请参阅 在 Incident Manager 中创建待命时间表和轮换。
5. 选择更新。

> **Important**
>
> 如果您编辑包含替换的时间表，则您所做的更改会影响替换。为确保您的替换按预期配置，我们建议您在更新时间表后仔细检查您的轮班替换。

复制待命时间表

要将现有待命时间表的配置作为新时间表的起点，您可以创建一个日历副本并根据需要对其进行修改。

要复制待命时间表

1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 选择要复制的待命时间表行中的单选按钮。
4. 选择复制。
5. 对日历及其轮换进行任何必要的修改。您可以根据需要更改、添加或删除轮换。

   > **Note**
   >
   > 复制现有时间表时，必须为每次轮换指定新的开始日期。复制的时间表不支持以过去的开始日期进行轮换。

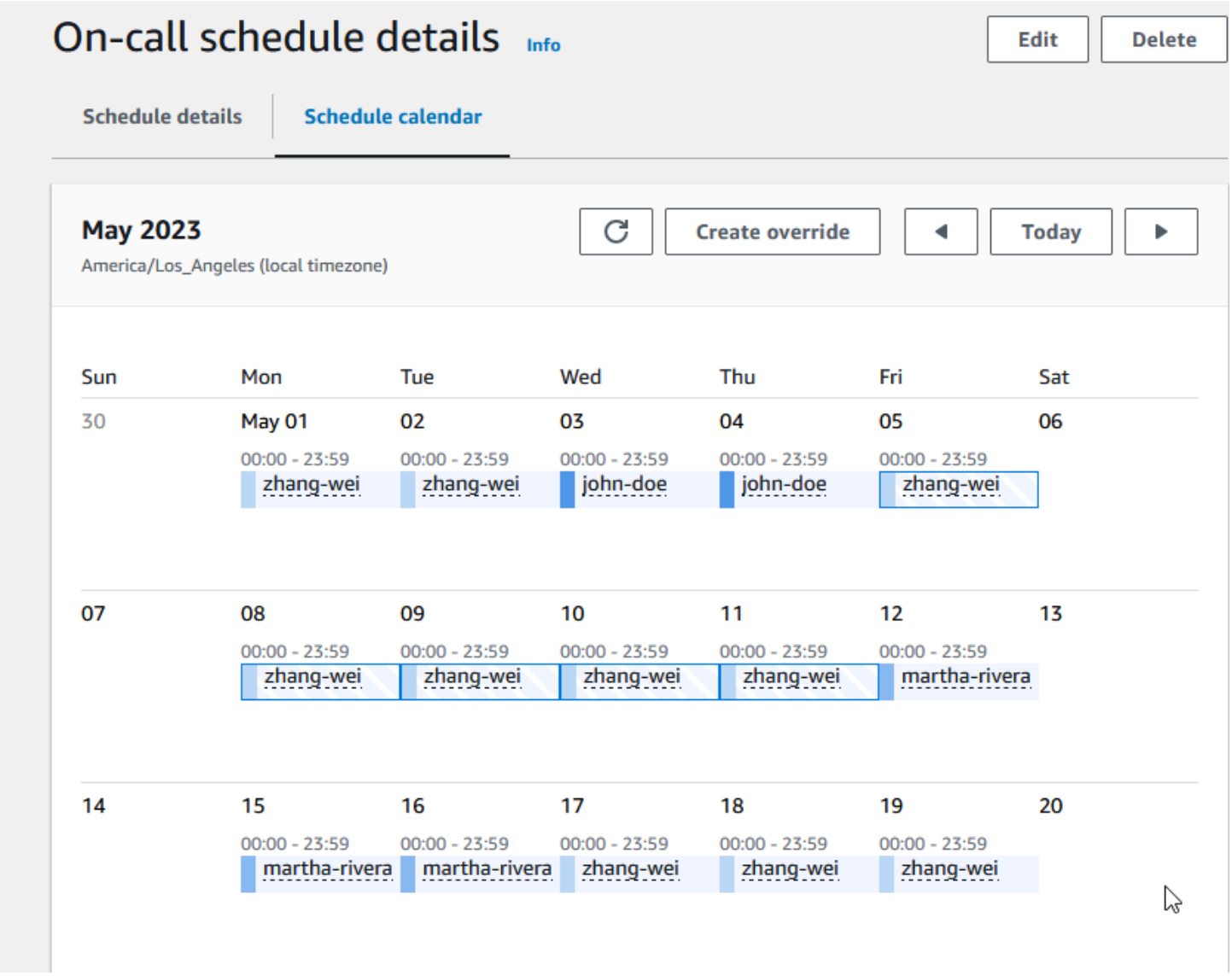
   有关使用页面选项的信息，请参阅 在 Incident Manager 中创建待命时间表和轮换。
6. 选择创建副本。

创建待命时间表轮换的替换

如果您需要对现有的轮换时间表进行一次性更改，则可以创建替换。通过替换，您可以将联系人的全部或部分轮班替换为另一个联系人。您还可以创建跨越多个轮班的替换。

您只能将联系人分配给已分配给轮换的替换对象。

在日历预览中，替换的轮班以条纹背景而不是纯色背景显示。在下图中，我们可以看到联系人 Zhang Wei 正在待命，其中包括 John Doe 和 Martha Rivera 的部分轮班，从 5 月 5 日开始到 5 月 11 日结束。



要创建待命时间表的替换

1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 在要查看的待命时间表行中，请执行以下操作之一：
   - 选择时间表别名，然后选择时间表日历选项卡。
   - 选择查看日历

     。
4. 请执行下列操作之一：
   - 选择创建替换。
   - 在日历预览中选择联系人的姓名，然后选择替换轮班。

5. 在创建轮班替换对话框中，请执行以下操作：

> **Note**
>
> 替换时间必须至少为 30 分钟。您只能为未来不超过 6 个月的轮班指定替换。

   a. 对于选择轮换，选择要在其中创建替换的轮换名称。
   b. 对于开始日期，选择或输入替换开始的日期。
   c. 对于开始时间，以 hh:mm 格式输入替换开始的时间。
   d. 对于结束日期，选择或输入替换结束的日期。
   e. 对于结束时间，以 hh:mm 格式输入替换结束的时间。
   f. 对于选择替换联系人，选择在替换期间待命的轮换联系人姓名。
6. 选择创建替换。

创建替换后，您可以通过条纹背景来识别它。当您为一个替换的轮班选择联系人姓名时，一个信息框会将其标识为替换的轮班。您可以选择删除替换将其删除并恢复原始的待命分配。

删除待命时间表

当您不再需要特定的待命时间表时，可以将其从 Incident Manager 中删除。

如果任何上报计划或响应计划目前使用待命时间表作为上报渠道，则应在删除时间表之前将其从这些计划中删除。

要删除待命时间表

1. 打开 Incident Manager 控制台。
2. 在左侧导航窗格中，选择待命时间表。
3. 选择要删除的待命时间表行中的单选按钮。
4. 选择删除。
5. 在删除待命时间表中？对话框中，在文本框中输入 **confirm**。
6. 选择删除。

在 Incident Manager 中使用上报计划

AWS Systems Manager Incident Manager 通过您定义的联系人或待命时间表（统称为上报渠道）提供上报途径。您可以同时将多个上报渠道引入一个事件。如果上报渠道中的指定联系人没有响应，Incident Manager 会上报到下一组联系人。您还可以选择在用户确认互动后计划是否停止上报。您可以将上报计划添加到响应计划中，以便在事件开始时自动开始上报。您也可以为活动事件添加上报计划。

主题

阶段

上报计划分阶段进行，每个阶段持续规定的分钟数。每个阶段显示以下信息：

- 持续时间——计划在下一阶段开始之前等待的时间。互动开始后，上报计划的第一阶段就开始了。
- 上报渠道——上报渠道可以是单个联系人，也可以是待命时间表，该时间表由多个联系人组成，他们按规定的时间表轮职。上报计划使用其定义的互动计划使每个渠道进行互动。您可以设置每个上报渠道，以便在上报计划进入下一阶段之前停止其进展。每个阶段可以有多个上报渠道。

  有关设置单个联系人的信息，请参阅 在 Incident Manager 中使用联系人。有关创建待命时间表的信息，请参阅 在 Incident Manager 中使用待命时间表。

制定上报计划

1. 打开 Incident Manager 控制台，然后从左侧导航栏中选择上报计划。
2. 选择创建上报计划。
3. 对于名称，输入上报计划的唯一名称，例如 **`My Escalation Plan`**。
4. 对于别名，输入别名以帮助您识别计划，例如 **`my-escalation-plan`**。
5. 对于阶段持续时间，输入 Incident Manager 在进入下一阶段之前等待的分钟数。
6. 对于上报渠道，请选择一个或多个联系人或待命时间表以在此阶段进行互动。
7. （可选）要让联系人在确认互动后停止上报计划，请选择确认停止计划进展。
8. 要向该阶段添加另一个渠道，请选择添加上报渠道。

9. 要向上报计划添加另一个阶段，请选择添加阶段。
10. 重复步骤 5 到 9，直到您完成为该上报计划添加所需的上报渠道和阶段。
11. （可选）在标签 区域，将一个或多个标签密钥名称和值对应用到上报计划。

    标签是您分配给资源的可选元数据。标签可让您按不同的方式（如用途、拥有者或环境）对资源进行分类。例如，您可以标记一个上报计划，以确定其用于的事件类型、包含的上报渠道类型或支持的上报计划。有关标记 Incident Manager 资源的更多信息，请参阅 在 Incident Manager 中标记资源。
12. 选择创建上报计划。

在 Incident Manager 中使用聊天频道

Incident Manager 是一种 AWS Systems Manager 功能，使事件响应者能够在事件发生期间直接通过聊天频道进行沟通。聊天频道是您在 AWS Chatbot 中设置的聊天室。然后，您可以将该频道连接到 Incident Manager 中的响应计划。

在事件发生期间，响应者使用聊天频道就事件相互沟通。Incident Manager 还会将有关事件的所有更新和通知直接推送到聊天频道。它会使用您在聊天室配置中指定的一个或多个 Amazon Simple Notification Service (Amazon SNS) 主题发送这些通知。

AWS Chatbot 和 Incident Manager 支持以下应用程序中的聊天频道：

- Slack
- Microsoft Teams
- Amazon Chime

在事件中设置聊天频道的过程包括在三种不同的 Amazon Web Services 服务中执行任务。

任务

- 任务 1：为您的聊天频道创建或更新 Amazon SNS 主题
- 任务 2：在 AWS Chatbot 中创建聊频道
- 任务 3：将聊天频道添加到 Incident Manager 的响应计划中
- 通过聊天频道进行互动

任务 1：为您的聊天频道创建或更新 Amazon SNS 主题

Amazon SNS 是一项托管服务，提供从发布者向订阅者（也称为创建者和使用者）的消息传输。发布者通过将消息发送至主题与订阅者进行异步交流，主题是一个逻辑访问点和通信渠道。Incident Manager 使用与响应计划关联的一个或多个主题，向事件响应者发送有关事件的通知。

在响应计划中，您可以在事件通知中加入一个或多个 Amazon SNS 主题。作为最佳实践，您应该在复制集中添加的每个 AWS 区域 中创建一个 SNS 主题。

> **Tip**
>
> 要使设置工作流程更有条理，我们建议您先配置 Amazon SNS 主题，以便与 Incident Manager 一起使用。配置完成后，您就可以创建聊天频道了。

要为您的聊天频道创建或更新 Amazon SNS 主题

1. 请按照《Amazon Simple Notification Service 开发人员指南》中的创建 Amazon SNS 主题的步骤进行操作。

   > **Note**
   >
   > 创建主题后，编辑主题以更新其访问策略。

2. 选择创建的主题，并记下或复制主题的 Amazon 资源名称 (ARN)，格式如 `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`。
3. 选择编辑，然后展开访问策略部分，配置默认值之外的其他访问权限。
4. 将以下语句添加到策略的语句数组：

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

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

按如下方式替换####：

- *snsnsopic-arn* 是您为该区域创建的主题的 Amazon 资源名称(ARN)，格式为 `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`。
- *account-id* 是您正在使用的 AWS 账户 的 ID，例如 `111122223333`。

5. 选择保存更改。
6. 在复制集中包含的每个区域重复该过程。

任务 2：在 AWS Chatbot 中创建聊频道

您可以在 Slack、Microsoft Teams 或 Amazon Chime 中创建聊天频道。每个响应计划只需一个聊天频道。

对于您的聊天频道，我们建议您遵循最低权限原则（不要向用户提供超过完成任务所需的权限）。您还应定期查看 AWS Chatbot 聊天频道的成员情况。查看有助于检查只有相应的响应者和其他利益相关者才能访问聊天频道。

在启用了 AWS Chatbot 的 Slack 频道和 Microsoft Teams 频道中，事件响应者可以直接从 Slack 或 Microsoft Teams 应用程序中运行大量 Incident Manager CLI 命令。有关更多信息，请参阅 通过聊天频道进行互动。

> **Important**
>
> 您添加到聊天频道的用户必须与上报或响应计划中列出的联系人相同。您还可以向聊天频道添加其他用户，例如利益相关者和事件观察者。

有关 AWS Chatbot 的一般信息，请参阅《AWS Chatbot 管理员指南》中的什么是 AWS Chatbot？。

从以下应用程序中进行选择以创建您的频道：

Slack

该步骤提供了建议的权限设置，允许所有频道用户使用 Incident Manager 的聊天命令。使用支持的聊天命令，您的事件响应者可直接从 Slack 聊天频道更新事件并与之互动。有关信息，请参阅 通过聊天频道进行互动。

要在 Slack 中创建聊天频道

- 按照《AWS Chatbot 管理员指南》中的教程：开始使用 Slack 中的步骤进行操作，并在配置中加入以下内容。
  - 在步骤 10 中，对于角色设置，选择 频道角色。
  - 在步骤 10d 中，对于策略模板，选择Incident Manager 权限。
  - 在步骤 11 中，对于频道防护机制策略，在策略名称中，选择 AWSIncidentManagerResolverAccess。
  - 在步骤 12 中的 SNS 主题部分，执行以下操作：
    - 对于区域 1，选择您的复制集中包含的 AWS 区域。
    - 对于主题 1，选择您在该区域创建的 SNS 主题，用于向聊天频道发送事件通知。
    - 对于复制集中的每个其他区域，请选择添加其他区域，然后添加其他区域和 SNS 主题。

Microsoft Teams

该步骤提供了建议的权限设置，允许所有频道用户使用 Incident Manager 的聊天命令。使用支持的聊天命令，您的事件响应者可直接从 Microsoft Teams 聊天频道更新事件并与之互动。有关信息，请参阅 通过聊天频道进行互动。

要在 Microsoft Teams 中创建聊天频道

- 按照《AWS Chatbot 管理员指南》中的教程：开始使用 Microsoft Teams 中的步骤进行操作，并在配置中加入以下内容：
  - 在步骤 10 中，对于角色设置，选择 频道角色。
  - 在步骤 10d 中，对于策略模板，选择Incident Manager 权限。
  - 在步骤 11 中，对于频道防护机制策略，在策略名称中，选择 AWSIncidentManagerResolverAccess。
  - 在步骤 12 中的 SNS 主题部分，执行以下操作：
    - 对于区域 1，选择您的复制集中包含的 AWS 区域。

- 对于主题 1，选择您在该区域创建的 SNS 主题，用于向聊天频道发送事件通知。
- 对于复制集中的每个其他区域，请选择添加其他区域，然后添加其他区域和 SNS 主题。

Amazon Chime

要在 Amazon Chime 中创建聊天频道

- 按照《AWS Chatbot 管理员指南》中的教程：开始使用 Amazon Chime中的步骤进行操作，并在配置中加入以下内容：
  - 在步骤 11 中，对于策略模板，选择 Incident Manager 权限。
  - 在步骤 12 中，在 SNS 主题部分，选择将向 Amazon Chime 网络钩子发送通知的 SNS 主题：
    - 对于区域 1，选择您的复制集中包含的 AWS 区域。
    - 对于主题 1，选择您在该区域创建的 SNS 主题，用于向聊天频道发送事件通知。
    - 对于复制集中的每个其他区域，请选择添加其他区域，然后添加其他区域和 SNS 主题。

> **Note**
>
> Amazon Chime 不支持事件响应者可在 Slack 和 Microsoft Teams 聊天频道中使用的聊天命令。

任务 3：将聊天频道添加到 Incident Manager 的响应计划中

创建或更新响应计划时，您可以添加聊天渠道，供响应者通过聊天频道进行沟通和接收更新。

按照 制定响应计划 中的步骤操作时，在 （可选）指定事件响应聊天频道 部分中，选择要用于处理与该响应计划相关的事件的频道。

通过聊天频道进行互动

对于 Slack 和 Microsoft Teams 中的频道，Incident Manager 允许响应者使用以下 `ssm-incidents` 命令直接从聊天频道与事件进行互动：

- 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
- list-related-items
- list-related-items
- list-related-items

要在活动事件的聊天频道中运行命令，请使用以下格式。将 *cli-options* 替换为要包含在命令中的任何选项。

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

例如：

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

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

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

在 Incident Manager 中使用 Systems Manager Automation 运行手册

您可以使用 AWS Systems Manager 的一项功能 AWS Systems Manager 自动化中的运行手册来自动执行 AWS Cloud 环境中的常见应用程序和基础设施任务。

每个运行手册都定义了一个运行手册工作流程，该工作流程包括 Systems Manager 在托管式节点或其他 AWS 资源类型上执行的操作。您可以使用运行手册来自动维护、部署和修复 AWS 资源。

在 Incident Manager 中，运行手册推动事件响应和缓解，您可以指定要作为响应计划一部分的运行手册。

在响应计划中，您可以从数十个预先配置的运行手册中进行选择，用于执行常见的自动化任务，也可以创建自定义运行手册。当您在响应计划定义中指定运行手册时，系统可以在事件开始时自动启动运行手册。

> **Important**
>
> 跨区域失效转移创建的事件不会调用响应计划中指定的运行手册。

有关 Systems Manager Automation、运行手册以及将运行手册与 Incident Manager 一起使用的详细信息，请参阅以下主题：

- 要向响应计划添加运行手册，请参阅 在 Incident Manager 中使用响应计划。
- 要了解有关运行手册的更多信息，请参阅《AWS Systems Manager 用户指南》和《AWS Systems Manager 自动化运行手册参考》https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-runbook-reference.html中的 AWS Systems Manager 自动化。
- 有关使用运行手册的成本的信息，请参阅 Systems Manager 定价。
- 有关在 Amazon CloudWatch 警报或 Amazon EventBridge 事件创建事件时自动调用运行手册的信息，请参阅教程：将 Systems Manager Automation 运行手册与 Incident Manager 一起使用。

主题

启动和运行运行手册工作流程所需的 IAM 权限

作为事件响应的一部分，Incident Manager 需要运行手册的权限。要提供这些权限，您可以使用 AWS Identity and Access Management (IAM) 角色、运行手册服务角色和自动化 *AssumeRole*。

运行手册服务角色是必需的服务角色。该角色为 Incident Manager 提供了访问和启动运行手册工作流程所需的权限。

自动化 AssumeRole 提供了运行运行手册中指定的各个命令所需的权限。

> **Note**
>
> 如果未指定 AssumeRole，则 Systems Manager Automation 会尝试将运行手册服务角色用于单个命令。如果未指定 AssumeRole，则必须向运行手册服务角色添加必要的权限。否则，运行手册将无法运行这些命令。
> 但是，作为最佳安全实践，我们建议使用单独的 AssumeRole。使用单独的 AssumeRole，您可以限制必须添加到每个角色的必要权限。

有关自动化 AssumeRole 的更多信息，请参阅《AWS Systems Manager 用户指南》中的配置自动化的服务角色（代入角色）访问权限。

您可以在 IAM 控制台中手动创建任一类型的角色。-您也可以让 Incident Manager 在创建或更新响应计划时为您创建任一角色。

运行手册服务角色权限

运行手册服务角色权限通过类似于以下内容的策略提供。

第一条语句允许 Incident Manager 启动 Systems Manager StartAutomationExecution 操作。然后，该操作将在三种 Amazon 资源名称 (ARN) 格式表示的资源上运行。

当运行手册在受影响的账户中运行时，第二条语句允许运行手册服务角色代入另一个账户中的角色。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的在多个 AWS 区域 和账户中运行自动化。

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

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

自动化 AssumeRole 权限

创建或更新响应计划时，您可以从多个 AWS 托管式策略中进行选择，以附加到 Incident Manager 创建的 AssumeRole。这些策略提供了运行 Incident Manager 运行手册场景中使用的许多常见操作的权限。您可以选择一个或多个托管式策略来为您的 `AssumeRole` 策略提供权限。 下表描述了从 Incident Manager 控制台创建 `AssumeRole` 时可以选择的策略。

AWS 托管式策略名称	策略描述
`AmazonSSMAutomationRole`	授予 Systems Manager Automation 服务运行运行手册中定义的活动的权限。将此策略分配给管理员和可信高级用户。
`AWSIncidentManagerResolverAccess`	授予用户启动、查看和更新事件的权限。您还可以使用它们在事件控制面板中创建客户时间轴事件和相关项目。

您可以使用这些托管式策略向许多常见的事件响应场景授予权限。但是，您需要的特定任务所需的权限可能会有所不同。在这种情况下，您需要为 `AssumeRole` 提供额外的策略权限。有关信息，请参阅 AWS Systems Manager 自动化运行手册参考。

使用运行手册参数

将运行手册添加到响应计划时，您可以指定运行手册在运行时应使用的参数。响应计划支持具有静态和动态值的参数。对于静态值，在响应计划中定义参数时输入该值。对于动态值，系统通过收集事件信息来确定正确的参数值。Incident Manager 支持以下动态参数：

`Incident ARN`

Incident Manager 创建事件时，系统会捕获相应事件记录的 Amazon 资源名称 (ARN)，并将其输入到运行手册中的该参数。

> **Note**
>
> 该值只能分配给 `String` 类型的参数。如果分配给任何其他类型的参数，则运行手册将无法运行。

`Involved resources`

Incident Manager 创建事件时，系统会捕获事件中涉及的资源的 ARN。然后将这些资源 ARN 分配给运行手册中的该参数。

关于关联资源

Incident Manager 可以使用 CloudWatch 警报、EventBridge 事件和手动创建的事件中指定的 AWS 资源 ARN 填充运行手册参数值。这一部分介绍了在填充该参数时，Incident Manager 可以捕获 ARN 的不同资源类型。

CloudWatch 警报

当通过 CloudWatch 警报操作创建事件时，Incident Manager 会自动从关联的指标中提取以下类型的资源。然后，它使用以下相关资源填充所选参数：

AWS 服务	资源类型
Amazon DynamoDB	全局二级索引 流

AWS 服务	资源类型
	表
Amazon EC2	映像 实例
AWS Lambda	函数别名 函数版本 函数
Amazon Relational Database Service（Amazon RDS）	集群 数据库实例
Amazon Simple Storage Service（Amazon S3）	存储桶

EventBridge 规则

当系统根据 EventBridge 事件创建事件时，Incident Manager 会在事件中用 `Resources` 属性填充所选参数。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 事件。

手动创建的事件

当您使用 StartIncident API 操作创建事件时，Incident Manager会使用 API 调用中的信息填充所选参数。具体来说，它通过使用在 `relatedItems` 参数中传递的 `INVOLVED_RESOURCE` 类型项来填充参数。

> **Note**
>
> `INVOLVED_RESOURCES` 值只能分配给 `StringList` 类型的参数。如果分配给任何其他类型的参数，则运行手册将无法运行。

定义运行手册

创建运行手册时，您可以按照此处提供的步骤进行操作，也可以按照《Systems Manager 用户指南》中使用运行手册部分提供的更详细的指南进行操作。如果您要创建多账户、多区域运行手册，请参阅《Systems Manager 用户指南》中的在多个 AWS 区域 和账户中运行自动化。

定义运行手册

1. 通过 https://console.aws.amazon.com/systems-manager/ 打开 Systems Manager 控制台。
2. 在导航窗格中，选择文档。
3. 选择创建自动化。
4. 输入唯一且可识别的运行手册名称。
5. 输入运行手册的描述。
6. 提供自动化文档要代入的 IAM 角色。这允许运行手册自动运行命令。有关更多信息，请参阅为自动化工作流程配置服务角色访问权限。
7. （可选）添加运行手册启动时的任何输入参数。启动运行手册时，您可以使用动态或静态参数。动态参数使用运行手册启动时的事件中的值。静态参数使用您提供的值。
8. （可选）添加目标类型。
9. （可选）添加标签。
10. 填写运行手册运行时将采取的步骤。每个步骤都需要：
    - 名称。
    - 步骤的用途描述。
    - 要在步骤中运行的操作。运行手册使用暂停操作类型来描述手动步骤。
    - （可选）命令属性。
11. 添加所有必需的运行手册步骤后，选择创建自动化。

要启用跨账户功能，请将管理账户中的运行手册与在事件发生期间使用该运行手册的所有应用程序帐户共享。

共享运行手册

1. 通过 https://console.aws.amazon.com/systems-manager/ 打开 Systems Manager 控制台。
2. 在导航窗格中，选择文档。

3. 在文档列表中，选择要共享的文档，然后选择查看详细信息。在权限选项卡中，确保您是文档所有者。只有文档所有者才可共享文档。
4. 选择编辑。
5. 要公开共享命令，请选择公开，然后选择保存。要私下共享命令，请选择私有，输入 AWS 账户 ID，选择添加权限，然后选择保存。

Incent Manager 运行手册模板

Incident Manager 提供了以下运行手册模板，以帮助您的团队开始在 Systems Manager Automation 中编写运行手册。您可以按原样使用此模板，也可以对其进行编辑以包含特定于您的应用程序和资源的详细信息。

查找 Incident Manager 运行手册模板

1. 通过 https://console.aws.amazon.com/systems-manager/ 打开 Systems Manager 控制台。
2. 在导航窗格中，选择文档。
3. 在文档区域中，在搜索字段中输入 **`AWSIncidents-`** 以显示所有 Incident Manager 运行手册。

> **Tip**
>
> 输入 **`AWSIncidents-`** 作为自由文本，而不是使用文档名前缀筛选器选项。

使用模板

1. 通过 https://console.aws.amazon.com/systems-manager/ 打开 Systems Manager 控制台。
2. 在导航窗格中，选择文档。
3. 从文档列表中选择要更新的模板。
4. 选择内容选项卡，然后复制文档的内容。
5. 在导航窗格中，选择文档。
6. 选择创建自动化。
7. 输入唯一且可识别的名称。
8. 选择编辑器选项卡。
9. 选择编辑。
10. 在文档编辑器区域粘贴或输入复制的详细信息。

11. 选择创建自动化。

AWSIncidents-CriticalIncidentRunbookTemplate

AWSIncidents-CriticalIncidentRunbookTemplate 是一个以手动步骤提供 Incident Manager 事件生命周期的模板。这些步骤足够通用，可用于大多数应用程序，但也足够详细，可供响应者开始解决事件。

在 Incident Manager 中使用响应计划

响应计划允许您计划如何响应影响用户的事件。响应计划就像一个模板，其中包含有关参与人员、事件的预期严重程度、要启动的自动运行手册以及要监控的指标等信息。

最佳实践

提前计划事件时，可以减少事件对团队的影响。在设计响应计划时，团队应考虑以下最佳实践。

- 简化互动——确定最适合处理事件的团队。如果您互动的分发名单太广，或者您互动的团队不对，就会在事件中造成混乱，浪费响应者的时间。
- 可靠的上报——对于响应计划中的互动，我们建议您选择互动计划，而不是联系人或待命时间表。互动计划应明确在事件发生期间要参与的个人联系人或待命时间表（其中包含多个轮换联系人）。由于有时可能无法联系到您的互动计划中指定的响应者，因此您应在响应计划中配置备用响应者，以应对这些情况。有了备用联系人，如果无法联系主要联系人和次要联系人，或出现其他意外中断，Incident Manager 仍会将事件通知联系人。
- 运行手册——使用运行手册提供可重复、易于理解的步骤，以减轻响应者在事件期间所承受的压力。
- 协作——使用聊天频道简化事件期间的沟通。聊天频道可帮助响应者及时了解最新信息。他们还可以通过这些频道与其他响应者共享信息。

制定响应计划

使用以下步骤创建响应计划并自动执行事件响应。

要创建响应计划

1. 打开 Incident Manager 控制台并在导航栏中选择响应计划。
2. 选择创建响应计划。

3. 在 名称中，输入唯一且可识别的响应计划名称，以用于响应计划的 Amazon 资源名称（ARN）。
4. （可选）在显示名称中，输入更易于理解的名称，以帮助您在创建事件时识别响应计划。
5. 继续为事件记录指定默认值。

指定事件默认值

为了帮助您更有效地管理事件，您可以指定默认值。Incident Manager 将这些值应用于与响应计划关联的所有事件。

要指定事件默认值

1. 在标题中，输入该事件的标题，以帮助您在 Incident Manager 主页上识别该事件。
2. 在影响中，选择影响级别以指明根据该响应计划创建的事件的潜在范围，例如严重或低。有关 Incident Manager 中影响级别的信息，请参阅 分类。
3. （可选）在摘要中，输入根据该响应计划创建的事件类型的简短摘要。
4. （可选）对于重复数据删除字符串，输入重复数据删除字符串。Incident Manager 使用此字符串来防止相同的根本原因在同一个账户中创建多个事件。

   重复数据删除字符串是系统用来检查重复事件的术语或短语。如果您指定重复数据删除字符串，Incident Manager 会在创建事件时在 `dedupeString` 字段中搜索包含相同字符串的未解决事件。如果检测到重复事件，Incident Manager 会删除较新事件的重复数据到现有事件中。

   > **Note**
   >
   > 默认情况下，Incident Manager 会自动删除由同一 Amazon CloudWatch 警报或 Amazon EventBridge 事件创建的多个事件的重复数据。您无需输入自己的重复数据删除字符串即可防止这些资源类型出现重复。

5. （可选）在事件标签下，添加要分配给根据该响应计划创建的事件的标签密钥和值。

   您必须拥有事件记录资源的 `TagResource` 权限，才能在响应计划中设置事件标签。
6. 继续指定一个可选的聊天频道，供解决者就事件相互沟通。

（可选）指定事件响应聊天频道

当您在响应计划中加入聊天频道时，响应者会通过该频道接收事件更新。他们可以使用聊天命令直接从聊天频道与事件互动。

使用 AWS Chatbot，您可以为 Slack 或 Amazon Chime 创建一个频道，以便在您的响应计划中使用。有关在 AWS Chatbot 中创建聊天频道的信息，请参阅《AWS Chatbot 管理员指南》。

> **Important**
>
> Incident Manager 必须有发布到聊天频道的 Amazon Simple Notification Service (Amazon SNS) 主题的权限。如果没有向 SNS 主题发布的权限，则无法将其添加到响应计划中。Incident Manager 向 SNS 主题发布测试通知，以验证权限。

有关聊天频道的更多信息，请参阅 在 Incident Manager 中使用聊天频道。

要指定事件响应聊天频道

1. 对于聊天频道，选择一个 AWS Chatbot 响应者在事件期间可以进行交流的聊天频道。

   > **Tip**
   >
   > 要在 AWS Chatbot 中创建新的聊天频道，请选择配置新的 Chatbot 客户端。

2. 对于聊天频道 SNS 主题，选择要在事件发生期间发布到的其他 SNS 话题。在多个 AWS 区域 中添加 SNS 主题可增加冗余，以防事件发生时某个区域瘫痪。
3. 继续选择在事件发生时需要联系的联系人、待命时间表和上报计划。

（可选）选择与事件响应互动的资源

在事件发生时，务必要确定最合适的响应者。我们建议您采取以下措施作为最佳实践：

1. 在上报计划中添加联系人和待命时间表作为上报渠道。
2. 选择上报计划作为响应计划的互动方式。

有关联系人和上报计划的更多信息，请参阅 在 Incident Manager 中使用联系人 和 在 Incident Manager 中使用上报计划。

要选择与事件响应互动的资源

1. 对于互动，选择任意数量的上报计划、待命时间表和个人联系人。
2. 继续选择性地指定一个运行手册，作为事件缓解措施的一部分来运行。

（可选）指定事件缓解措施的运行手册

您可以使用 AWS Systems Manager 的一项功能 AWS Systems Manager 自动化中的运行手册来自动执行 AWS Cloud 环境中的常见应用程序和基础设施任务。

每个运行手册都定义了运行手册工作流程。运行手册工作流程包括 Systems Manager 在托管式或其他 AWS 资源类型上执行的操作。在 Incident Manager 中，运行手册推动事件响应和缓解措施。

有关在响应计划中使用运行手册的更多信息，请参阅 在 Incident Manager 中使用 Systems Manager Automation 运行手册。

要指定事件缓解措施的运行手册：

1. 对于运行手册，请执行以下操作之一：

   - 选择从模板中克隆运行手册，复制默认的 Incident Manager 运行手册。在运行手册名称中，为新运行手册输入描述性名称。
   - 选择选择现有运行手册。选择要使用的所有者、运行手册和版本。

   > **Tip**
   >
   > 要从头开始创建运行手册，请选择配置新运行手册。
   > 有关创建运行手册的更多信息，请参阅 在 Incident Manager 中使用 Systems Manager Automation 运行手册。

2. 在参数区域中，提供所选运行手册所需的任何参数。

   可用的参数由运行手册指定。一个运行手册可能需要的参数可能与另一个运行手册不同。有些参数可能是必填参，而另一些则是可选参数。

   在许多情况下，您可以选择手动输入参数的静态值，例如 Amazon EC2 实例 ID 列表。您也可以让 Incident Manager 提供事件动态生成的参数值。

3. （可选）对于 AutomationAssumeRole，请指定要使用的 AWS Identity and Access Management(IAM) 角色。该角色必须具有运行手册中指定的各个命令所需的权限。

   > **Note**
   >
   > 如果未指定 `AssumeRole`，Incident Manager 会尝试使用运行手册服务角色来运行运行手册中指定的各个命令。

请从以下内容中选择：

- 输入 ARN 值——手动输入 AsmeRole 的 Amazon 资源名称(ARN)，格式为 `arn:aws:iam::account-id:role/assume-role-name`。例如，**`arn:aws:iam::123456789012:role/MyAssumeRole`**。
- 使用现有服务角色——从账户现有角色列表中选择一个具有所需权限的角色。
- 创建新服务角色——从 AWS 托管式策略中选择要附加到您的 AssumeRole 的策略。选择此选项后，对于 AWS 托管式策略，请从列表中选择一个或多个策略。

  您可以接受建议的新角色默认名称，也可以输入自己选择的名称。

> **Note**
>
> 该新运行手册的服务角色与您选择的特定运行手册相关联。它不能用于不同的运行手册。这是因为策略的资源部分不支持其他运行手册。

4. 对于运行手册的服务角色，指定要使用的 IAM 角色来提供访问和启动运行手册本身的工作流程所需的权限。

   至少，该角色必须允许对您的特定运行手册执行 `ssm:StartAutomationExecution` 操作。要使运行手册跨账户运行，该角色还必须允许您在 Incident Manager 中的跨区域和跨账户事件管理 期间创建的 `AWS-SystemsManager-AutomationExecutionRole` 角色执行 `sts:AssumeRole` 操作。

   请从以下内容中选择：

   - 创建新的服务角色——Incident Manager 为您创建一个运行手册的服务角色，其中包括启动运行手册工作流程所需的最低权限。

     对于角色名称，您可以接受建议的默认名称，也可以输入自己选择的名称。我们建议使用建议的名称或在名称中保留运行手册的名称。这是因为新的 AssumeRole 与您选择的特定运行手册相关联，可能不包括其他运行手册所需的权限。
   - 使用现有的服务角色——您或 Incident Manager 之前创建的 IAM 角色会授予所需的权限。

     在角色名称中，选择要使用的现有角色的名称。

5. 展开其他选项，然后选择以下选项之一，指定运行手册工作流程应在其中运行的 AWS 账户。

- 响应计划所有者的帐户——在创建运行手册工作流程的 AWS 账户 中启动运行手册工作流程。
- 受影响的帐户——在开始或报告事件的账户中启动运行手册工作流程。

  当您使用 Incident Manager 处理跨账户场景，且运行手册需要访问受影响的账户中的资源进行补救时，请选择受影响的账户。

6. 继续可选地将 PagerDuty 服务集成到响应计划中。

（可选）将 PagerDuty 服务纳入响应计划中

要将 PagerDuty 服务纳入响应计划中

当您将 Incident Manager 与 PagerDuty 集成时，每当 Incident Manager 创建事件时，PagerDuty 都会创建相应的事件。PagerDuty 中的事件除了使用 Incident Manager 中的策略外，还使用您在其中定义的寻呼工作流程和上报策略。PagerDuty 可将 Incident Manager 中的时间轴事件作为事件备注。

1. 展开第三方集成，然后选择启用 PagerDuty 集成复选框。
2. 在选择密钥中，在 AWS Secrets Manager 中选择存储 PagerDuty 账户访问凭证的密钥。

   有关将 PagerDuty 凭证存储在 Secrets Manager 密钥中的信息，请参阅 将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中。
3. 对于 PagerDuty 服务，请从您的 PagerDuty 账户中选择要在其中创建 PagerDuty 事件的服务。
4. 继续添加可选标签并创建响应计划。

添加标签并创建响应计划

要添加标签并创建响应计划

1. （可选）在标签 区域，将一个或多个标签密钥名称/值对应用到响应计划。

   标签是您分配给资源的可选元数据。通过标签，您可以按各种标准（如用途、所有者或环境）对资源进行分类。例如，您可能想要标记一个响应计划，以确定其旨在缓解的事件类型、所包含的上报渠道类型或与之相关的上报计划。有关标记 Incident Manager 资源的更多信息，请参阅 在 Incident Manager 中标记资源。
2. 选择创建响应计划。

在 Incident Manager 中处理调查发现

在 Incident Manager 中，调查发现是有关在事件发生前后发生的 AWS CodeDeploy 部署和 AWS CloudFormation 堆栈更新的信息，这些信息涉及一个或多个可能与事件相关的资源。可以将每项调查发现视为事件的潜在原因进行审查。有关这些潜在原因的信息已添加到事件的事件详细信息页面。由于有关这些部署和变更的信息随时可用，响应者无需手动搜索这些信息。这样可以减少评估潜在原因所需的时间，从而缩短从事件中恢复的平均时间 (MTTR)。

目前，Incident Manager 支持从两个方面收集调查发现 AWS 服务：AWS CodeDeploy 和 AWS CloudFormation。

调查发现是一项可选特征。您可以在做准备向导中启用它，也可以在首次加入 Incident Manager 时启用，也可以稍后在设置页面上启用。

启用调查发现特征后，Incident Manager 会为您创建一个服务角色。该服务角色包括从 CodeDeploy 和 CloudFormation 检索调查发现所需的权限。

要在跨账户场景中使用调查发现，请在管理账户中启用该特征。之后，AWS Resource Access Manager(AWS RAM) 组织中的每个应用程序帐户都必须创建相应的服务角色。

请参阅以下主题，可帮助您使用调查发现特征。

主题

为调查发现启用和创建服务角色

启用调查发现特征后，Incident Manager 会代表您创建一个名为 `IncidentManagerIncidentAccessServiceRole` 的服务角色。该服务角色提供 Incident Manager 所需的权限，用于收集有关事件创建前后发生的 CodeDeploy 部署和 CloudFormation 堆栈更新的信息。

> **Note**
>
> 如果您在组织中使用 Incident Manager，则服务角色将在管理帐户中创建。要使用组织中其他账户的调查发现，必须在每个应用程序账户中创建服务角色。有关使用 CloudFormation 模板在您的应用程序账户中创建此角色的信息，请参阅 设置和配置跨账户事件管理 中的步骤 4。

此服务角色与 AWS 托管式策略相关联。有关该策略中权限的信息，请参阅 AWS 托管策略：AWSIncidentManagerIncidentAccessServiceRolePolicy。

有关在 Incident Manager 引导过程中启用调查发现的信息，请参阅 开始使用 Incident Manager。

有关在完成引导过程后启用调查发现的信息，请参阅 管理调查发现特征。

配置支持跨账户调查发现的权限

要在 AWS RAM 中设置了组织的账户中使用调查发现特征，每个应用程序帐户都必须配置权限，让 Incident Manager 代表其代入管理账户的服务角色。

可以通过部署由 AWS 提供的 AWS CloudFormation 模板在应用程序账户中配置这些权限，该模板将创建角色 `IncidentManagerIncidentAccessServiceRole`。

有关在应用程序账户中下载和部署该模板的信息，请参阅 Incident Manager 中的跨区域和跨账户事件管理 中的步骤 4。

在 Incident Manager 中创建事件

Incident Manager 是一项 AWS Systems Manager 功能，可帮助您管理和快速响应事件。您可以配置 Amazon CloudWatch 和 Amazon EventBridge 以基于 CloudWatch 警报和 EventBridge 事件自动创建事件。您也可以在事件列表页面上手动创建事件，或者使用 AWS CLI 或 AWS SDK 中的 StartIncident API 操作来创建事件。Incident Manager 会将同一个 CloudWatch 警报或 EventBridge 事件创建的事件重复数据删除到同一个事件中。

对于 CloudWatch 警报或 EventBridge 事件自动创建的事件，Incident Manager 会尝试在与事件规则或警报相同的 AWS 区域 中创建事件。如果在 AWS 区域 中没有 Incident Manager，CloudWatch 或 EventBridge 会自动在复制集中指定的可用区域中创建事件。有关更多信息，请参阅 Incident Manager 中的跨区域和跨账户事件管理。

系统创建事件时，Incident Manager 会自动收集事件相关 AWS 资源的信息，并将这些信息添加到相关项目选项卡中。如果您在响应计划中指定了运行手册，当系统创建事件时，Incident Manager 就可以将事件中涉及的 AWS 资源信息发送到运行手册。然后，系统可以在启动运行手册并尝试修复问题时瞄准这些资源。

当系统创建事件时，它还会在 OpsCenter（System Manager 的组件）中创建父操作工作项 (OpsItem)，并将其作为相关项目链接到该事件。您可以使用该 OpsItem 跟踪相关工作和未来的事件分析。调用 OpsCenter 会产生费用。有关 OpsCenter 定价的更多信息，请参阅 Systems Manager 定价。

> **Important**
>
> 请注意以下重要详细信息。
>
> - 如果 Incident Manager 不可用，则只有当您在复制集中指定了至少两个区域时，系统才能进行失效转移并在其他 AWS 区域 中创建事件。有关配置复制集的信息，请参阅 开始使用 Incident Manager。
> - 跨区域失效转移创建的事件不会调用响应计划中指定的运行手册。

使用 CloudWatch 警报自动创建事件

CloudWatch 使用您的 CloudWatch 指标来提醒您环境中的变化，并自动执行启动事件操作。当警报进入警报状态时，CloudWatch 会与 Systems Manager 和 Incident Manager 合作，根据响应计划模板创建事件。这需要以下先决条件：

- 已配置 Incident Manager 并创建复制集。该步骤将在您的账户中创建 Incident Manager 服务关联角色，并提供必要的权限。
- 配置的 Incident Manager 响应计划。要了解如何配置 Incident Manager 响应计划，请参阅 在 Incident Manager 中使用响应计划 本指南的事件准备部分。
- 已配置 CloudWatch 指标监控您的应用程序。有关监控最佳实践，请参阅本指南的事件准备部分的监控。

要使用开始事件操作创建警报

1. 在 CloudWatch 中创建警报。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 Amazon CloudWatch 警报。
2. 选择要执行的警报操作时，请选择添加 Systems Manager 操作。
3. 选择创建事件，然后选择该事件的响应计划。
4. 完成所选警报类型指南中的其余步骤。

> **Tip**
>
> 您还可以将创建事件操作添加到任何现有警报中。

使用 EventBridge 事件自动创建事件

EventBridge 规则可观察事件模式。如果事件符合定义的模式，Incident Manager 就会使用所选的响应计划创建事件。

使用 SaaS 合作伙伴事件创建事件

您可以将 EventBridge 配置为接收来自软件即服务 (SaaS) 合作伙伴应用程序和服务的事件，从而实现第三方集成。将 EventBridge 配置为接收来自第三方合作伙伴的事件后，您可以创建与合作伙伴事件相匹配的规则来创建事件。要查看第三方集成列表，请参阅接收来自 SaaS 合作伙伴的事件。

将 EventBridge 配置为接收来自 SaaS 集成的事件。

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 在导航窗格中，选择合作伙伴事件源。

3. 使用搜索栏查找所需的合作伙伴，然后为该合作伙伴选择设置。
4. 选择复制，将您的账户 ID 复制到剪贴板。

> **Note**
>
> 要与 Salesforce 集成，请使用《Amazon AppFlow 用户指南》https://docs.aws.amazon.com/appflow/latest/userguide/EventBridge.html中描述的步骤。

5. 转到合作伙伴的网站，并按照说明创建合作伙伴事件源。对此操作使用您的账户 ID。您创建的事件源只能在您的账户中使用。
6. 返回 EventBridge 控制台，选择导航窗格中的合作伙伴事件源。
7. 选择合作伙伴事件源旁边的按钮，然后选择与事件总线关联。

创建可触发来自 SaaS 合作伙伴的事件的规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
5. 对于事件总线，请选择对应于该合作伙伴的事件总线。
6. 对于规则类型，选择具有事件模式的规则。
7. 选择下一步。
8. 对于事件源，选择 AWS 事件或 EventBridge 合作伙伴事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择EventBridge 合作伙伴
11. 对于合作伙伴，请选择合作伙伴的名称。
12. 对于事件类型，选择所有事件或选择要用于此规则的事件类型。如果您选择所有事件，此合作伙伴事件源发送的所有事件都将匹配规则。

    如果您希望自定义事件模式，请选择编辑，做出修改，然后选择保存。
13. 选择下一步。
14. 对于选择目标，选择 Incident Manager 响应计划，然后选择响应计划。

> **Note**
>
> 选择响应计划时，您拥有并已与您的账户共享的所有响应计划都会显示在响应计划下拉列表中。

15. EventBridge 可以创建运行规则所需的 IAM 角色：
    - 要自动创建 IAM 角色，请选择为此特定资源创建新角色。
    - 要使用您之前创建的 IAM 角色，请选择使用现有角色。
16. 选择下一步。
17. （可选）为规则输入一个或多个标签。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 标签。
18. 选择下一步。
19. 检查规则，然后选择创建规则。

使用 AWS 服务事件创建事件

EventBridge 还接收来自支持 AWS 服务事件中列出的 AWS 服务的事件。与为 SaaS 合作伙伴配置规则的方式类似，您也可以为 AWS 服务配置规则。

创建可触发 AWS 服务事件的规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
5. 对于事件总线，选择默认。
6. 对于规则类型，选择具有事件模式的规则。
7. 选择下一步。
8. 对于事件源，选择 AWS 事件或 EventBridge 合作伙伴事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择 AWS 服务。

11. 对于服务名称，选择监控事件的服务。
12. 对于事件类型，选择所有事件或选择要用于此规则的事件类型。如果您选择所有事件，此合作伙伴事件源发送的所有事件都将匹配规则。

    如果您希望自定义事件模式，请选择编辑，做出修改，然后选择保存。
13. 选择下一步。
14. 对于选择目标，选择 Incident Manager 响应计划，然后选择响应计划。

    > **Note**
    >
    > 选择响应计划时，您拥有并已与您的账户共享的所有响应计划都会显示在响应计划下拉列表中。

15. EventBridge 可以创建运行规则所需的 IAM 角色：

    - 要自动创建 IAM 角色，请选择为此特定资源创建新角色。
    - 要使用您之前创建的 IAM 角色，请选择使用现有角色。
16. 选择下一步。
17. （可选）为规则输入一个或多个标签。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 标签。
18. 选择下一步。
19. 检查规则，然后选择创建规则。

手动创建事件

响应者可以使用预定义的响应计划，使用 Incident Manager 控制台手动跟踪事件。请按照以下步骤创建事件。

1. 打开 Incident Manager 控制台。
2. 选择启动事件。
3. 对于响应计划，请从列表中选择一个响应计划。
4. （可选）要覆盖已定义的响应计划提供的标题，请输入事件标题。
5. （可选）要覆盖定义的响应计划提供的影响，请输入事件的影响。

在 Incident Manager 中跟踪事件

AWS Systems Manager Incident Manager 可跟踪事件从发现到解决的整个过程，并进行事后分析。您可以在 Incident Manager 控制台的事件列表页面上查找所有事件，其中包含直接指向事件详细信息的链接。

主题

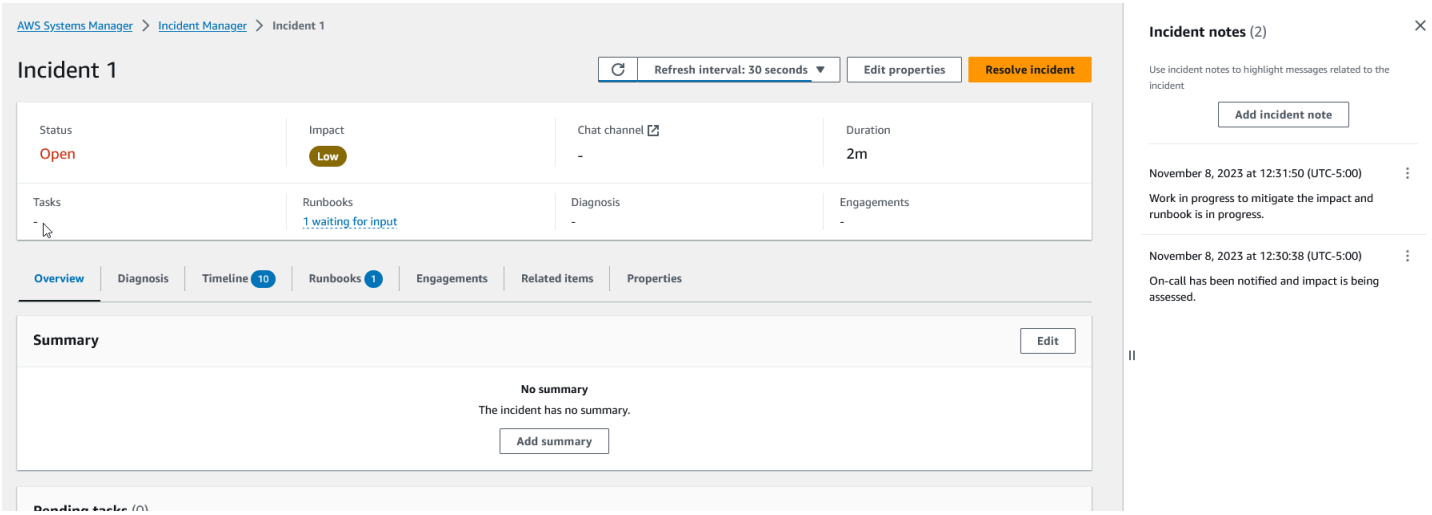
事件列表

事件列表页面包含三个部分：未解决的事件、已解决的事件和分析。您可以在该页面手动跟踪新事件并创建分析。要了解有关手动跟踪事件的更多信息，请参阅手动创建事件本指南的事件创建部分。要了解事后分析，请参阅本指南的 在 Incident Manager 中执行事件后分析 部分。

事件详细信息会以图块形式显示未解决的事件，其中包括该事件的标题、影响、持续时间和聊天频道。解决事件后，事件会移动到已解决事件列表中。分析位于第二个选项卡中。

事件详细信息

事件详细信息页面提供了可以用于管理事件的详细洞察力和工具。在此页面上，您可以启动运行手册以缓解事件，添加事件备注，与其他解决者互动，并查看事件详细信息，例如时间轴、指标、属性和相关资源。事件详细信息页面包括以下部分：顶部横幅、事件备注以及包含其他信息和资源的七个选项卡。默认情况下，所有事件详细信息页面都会显示顶部横幅和事件备注部分。



本主题说明了事件详细信息页面的元素以及您可以从该页面执行的操作。

顶部横幅

每个事件详细信息页面的顶部横幅都包含以下信息：

- 状态——事件的当前状态可以是未解决或已解决。
- 影响——事件对您的环境的影响。它可以是高、中和低。要更改事件的影响，请选择编辑属性。
- 聊天频道——访问聊天频道的链接，您可以在其中查看事件更新和通知。
- 持续时间——响应者解决事件之前经过的时间。
- 运行手册——与此事件相关的运行手册的状态。状态可以是等待输入、成功或失败。如果运行手册的状态是正在等待输入，则可以选择该运行手册来查看操作详细信息。您可以选择不成功来查看超时、故障或取消的运行手册。
- 参与度——互动总数和每次互动的状态。创建互动时，其状态为已互动。确认互动后，状态将从已互动更改为已确认。Incident Manager 不支持第三方互动的确认。此类互动仍处于已互动状态。

您可以通过选择横幅右上角的编辑来编辑事件标题、影响和聊天频道。

事件备注

屏幕右侧显示事件备注部分。使用备注，您可以与其他处理事件的用户进行协作和沟通。您可以解释所采用的缓解措施、所发现的潜在根本原因或事件的当前状态。最佳实践是，使用事件备注部分发布状态更新以及您或其他人对事件采取的行动。如果您需要与其他解决者进行实时沟通，请使用 Incident Manager 中提供的聊天频道。

要添加备注，请选择添加事件备注按钮，然后输入您的备注。备注可以包含有关事件状态的更新或任何其他向其他用户提供可见性的相关信息。如果需要，您还可以编辑或删除事件备注。

> **Note**
>
> 任何拥有运行 `ssm-incidents:UpdateTimelineEvent` 和 `ssm-incidents:DeleteTimelineEvent` 操作的 IAM 权限的用户都可以编辑和删除备注。但是，当您与其他账户共享事件时，资源策略不包括 `ssm-incidents:DeleteTimelineEvent` 操作。这样可以防止与您共享事件的用户删除备注。您可以在 AWS CloudTrail 控制台中查看 Incident Manager 事件中备注的审计跟踪记录。

选项卡

事件详细信息页面有七个选项卡，方便响应者在事件发生时查找和查看信息。选项卡名称中显示一个计数器，表示该选项卡的更新次数。有关各选项卡内容和可用操作的更多信息，请继续阅读。

概述

概述选项卡是响应者的登录页面。它包含事件摘要、最近的时间轴事件列表和当前运行手册步骤。

响应者使用摘要来了解已采取的行动、任何变更的结果、可能的后续步骤以及有关事件影响的信息。要更新摘要，请选择摘要部分右上角的编辑。

> **Important**
>
> 如果多个响应者同时编辑摘要字段，则最后提交编辑内容的响应者将覆盖所有其他输入。

最近的时间轴事件部分包含 Incident Manager 填充的时间轴，其中包含五个最新的事件。利用这一部分了解事件的状态和最近发生的情况。要查看完整的时间轴，请继续进入时间轴选项卡。

概述页面还显示当前运行手册步骤。该步骤可能是在 AWS 环境中自动运行的步骤，也可能是一组针对响应者的手动指令。要查看完整的运行手册，包括之前和接下来的步骤，请选择运行手册选项卡。

诊断

诊断选项卡包含有关您的 AWS 托管应用程序和系统的重要信息，包括有关指标的信息以及调查发现（如果启用）。

使用指标

Incident Manager 使用 Amazon CloudWatch 填充该选项卡上的指标和警报图。要了解有关定义警报和指标的事件管理最佳实践的更多信息，请参阅 监控 本用户指南的事件计划部分。

要添加指标

- 选择该选项卡右上角的添加。
  - 要从现有 CloudWatch 控制面板添加指标，请选择来自现有 CloudWatch 控制面板。
    a. 选择控制面板。这会添加所选控制面板中的所有指标和警报。
    b. （可选）您也可以从控制面板中选择指标来查看特定指标。

- 通过选择来自 CloudWatch 并粘贴指标来源添加单个指标。要复制指标来源：

  a. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
  b. 在导航窗格中，请选择指标。
  c. 在全部指标选项卡上的搜索字段中，输入搜索词（例如，指标名称或资源名称），然后选择输入。

     例如，如果您搜索`CPUUtilization`指标，则将显示具有该指标的关联命名空间和维度。
  d. 选择一个搜索结果，查看指标。
  e. 选择来源选项卡并复制来源。

指标警报图只能通过相关的响应计划添加到事件详细信息中，或者在添加指标时选择来自现有 CloudWatch 控制面板。

要删除指标，请选择删除，然后从提供的指标下拉列表中选择要删除的指标。

查看 AWS CodeDeploy 和 AWS CloudFormation 的调查发现

启用调查发现并配置所有必要权限后，任何可能与特定事件相关的调查发现都会附加到该事件中。响应者可以在事件详细信息页面上查看有关这些调查发现的信息。

要查看 CodeDeploy 和 CloudFormation 的调查发现

1. 打开 Incident Manager 控制台。
2. 选择要调查的事件名称。
3. 在诊断选项卡的调查发现区域中，将任何报告的调查发现的开始时间与事件的开始时间进行比较。
4. 要查看有关某项调查发现的更多详细信息，请在参考列中，选择 CodeDeploy 或 CloudFormation 调查发现的链接。

时间轴

使用时间轴选项卡跟踪事件期间发生的事件。Incident Manager 会自动填充时间轴事件，以识别事件期间发生的重大事件。响应者可以根据手动检测到的事件添加自定义事件。在事后分析期间，时间轴选项卡提供了有关如何更好地准备和响应未来的事件的宝贵洞察力。有关事后分析的更多信息，请参阅 在 Incident Manager 中执行事件后分析。

要添加自定义时间轴事件，请选择添加。使用日历选择日期，然后输入时间。所有时间都采用您的本地时区。提供在时间轴上显示的事件的简要说明。

要编辑现有的自定义事件，请在时间轴上选择该事件，然后选择编辑。您可以更改自定义事件的时间、日期和描述。您只能编辑自定义事件。

运行手册

响应者可以在事件详细信息页面的运行手册选项卡中查看运行手册步骤并启动新的运行手册。

要启动新的运行手册，请在运行手册部分中选择启动运行手册。使用搜索字段查找要启动的运行手册。提供启动运行手册时要使用的所有必需参数和运行手册的版本。在事件发生期间从运行手册选项卡启动的运行手册使用当前登录账户的权限。

要在 Systems Manager 中导航到运行手册定义，请在运行手册下选择运行手册的标题。要在 Systems Manager 中导航到运行手册的运行实例，请在执行详细信息下选择执行详细信息。这些页面显示了用于启动运行手册的模板，以及当前运行的自动化文档实例的具体详细信息。

运行手册步骤部分显示了所选运行手册自动执行或响应者手动执行的步骤列表。这些步骤会随着其成为当前步骤而展开，显示完成该步骤所需的信息或有关该步骤操作的详细信息。自动运行手册步骤在自动化完成后解析。手动步骤要求响应者在每个步骤的底部选择下一步。步骤完成后，步骤输出将显示为下拉菜单。

要取消运行手册的执行，请选择取消运行手册。这将停止运行手册的执行，并且不会完成运行手册中的任何其他步骤。

互动

事件详细信息的互动选项卡推动了响应者和团队的互动。在该选项卡中，您可以看到与谁互动，谁已响应，以及哪些响应者将作为上报计划的一部分互动。响应者可以直接通过该选项卡与其他联系人互动。要了解有关创建联系人和上报计划的更多信息，请参阅本指南的 在 Incident Manager 中使用联系人 和 在 Incident Manager 中使用上报计划 部分。

您可以配置包含联系人和上报计划的响应计划，以便在事件开始时自动开始互动。要了解有关配置响应计划的更多信息，请参阅本指南的 在 Incident Manager 中使用响应计划 部分。

您可以在表格中查找有关每个联系人的信息。该表格包含以下信息：

- 名称——指向显示联系方式和互动计划的联系人详细信息页面的链接。
- 上报计划——指向与联系人互动的上报计划的链接。

- 联系人来源——标识与该联系人互动的服务，例如 AWS Systems Manager 或 PagerDuty。
- 已互动——显示计划何时与联系人互动，或何时作为上报计划的一部分与联系人互动。
- 已确认——显示联系人是否已确认互动。

要确认互动，响应者可以执行下列操作之一：

- 电话呼叫——出现提示时输入 **1**。
- 短信——使用提供的代码回复消息，或在事件的互动选项卡上输入提供的代码。
- 电子邮件——在事件的互动选项卡上输入提供的代码。

相关术语

相关项目选项卡用于收集与事件缓解相关的资源。这些资源可以是 ARN、外部资源链接或上传到 Amazon S3 存储桶的文件。该表显示描述性标题以及 ARN、链接或存储桶详细信息。在使用 S3 存储桶之前，请查看《Amazon S3 用户指南》中的 Amazon S3 安全最佳实践。

将文件上传到 Amazon S3 存储桶时，该存储桶上的版本控制要么已启用，要么已暂停。在存储桶上启用版本控制后，上传的文件如果与现有文件同名，就会被添加为该文件的新版本。如果暂停版本控制，上传的文件如果与现有文件同名，就会覆盖现有文件。要了解有关版本控制的更多信息，请参阅《Amazon S3 用户指南》中的在 S3 存储桶中使用版本控制。

删除文件相关项目时，该文件会从事件中删除，但不会从 Amazon S3 存储桶中删除。要了解有关从 Amazon S3 存储桶中删除对象的更多信息，请参阅《Amazon S3 用户指南》中的删除 Amazon S3 对象。

属性

属性选项卡提供了有关事件的以下详细信息。

在事件属性部分，您可以查看以下内容：

- 状态——描述事件的当前状态。事件可以是未解决或 已解决。
- 开始时间——在 Incident Manager 中创建事件的时间。
- 解决时间——在 Incident Manager 中解决事件的时间。
- Amazon 资源名称（ARN）——事件的 ARN。通过聊天或使用 AWS Command Line Interface (AWS CLI) 命令引用事件时，请使用 ARN。
- 响应计划——确定所选事件的响应计划。选择响应计划会打开响应计划的详细信息页面。

- 父项 OpsItem——将创建的 OpsItem 标识为事件的父项。父项 OpsItem 可以有多个相关事件和后续操作项目。选择父项 OpsItem 会在 OpsCenter 中打开 OpsItems 详细信息页面。
- 分析——标识根据此事件创建的分析。根据已解决的事件创建分析，以改进您的事件响应流程。选择分析以打开分析详细信息页面。
- 所有者——创建事件的账户。

在标签部分，您可以查看和编辑与事件记录关联的标签密钥和值。有关 Incident Manager 中标签的更多信息，请参阅 在 Incident Manager 中标记资源。

在 Incident Manager 中执行事件后分析

事件后分析将指导您确定事件响应的改进措施，包括检测和缓解时间。分析还可以帮助您了解事件的根本原因。Incident Manager 会创建建议的操作项目，以改善您的事件响应。

事件后分析的好处

- 改进事件响应
- 了解问题的根本原因
- 使用可交付的措施项解决根本原因
- 分析事件的影响
- 在组织内收集和分享学习成果

哪些情况不能进行分析

分析不会指责任何人，也不会提出任何人的姓名。

“无论我们发现了什么，我们都理解并真正相信，每个人都尽了自己最大的努力，考虑到了他们当时所知道的情况、他们的技能和能力、可用的资源以及当时的情况。” ——Norm Kerth，《项目回顾：团队审查手册》

分析详细信息

分析详细信息页面可指导您收集信息、评估改进措施和创建行动项目。分析详细信息页面与事件详细信息类似，但有一些主要区别，例如历史指标、可编辑的时间轴以及改进未来事件的问题。

概述

概述是事件的摘要。该摘要包括背景、发生了什么、为什么发生、如何缓解、持续时间以及防止事件再次发生的关键行动项目。概述是高层次的。您将在分析的问题选项卡中浏览更多详细信息。

指标

使用指标选项卡可视化事件持续时间内应用程序中的密钥指标。您可以在此添加指标图表，在同一图表中描述一个或多个指标。事件期间使用的指标会自动填入在该选项卡上。我们建议您在事件发生期间添加描述、标题和关键时间点的注释。

在分析指标图表时可以考虑的一些关键时间点：

- 部署变更
- 配置更改
- 事件开始时间
- 警报时间
- 互动时间
- 缓解开始时间
- 事件解决时间

限制

- CloudWatch 警报和指标表达式不会从事件中导入。
- Incident Manager 不支持的区域中的指标不会从事件中导入。
- 应用程序账户中的指标要求在创建分析之前配置 `CloudWatch-CrossAccountSharingRole`。有关该角色的更多信息，请参阅《CloudWatch 用户指南》中的跨账户跨区域 CloudWatch 控制台。

时间轴

在深入了解事件时，请描述时间轴上的关键时间点。事件时间轴会自动填入该选项卡。您可以删除与分析无关的时间点。您还可以添加和编辑时间点，以便更准确地描述事件及其影响。

使用时间轴选项卡回答您在问题选项卡上查找的有关事件响应的问题。

问题

使用 Incident Manager 问题可缩短解决应用程序中事件的时间，并减少事件的发生。回答问题时，请更新指标和时间轴选项卡以确保准确性。这些问题侧重于事件响应的以下关键方面：

- 检测——您能否缩短检测时间？ 是否更新了可以更快地检测到事件的指标和警报？
- 诊断——您能否缩短诊断时间？ 您的响应计划或上报计划是否有更新，可以更快地与正确的响应者进行互动？
- 缓解——您能否缩短缓解时间？ 是否有可以添加或改进的运行手册步骤？
- 预防——您能否防止未来事件的发生？ 为了发现事件的根本原因，Amazon 在问题调查中采用了“5 个为什么”的方法。

操作

Incident Manager 会创建建议的操作项目供您在完成问题时查看。您可以选择通过该选项卡接受并完成这些操作，也可以取消这些操作。您可以通过选择已撤销的措施项目来查看已撤销的措施项目。操作项目是一种与 OpsCenter 中的分析和事件相关联的 OpsItem。

清单

在结束分析之前，请使用清单查看响应者应采取的操作。当响应者完成清单中的操作时，操作旁边的图标会从省略号变为复选标记，表示操作已完成。如果您尚未完成清单项目，Incident Manager 会显示一条消息，确认响应者希望在不完成分析的情况下关闭分析。

分析模板

分析模板提供了一组问题，深入探讨了事件的根本原因。您可以使用这些问题的答案来改善应用程序性能和事件响应。

AWS 标准模板

Incident Manager 提供了一个基于 AWS 事件响应和问题分析最佳实践的标准问题模板，标题为 `AWSIncidents-PostIncidentAnalysisTemplate`。

创建分析模板

我们鼓励您使用默认 `AWSIncidents-PostIncidentAnalysisTemplate` 模板并添加适合您的用例的其他问题或部分。基于默认模板创建分析模板使用该模板作为起点在管理账户中创建分析模板。然后，您可以将分析模板复制到启用 Incident Manager 的每个区域。

创建分析模板

1. 调用 `GetDocument` 操作并使用其 `Name` 参数下载 `AWSIncidents-PostIncidentAnalysisTemplate`。有关 `GetDocument` 语法的更多信息，请参阅 Systems Manager API 参考。
2. 响应中的内容包含用于分析的 JSON 构建块。使用问题构建块在分析中插入其他问题。我们建议您在 `Incident questions` 部分添加问题或章节。
3. 要创建新模板，请使用上一步中更新的 JSON 的 `CreateDocument` 操作。您必须包括以下内容，其中 *`Analysis_Template_Name`* 是您的模板的名称，

   - `DocumentFormat: "JSON"`

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

创建分析。

1. 要创建分析，请从已关闭事件的事件详细信息页面中选择创建分析。
2. 选择用于创建该分析的分析模板，然后输入分析的描述性名称。
3. 选择创建。

打印格式化的事件分析

您可以生成一份格式适合打印的完整或不完整分析副本。您也可以将此副本另存为 PDF。您可以一次打印一个分析。当前不支持批量打印多个分析。

要打印格式化分析

1. 打开 Incident Manager 控制台。
2. 选择分析选项卡。
3. 选择要打印的分析标题。
4. 在分析详细信息页面的右上角，选择打印。
5. 在打印事件分析对话框中，清除不想包含在打印版本中的分析部分。默认情况下，所有部分都处于选中状态。
6. 选择打印以打开设备的本地打印控件。
7. 选择您的打印目的地或格式。您可以选择本地或网络打印机，也可以将分析结果保存为 PDF。如果需要，可以对剩余的打印选项进行任何更改，然后选择打印。

> **Note**
>
> 本地打印控件是指您的网络浏览器和设备提供的用户界面。
> 打印目的地是针对您的设备配置并可从您的设备访问的目的地。

Incident Manager 教程

这些 AWS Systems Manager 事件管理器教程可帮助您构建更强大的事件管理系统。这些教程涵盖了在事件或支持事件响应期间发生的常见活动。

主题

将 Systems Manager Automation 运行手册与 Incident Manager 一起使用

您可以使用AWS Systems Manager 自动化运行手册来简化 AWS 服务的常见维护、部署和修复任务。在本教程中，您将创建一个自定义运行手册，以便在 Incident Manager 中自动执行事件响应。本教程的场景涉及分配给 Amazon EC2 指标的亚马逊 CloudWatch 警报。当实例进入触发警报的状态时，Incident Manager 会自动执行以下任务：

1. 在 Incident Manager 中创建事件。
2. 启动尝试修复问题的运行手册。
3. 将运行手册结果发布到 Incident Manager 中的事件详细信息页面。

本教程中描述的过程也可以用于 Amazon EventBridge 事件和其他类型的 AWS 资源。通过自动对警报和事件进行修复响应，您可以减少事件对组织及其资源的影响。

本教程介绍如何编辑为事件管理器响应计划分配给 Amazon EC2 实例的 CloudWatch 警报。如果您没有配置警报、实例或响应计划，我们建议您在开始之前配置这些资源。有关更多信息，请参阅以下主题：

- 使用亚马逊 CloudWatch 用户指南中的亚马逊 CloudWatch 警报
- 亚马逊 EC2 用户指南中的亚马逊 EC2 实例
- 亚马逊 EC2 用户指南中的亚马逊 EC2 实例
- 在 Incident Manager 中使用响应计划

> **Important**
>
> 创建 AWS 资源和使用运行手册自动化步骤将产生成本。有关更多信息，请参阅AWS 定价。

主题

任务 1：创建运行手册

使用以下步骤在 Systems Manager 控制台中创建运行手册。当从 Incident Manager 事件中调用时，运行手册会重新启动 Amazon EC2 实例，并使用有关运行手册执行的信息更新事件。在开始之前，请确认您拥有创建运行手册的权限。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的设置自动化。

> **Important**
>
> 查看以下有关创建本教程运行手册的重要详细信息：
>
> - 该运行手册适用于由 CloudWatch 警报源创建的事件。如果您将该运行手册用于其他类型的事件，例如手动创建的事件，则无法找到第一个运行手册步骤中的时间轴事件，系统会返回错误信息。
> - 运行手册要求 CloudWatch 警报包含一个名`InstanceId`为的维度。Amazon EC2 实例指标的警报具有该维度。如果您将此运行手册与其他指标（或其他事件源，例如 EventBridge）一起使用，则必须更改`JsonDecode2`步骤以匹配在您的场景中捕获的数据。
> - 运行手册会尝试通过重启 Amazon EC2 实例来修复触发警报的问题。对于真实事件，您可能不想重启实例。使用您希望系统采取的特定修复措施更新运行手册。

有关创建运行手册的更多信息，请参阅《AWS Systems Manager 用户指南》中的使用运行手册。

要创建运行手册

1. 打开 AWS Systems Manager 控制台，网址为 https://console.aws.amazon.com/systems-manager/。
2. 在导航窗格中，选择文档。
3. 选择自动化。
4. 对于名称，为运行手册输入一个描述性名称，例如 **IncidentResponseRunbook**。
5. 选择编辑器选项卡，然后选择编辑。
6. 将以下内容粘贴到编辑器中：

```
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. 选择创建自动化。

任务 2：创建 IAM 角色

使用以下教程创建一个 AWS Identity and Access Management (IAM) 角色，该角色向事件管理员授予启动响应计划中指定的 Runbook 的权限。本教程中的运行手册会重新启动 Amazon EC2 实例。当您将运行手册连接到您的响应计划时，您将在下一个任务中指定该 IAM 角色。

创建一个 IAM 角色，从响应计划启动运行手册

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 确保在AWS 受信任实体的类型下选择了服务。
4. 在用例下的其他 AWS 服务的用案字段中，输入 **`Incident Manager`**。
5. 选择 Incident Manager，然后选择下一步。
6. 在添加权限页面上，选择创建策略。权限编辑器将在新的浏览器窗口或选项卡中打开。
7. 在编辑器中，选择 JSON 选项卡。
8. 将以下权限策略复制并粘贴到 JSON 编辑器中。将 *`account_ID`* 替换为您的 AWS 账户 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. 选择下一步：标签。
10. （可选）如果需要，在您的策略中添加标签。
11. 选择下一步：查看。
12. 在名称字段中，输入一个可以帮助您识别本教程使用的角色的名称。
13. （可选）在描述字段中，输入描述。
14. 选择创建策略。
15. 返回您正在创建的角色的浏览器窗口或选项卡。显示添加权限页面。
16. 选择刷新按钮（位于创建策略按钮旁边），然后在筛选框中输入您创建的权限策略的名称。
17. 选择您创建的权限策略，然后选择下一步。
18. 在名称、查看和创建页面的角色名称中，输入一个有助于您识别本教程使用的角色的名称。

19. （可选）在描述字段中，输入描述。
20. 查看角色详细信息，必要时添加标签，然后选择创建角色。

任务 3：将运行手册与您的响应计划关联起来

通过将运行手册连接到您的 Incident Manager 响应计划，可以确保一致、可重复和及时的缓解流程。运行手册还是解决者决定下一步行动的起点。

要将运行手册分配给响应计划

1. 打开 Incident Manager 控制台。
2. 选择响应计划。
3. 对于响应计划，选择现有的响应计划并选择编辑。如果您没有现有的响应计划，请选择创建响应计划来创建新计划。

   填写以下字段：

   a. 在运行手册部分，选择选择现有运行手册。
   b. 对于所有者，确认已选择我拥有。
   c. 对于运行手册，选择您在 任务 1：创建运行手册 中创建的运行手册。
   d. 对于版本，选择在执行时默认。
   e. 在输入部分，对于 IncidentRecordArn 参数，选择事件 ARN。
   f. 在执行权限部分，选择您在 任务 2：创建 IAM 角色 中创建的 IAM 角色。
4. 保存您的更改。

任务 4：为响应计划分配 CloudWatch 警报

使用以下步骤将 Amazon EC2 实例的 CloudWatch 警报分配给您的响应计划。

为您的响应计划分配 CloudWatch 警报

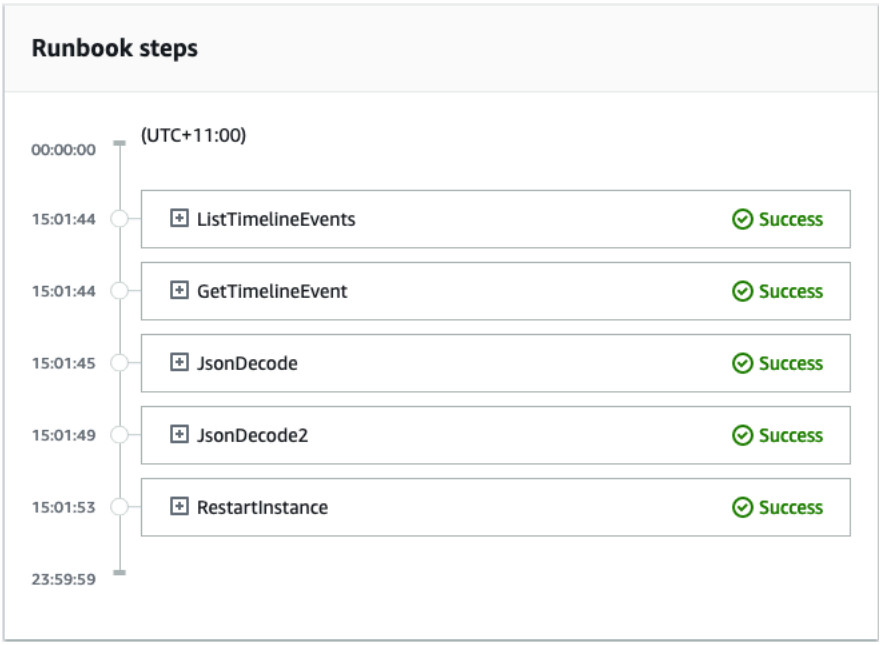
1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中的警报下，选择所有警报。
3. 选择适用于您要连接到响应计划的 Amazon EC2 实例的警报。
4. 选择操作，然后选择编辑。验证该指标是否有一个名为 `InstanceId` 的维度。

5. 选择下一步。
6. 对于配置操作向导，选择添加 Systems Manager 操作。
7. 选择创建事件。
8. 选择您在 任务 3：将运行手册与您的响应计划关联起来 中创建的响应计划。
9. 选择更新警报。

任务 5：验证结果

要验证 CloudWatch 警报是否创建了事件，然后处理了响应计划中指定的运行手册，您必须触发警报。触发警报且运行手册处理完毕后，您可以使用以下步骤验证运行手册的结果。有关触发警报的信息，请参阅《AWS CLI 命令参考》中的 set-alarm-state。

1. 打开 Incident Manager 控制台。
2. 选择 CloudWatch 警报造成的事件。
3. 选择运行手册选项卡。
4. 在运行手册步骤部分中查看在您的 Amazon EC2 实例上执行的操作。下图的示例显示了您在本教程中创建的运行手册所采取的步骤。每个步骤都列出了时间戳和状态消息。



要查看 CloudWatch 警报中的所有详细信息，请展开 JsonDecode2 步骤，然后展开 O utput。

> **Important**
>
> 您必须清理在本教程中实施的所有不想保留的资源更改。这包括对事件管理器资源（例如资源计划和事件）的更改、 CloudWatch 警报的更改以及您为本教程创建的 IAM 角色。

在 Incident Manager 中管理安全事件

您可以同时使用 AWS Security Hub Amazon EventBridge 和 Incident Manager 来识别和管理 AWS 托管应用程序中的安全事件。本教程将引导您配置一条 EventBridge 规则，该规则将基于 Security Hub 自动发送的发现结果创建事件。

> **Note**
>
> 本教程使用 S EventBridge ecurity Hub。您可能会因使用这些服务而产生费用。

先决条件

- 设置 Security Hub。有关更多信息，请参阅设置 AWS Security Hub。
- 在 Security Hub 中创建或更新调查发现。有关更多信息，请参阅AWS Security Hub中的调查发现。
- 配置响应计划，以便 Incident Manager 在创建安全事件时将其用作模板。有关更多信息，请参阅 在 Incident Manager 中为事件做准备。

在本教程中，我们使用预定义的模式来创建 EventBridge 规则。要使用自定义模式创建规则，请参阅 AWS Security Hub 用户指南中的使用自定义模式创建规则。

创建 EventBridge 规则

1. 打开亚马逊 EventBridge 控制台，网址为 https://console.aws.amazon.com/events/。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
5. 对于事件总线，选择默认。
6. 对于规则类型，选择具有事件模式的规则。

7. 选择下一步。
8. 对于事件来源，选择AWS 事件或 EventBridge合作伙伴事件。
9. 对于事件模式，选择事件模式表。
10. 对于事件源，选择AWS 服务。
11. 对于AWS 服务，选择 Security Hub。
12. 对于事件类型，选择 Security Hub 调查发现——已导入。
13. 默认情况下， EventBridge 配置不带任何筛选值的事件模式。对于每个属性，将选择任意####选项。更新这些筛选器，以便根据对您的环境影响最大的安全调查发现创建事件。
14. 单击下一步。
15. 对于目标类型，选择AWS 服务。
16. 对于选择目标，选择 Incident Manager 响应计划。
17. 对于响应计划，选择一个响应计划，作为已创建事件的模板。
18. EventBridge 可以创建规则运行所需的 IAM 角色。
    - 要自动创建 IAM 角色，请选择为此特定资源创建新角色。
    - 要使用账户中已存在的 IAM 角色，请选择 使用现有角色。
19. （可选）为规则输入一个或多个标签。
20. 选择下一步。
21. 查看规则详细信息并选择创建规则。

既然您已经创建了此 EventBridge 规则，那么与您定义的属性值相匹配的安全发现将在事件管理器中创建事件。您可以对这些事件进行分类、管理、监控并创建事件后分析。

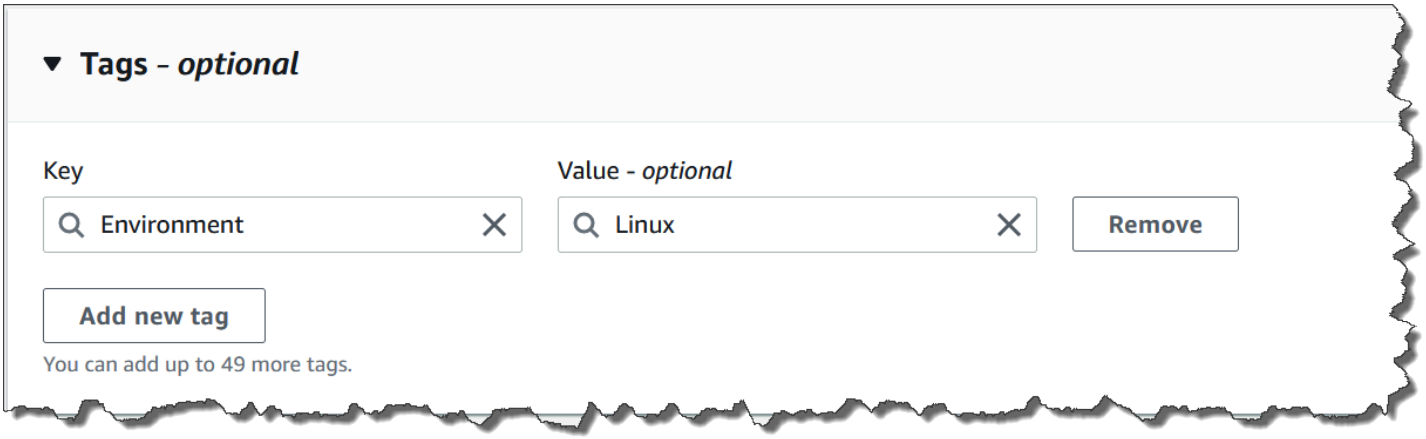
在 Incident Manager 中标记资源

标签是可选的元数据，您可以将其分配给复制集中指定的 AWS 区域 中的 Incident Manager 资源。您可以为响应计划、事件记录和联系人分配标签。您还可以为待命时间表和轮换添加标签。您还可以为复制集本身添加标签。标签使您能够以不同方式对这些资源的访问进行分类和控制。每个标签都包含定义的一个密钥和一个可选值。我们建议您为每种 Incident Manager 资源类型设计一套符合需求的标签密钥。使用一组连续的标签密钥，可以让您更轻松地管理这些资源并管理对它们的访问。您可以根据标签搜索和筛选资源。有关使用标签控制资源访问的更多信息，请参阅《IAM 用户指南》中的使用标签来控制对 AWS 资源的访问。

创建响应计划时，您可以在事件默认设置部分指定标签。使用响应计划创建事件时，这些标签会应用到事件记录中。

> **Note**
>
> 标签没有任何语义含义。标签严格按字符串进行解释。

您可以使用 Incident Manager 控制台添加或删除标签。以下屏幕截图显示了创建新响应计划时的标签部分。



要以编程方式处理标签，请使用以下 API 操作：

- TagResource
- UntagResource
- ListTagsForResource

Important

只有资源所有者账户才能查看和修改应用于响应计划、事件记录、联系人、待命时间表和轮换以及复制集的标签。

安全性 AWS Systems Manager Incident Manager

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方 AWS 的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云 AWS 服务 中运行的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS Systems Manager Incident Manager，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括数据的敏感性、公司的要求以及适用的法律法规。

此文档有助于了解如何在使用 Incident Manager 时应用责任共担模式。以下主题说明如何配置 Incident Manager，实现安全性和合规性目标。您还将学习如何使用其他 AWS 服务 方法来监控和保护您的事件管理器资源。

主题

Incident Manager 中的数据保护

分 AWS 担责任模型适用于中的数据保护 AWS Systems Manager Incident Manager。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参

阅数据隐私FAQ。 有关欧洲数据保护的信息，请参阅责任AWS 共担模型和AWS安全GDPR博客上的博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭据并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用SSL/TLS与 AWS 资源通信。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或访问时需要 FIPS 140-3 经过验证的加密模块API，请使用端点。FIPS有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API AWS CLI、或与事件管理器或其他人合作的情况 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

默认情况下，事件管理器使用SSL/TLS对传输中的数据进行加密。

数据加密

事件管理器使用 AWS Key Management Service (AWS KMS) 密钥加密您的事件管理器资源。有关的更多信息 AWS KMS，请参阅《AWS KMS 开发人员指南》。 AWS KMS 将安全、高度可用的硬件和软件相结合，提供可扩展到云端的密钥管理系统。事件管理器使用您指定的密钥加密您的数据，并使用 AWS 自有密钥加密元数据。要使用 Incident Manager，您必须设置复制集，其中包括设置加密。Incident Manager 需要数据加密才能使用。

您可以使用 AWS 自有密钥来加密您的复制集，也可以使用您在中创建的自己的客户托管密钥 AWS KMS 来加密复制集中的区域。事件管理器仅支持对称加密 AWS KMS 密钥来加密您在其中创建的数据。 AWS KMS事件管理器不支持带有导入 AWS KMS 密钥材料的密钥、自定义密钥存储库、基于哈希的消息身份验证码 (HMAC) 或其他类型的密钥。如果您使用客户托管密钥，则可以使用AWS KMS控制台或 AWS KMS APIs集中创建客户托管密钥，并定义控制事件经理如何使用客户托管密钥的密钥

策略。当您使用客户托管密钥通过 Incident Manager 进行加密时， AWS KMS 客户托管密钥必须与资源位于同一区域。要了解有关在 Incident Manager 中设置数据加密的更多信息，请参阅 准备向导。

使用 AWS KMS 客户托管密钥需要支付额外费用。有关更多信息，请参阅《AWS Key Management Service 开发者指南》中的AWS KMS 概念-KMS 密钥和AWS KMS 定价。

> **Important**
>
> 如果您使用客户管理的密钥 (CMK) 来加密您的复制集和 Incident Manager 数据，但后来决定删除该复制集，请确保在禁用或删除复制集之前删除该复制集CMK。

要允许 Incident Manager 使用客户自主管理型密钥来加密数据，您必须在客户自主管理型密钥的密钥策略中添加以下策略声明。要了解有关在账户中设置和更改密钥策略的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的在 AWS KMS中使用密钥策略。该策略提供了以下权限：

- 允许事件管理器执行只读操作，以便在您的账户中查找事件管理器。 CMK
- 允许 Incident Manager 使用CMK来创建授权和描述密钥，但前提是它代表账户中有权使用 Incident Manager 的委托人行事。如果策略声明中指定的委托人无权使用KMS密钥和使用事件管理器，则即使呼叫来自事件管理器服务，呼叫也会失败。

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

```
    }
```

将该Principal值替换为创建复制集IAM的主体。

事件管理器在加密操作的所有请求中都使用加密上下文。 AWS KMS 您可以使用此加密上下文来识别 Incident Manager 使用您的KMS密钥的 CloudTrail 日志事件。Incident Manager 使用以下加密上下文：

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

适用于 Identity and Access 管理 AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用事件管理器资源。IAM无需支付额外费用即可使用。 AWS 服务

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS Systems Manager Incident Manager 如何使用 IAM
- 适用于 AWS Systems Manager Incident Manager的基于身份的策略示例
- 基于资源的策略示例 AWS Systems Manager Incident Manager
- 防止 Incident Manager 中的跨服务混淆代理
- 使用 Incident Manager 的服务相关角色
- AWS 的托管策略 AWS Systems Manager Incident Manager
- 对 AWS Systems Manager Incident Manager 身份和访问进行故障排除

受众

使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于您在事件管理器中所做的工作。

服务用户——如果您使用 Incident Manager 服务来完成任务，则管理员会提供所需的凭证和权限。当您使用更多 Incident Manager 特征来完成工作时，可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Incident Manager 中的特征，请参阅 对 AWS Systems Manager Incident Manager 身份和访问进行故障排除。

服务管理员——如果您是公司 Incident Manager 器资源的负责人，则可能拥有对 Incident Manager 的完全访问权限。您有责任确定服务用户应该访问哪些 Incident Manager 的特征和资源。然后，您必须向IAM管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM使用事件管理器，请参阅AWS Systems Manager Incident Manager 如何使用 IAM。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写策略来管理对事件管理器的访问权限。要查看可在中使用的 Incident Manager 基于身份的策略示例IAM，请参阅。适用于 AWS Systems Manager Incident Manager的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户、IAM用户身份或通过担任IAM角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM身份中心）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员之前使用IAM角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅IAM用户指南中的签署 AWS API请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅用户指南中的多重身份验证和AWS IAM Identity Center 用户指南 AWS中的使用多因素身份验证 (MFA)。IAM

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用

户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM任务”。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 Ident IAM ity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关IAM身份中心的信息，请参阅什么是IAM身份中心？ 在《AWS IAM Identity Center 用户指南》中。

IAM 用户和组

IAM用户是您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的定期轮换需要长期凭证的用例的访问密钥。

IAM群组是指定IAM用户集合的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并授予该群组管理IAM资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM用户指南》中的何时创建IAM用户（而不是角色）。

IAM角色

IAM角色是您内部具有特定权限 AWS 账户 的身份。它与IAM用户类似，但与特定人员无关。您可以 AWS Management Console 通过切换IAM角色在中临时扮演角色。您可以通过调用 AWS CLI 或 AWS API操作或使用自定义操作来代入角色URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的使用IAM角色。

IAM具有临时证书的角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序EC2或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS)-当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。
  - 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》 AWS 服务中的创建角色以向委派权限。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行并发出 AWS CLI 或 AWS API请求的应用程序的临时证书。这比在EC2实例中存储访问密钥更可取。要为EC2实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在EC2实例上运行的程序获得临时证书。有关更多信息，请参阅IAM用户指南中的使用IAM角色向在 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用IAM角色还是使用IAM用户，请参阅《用户指南》中的何时创建IAM角色（而不是IAM用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以JSON文档的 AWS 形式存储在中。有关JSON策略文档结构和内容的更多信息，请参阅《IAM用户指南》中的JSON策略概述。

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或获取角色信息 AWS API。

基于身份的策略

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的创建IAM策略。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略IAM中使用 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例ACLs。 AWS WAF要了解更多信息ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向IAM实体（IAM用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM用户指南》中的IAM实体的权限边界。
- 服务控制策略 (SCPs)-SCPs 是为中的组织或组织单位 (OU) 指定最大权限的JSON策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。对成员账户中的实体（包括每个实体）的权限进行了SCP限制 AWS 账户根用户。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

AWS Systems Manager Incident Manager 如何使用 IAM

在使用IAM管理事件管理器的访问权限之前，请先了解事件管理器可以使用哪些IAM功能。

IAM你可以使用的功能 AWS Systems Manager Incident Manager

IAM功能	Incident Manager 支持
基于身份的策略	是
基于资源的策略	是
策略操作	是
策略资源	是
策略条件密钥	否
ACLs	否
ABAC（策略中的标签）	否
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	是

要全面了解事件管理器和其他 AWS 服务如何使用大多数IAM功能，请参阅《IAM用户指南》IAM中与之配合使用的AWS 服务。

Incident Manager 不支持拒绝访问使用共享的资源的策略 AWS RAM。

Incident Manager 的基于身份的策略

支持基于身份的策略：是

基于身份的策略是可以附加到身份（例如IAM用户、用户组或角色）的JSON权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅IAM用户指南中的创建IAM策略。

使用IAM基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

Incident Manager 的基于身份的策略示例

要查看 Incident Manager 基于身份的策略的示例，请参阅 适用于 AWS Systems Manager Incident Manager的基于身份的策略示例。

Incident Manager 内基于资源的策略

支持基于资源的策略：是

基于资源的JSON策略是您附加到资源的策略文档。基于资源的策略的示例包括IAM角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问权限，您可以将整个账户或另一个账户中的IAM实体指定为基于资源的策略中的委托人。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的IAM管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM用户指南》IAM中的跨账户资源访问权限。

事件管理器服务仅支持两种类型的基于资源的策略，使用 AWS RAM 控制台或 PutResourcePolicy 操作调用，后者附加到响应计划或联系人。该策略定义了哪些主体可以对响应计划、联系人、上报计划和事件采取行动。Incident Manager 使用基于资源的策略在账户之间共享资源。

Incident Manager 不支持拒绝访问使用共享的资源的策略 AWS RAM。

要了解如何将基于资源的策略附加到响应计划或联系人，请参阅 Incident Manager 中的跨区域和跨账户事件管理。

Incident Manager 内基于资源的策略示例

要查看 Incident Manager 基于资源的策略的示例，请参阅 基于资源的策略示例 AWS Systems Manager Incident Manager。

Incident Manager 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

JSON策略Action元素描述了可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API操作同名。也有一些例外，例如没有匹配API操作的仅限权限的操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Incident Manager 操作的列表，请参阅《服务授权参考》中的 AWS Systems Manager Incident Manager定义的操作。

Incident Manager 中的策略操作在此操作之前使用以下前缀：

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

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 Get 开头的所有操作，包括以下操作：

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

要查看 Incident Manager 基于身份的策略的示例，请参阅 适用于 AWS Systems Manager Incident Manager的基于身份的策略示例。

Incident Manager 在两个不同的命名空间中使用操作，即 ssm-事件和 ssm-联系人。创建 Incident Manager 的策略时，请确保为操作使用正确的命名空间。SSM-事件用于响应计划和与事件相关的行动。SSM-联系人用于与联系人和联系人互动相关的操作。例如：

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

Incident Manager 的策略资源

支持策略资源：是

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看事件管理器资源类型及其列表ARNs，请参阅《服务授权参考》 AWS Systems Manager Incident Manager中定义的资源。要了解您可以使用哪些操作来指定每ARN种资源，请参阅由定义的操作 AWS Systems Manager Incident Manager。

要查看 Incident Manager 基于身份的策略的示例，请参阅 适用于 AWS Systems Manager Incident Manager的基于身份的策略示例。

Incident Manager 资源用于创建事件、在聊天频道中进行协作、解决事件以及与响应者互动。如果用户有访问响应计划的权限，则可以访问根据该计划创建的所有事件。如果用户有访问联系人或上报计划的权限，则他们就可以将联系人参与到上报计划

Incident Manager 的策略条件密钥

支持特定于服务的策略条件密钥：否

管理员可以使用 AWS JSON策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。有关更多信息，请参阅《IAM用户指南》中的IAM策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅《IAM用户指南》中的AWS 全局条件上下文密钥。

事件管理器中的访问控制列表 (ACLs)

支持ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACLs与基于资源的策略类似，尽管它们不使用JSON策略文档格式。

使用事件管理器进行基于属性的访问控制 (ABAC)

支持ABAC（策略中的标签）：否

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。在中 AWS，这些属性称为标签。您可以将标签附加到IAM实体（用户或角色）和许多 AWS 资源。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关的更多信息ABAC，请参阅什么是ABAC？ 在《IAM用户指南》中。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的使用基于属性的访问控制 (ABAC)。

通过 Incident Manager 使用临时凭证

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关其他信息，包括哪些 AWS 服务 适用于临时证书 AWS 服务 ，请参阅《IAM用户指南》IAM中的 “适用于临时证书”。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或手动创建临时证书 AWS API。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅中的临时安全证书IAM。

Incident Manager 的跨服务主体权限

支持转发访问会话 (FAS)：是

当您使用IAM用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS使用调用委托人的权限 AWS 服务以及 AWS 服务 向下游服务发出请求的请求。FAS只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出请求。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。

Incident Manager 的服务角色

支持服务角色：是

服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅《IAM用户指南》 AWS 服务中的创建角色以向委派权限。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Incident Manager 的功能。仅当 Incident Manager 提供相关指导时才编辑服务角色。

在事件管理器中选择IAM角色

在 Incident Manager 中创建响应计划资源时，您必须选择一个角色以允许 Incident Manager 代表您运行 Systems Manager Automation 文档。如果您之前已经创建了一个服务角色或服务相关角色，则 Incident Manager 会提供一个角色列表供您选择。请务必选择一个允许访问以运行自动化文档实例的角色。有关更多信息，请参阅 在 Incident Manager 中使用 Systems Manager Automation 运行手册。当您创建要在事件发生期间使用的 AWS Chatbot 聊天频道时，您可以选择一个允许您直接使用聊天

命令的服务角色。要了解有关如何为事件协作创建聊天频道更多信息，请参阅 在 Incident Manager 中使用聊天频道。要详细了解中的IAM策略 AWS Chatbot，请参阅《AWS Chatbot 管理员指南》 AWS Chatbot中的 “使用管理运行命令的权限”。

Incident Manager 的服务相关角色

支持服务相关角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Incident Manager 服务相关角色的信息，请参阅 使用 Incident Manager 的服务相关角色。

适用于 AWS Systems Manager Incident Manager的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Incident Manager 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或来执行任务 AWS API。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的创建IAM策略。

有关 Incident Manager 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》 AWS Systems Manager Incident Manager中的操作、资源和条件密钥。ARNs

主题

- 策略最佳实践
- 使用 Incident Manager 控制台
- 允许用户查看他们自己的权限
- 访问响应计划

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除账户中的 Incident Manager 资源。这些操作可能会使 AWS 账户产生费用。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM用户指南》中的AWS 托AWS 管策略或工作职能托管策略。
- 应用最低权限权限-使用IAM策略设置权限时，仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限IAM的更多信息，请参阅《IAM用户指南》IAM中的策略和权限。
- 使用IAM策略中的条件进一步限制访问权限-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM用户指南》中的IAMJSON策略元素：条件。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 IAMAccess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的配置MFA受保护的API访问权限。

有关中最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM中的安全最佳实践。

使用 Incident Manager 控制台

要访问 AWS Systems Manager Incident Manager 控制台，您必须拥有一组最低权限。这些权限必须允许列出和查看有关 AWS 账户中的 Incident Manager 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

您无需为仅拨打 AWS CLI 或的用户设置最低控制台权限 AWS API。相反，只允许访问与他们尝试执行的API操作相匹配的操作。

为确保用户和角色可以使用事件管理器控制台解决事件，还要将事件管理器`IncidentManagerResolverAccess` AWS 托管策略附加到实体。有关更多信息，请参阅《用户指南》中的向IAM用户添加权限。

```
IncidentManagerResolverAccess
```

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用或以编程方式完成此操作的 AWS CLI 权限。 AWS API

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

访问响应计划

在本示例中，您想授予您的 Amazon Web Services 账户中的IAM用户访问您的事件管理器响应计划的权限`exampleplan`。您还想要允许该用户添加、更新和删除响应计划。

该策略为用户授予 ssm-incidents:ListResponsePlans、ssm-incidents:GetResponsePlan、ssm-incidents:UpdateResponsePlan 和 ssm-incident:ListResponsePlan 权限。

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

基于资源的策略示例 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 支持事件管理器响应计划和联系人的基于资源的权限策略。

事件管理器不支持基于资源的策略，这些策略拒绝访问使用 AWS RAM共享的资源。

要了解如何创建响应计划或联系人，请参阅 在 Incident Manager 中使用响应计划 和 在 Incident Manager 中使用联系人。

限制组织访问 Incident Manager 响应计划

以下示例向组织中具有组织 ID o-abc123def45 的用户授予权限，以响应使用响应计划 myplan 创建的事件。

该Condition模块使用StringEquals条件和aws:PrincipalOrgID条件键，后者是 AWS Organizations 特定的条件键。有关这些条件密钥的更多信息，请参阅在策略中指定条件。

```
{
  "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 联系人访问主体的权限

以下示例向委托人授予与该ARN`arn:aws:iam::999988887777:root`联系`mycontact`人创建互动的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

防止 Incident Manager 中的跨服务混淆代理

混淆代理问题是一个信息安全问题，当一个没有权限执行操作的实体调用一个更有权限的实体来执行操作时，就会出现这个问题。恶意行为者会借此机会运行原本无权运行的命令或修改原本无权访问的资源。

在中 AWS，跨服务模仿可能会导致副手场景混乱。跨服务模拟是指一种服务（正在调用服务）调用另一种服务（被调用的服务）。恶意行为者可以使用调用服务，使用他们通常不会拥有的权限更改另一种服务中的资源。

AWS 为服务委托人提供对您账户中资源的托管访问权限，以帮助您保护资源的安全。我们建议在资源策略中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文密钥。这些密钥限制了向该资源 AWS Systems Manager Incident Manager 提供其他服务的权限。如果您同时使用两个全局条件

上下文密钥，则在同一策略语句中使用 aws:SourceAccount 值和 aws:SourceArn 值中引用的账户时，必须使用相同的账户 ID。

的值aws:SourceArn必须是受影响的事件记录ARN的值。如果您不知道资源的全部ARN内容，或者要指定多个资源，请使用带有*通配符的aws:SourceArn全局上下文条件键来表示未知部分。ARN例如，您可以将 aws:SourceArn 设置为 arn:aws:ssm-incidents::*111122223333*:*。

在以下信任策略示例中，我们使用aws:SourceArn条件键根据事件记录限制对服务角色的访问权限ARN。只有从响应计划 myresponseplan 创建的事件记录才能使用此角色。

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

使用 Incident Manager 的服务相关角色

AWS Systems Manager Incident Manager 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的IAM角色类型，直接链接到事件经理。服务相关角色由 Incident Manager 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可更轻松地设置 Incident Manager，因为您不必手动添加必要的权限。Incident Manager 定义其服务相关角色的权限，除非另外定义，否则只有 Incident Manager 可以代入该角色。定义的权限包括信任策略和权限策略，并且该权限策略不能附加到任何其他IAM实体。

只有在首先删除相关资源后，您才能删除服务相关角色。这将保护 Incident Manager 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与之配合使用的AWS 服务，IAM并在 “服务相关角色” 列中查找标有 “是” 的服务。请选择是与查看该服务的服务相关角色文档的链接。

Incident Manager 的服务相关角色权限

事件经理使用名为的服务相关角色 AWSServiceRoleforIncidentManager——允许事件经理代表你管理事件经理事件记录和相关资源。

AWSServiceRoleforIncidentManager 服务相关角色信任以下服务来代入该角色：

- `ssm-incidents.amazonaws.com`

角色权限策略 `AWSIncidentManagerServiceRolePolicy` 允许 Incident Manager 对指定资源完成以下操作：

- 操作：与该操作相关的所有资源上的 `ssm-incidents:ListIncidentRecords`。
- 操作：与该操作相关的所有资源上的 `ssm-incidents:CreateTimelineEvent`。
- 操作：与该操作相关的所有资源上的 `ssm:CreateOpsItem`。
- 操作：`all resources related to the action.` 上的 `ssm:AssociateOpsItemRelatedItem`
- 操作：与该操作相关的所有资源上的 `ssm-contacts:StartEngagement`。
- 操作：`cloudwatch:PutMetricData`针对`AWS/IncidentManager`命名空间内的 CloudWatch 指标

必须配置权限以允许实IAM体（例如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM用户指南》中的服务相关角色权限。

创建 Incident Manager 的服务相关角色

您无需手动创建服务相关角色。在、或中创建复制集时 AWS Management Console AWS CLI AWS API，事件管理器会为您创建与服务相关的角色。

如果您删除此服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。创建复制集时，Incident Manager 会再次为您创建服务相关角色。

编辑 Incident Manager 的服务相关角色

事件管理器不允许您编辑 AWSServiceRoleforIncidentManager 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是，您可以使用编辑角色的描述IAM。有关更多信息，请参阅IAM用户指南中的编辑服务相关角色。

删除 Incident Manager 的服务相关角色

如果您不再需要使用某个需要服务相关角色的特征或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

要删除服务相关角色，您必须先删除复制集。删除复制集会删除在 Incident Manager 中创建和存储的所有数据，包括响应计划、联系人和上报计划。您还将丢失所有先前创建的事件。任何指向已删除响应计划的警报和 EventBridge 规则都不会再在警报或规则匹配时创建事件。要删除复制集，您必须删除该集合中的每个区域。

> **Note**
>
> 如果在您试图删除资源时 Incident Manager 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除所使用的复制集中的区域 AWSServiceRoleforIncidentManager

1. 打开 Incident Manager 控制台，然后从左侧导航栏中选择设置。
2. 在复制集中选择一个区域。
3. 选择删除。
4. 要确认删除区域，请输入区域名称并选择删除。
5. 重复这些步骤，直到删除复制集中的所有区域。删除最后一个区域时，控制台会通知您同时删除复制集。

使用手动删除服务相关角色 IAM

使用IAM控制台 AWS CLI、或删除 AWSServiceRoleforIncidentManager服务相关角色。 AWS API有关更多信息，请参阅IAM用户指南中的删除服务相关角色。

Incident Manager 服务相关角色支持的区域

Incident Manager 支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

AWS 的托管策略 AWS Systems Manager Incident Manager

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户托管式策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 当新服务启动或现有服务 AWS 服务 有新API操作可用时，最有可能更新 AWS 托管策略。

有关更多信息，请参阅《IAM用户指南》中的AWS 托管策略。

AWS 托管策略： AWSIncidentManagerIncidentAccessServiceRolePolicy

你可以附加AWSIncidentManagerIncidentAccessServiceRolePolicy到你的IAM实体。Incident Manager 还会将该策略附加到允许 Incident Manager 代表您执行操作的 Incident Manager 角色。

此策略授予只读权限，允许事件管理员读取某些其他资源中的资源 AWS 服务 ，以识别与这些服务中的事件相关的发现。

权限详细信息

该策略包含以下权限。

- cloudformation— 允许主体描述 AWS CloudFormation 堆栈。这是事件管理器识别与事件相关 CloudFormation 的事件和资源所必需的。
- codedeploy— 允许委托人读取 AWS CodeDeploy 部署。这是事件管理器识别与事件相关的 CodeDeploy 部署和目标所必需的。
- autoscaling— 允许委托人确定亚马逊弹性计算云 (EC2) 实例是否属于 Auto Scaling 组。这是必需的，这样事件管理器才能为属于 Auto Scaling 组的EC2实例提供调查结果。

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

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

要查看有关策略的更多详细信息，包括最新版本的JSON策略文档，请参阅AWSIncidentManagerIncidentAccessServiceRolePolicy《AWS 托管策略参考指南》。

AWS 托管式策略：**AWSIncidentManagerServiceRolePolicy**

你无法附着AWSIncidentManagerServiceRolePolicy在你的IAM实体上。该附加到服务相关角色的策略允许 Incident Manager 代表您执行操作。有关更多信息，请参阅 使用 Incident Manager 的服务相关角色。

此政策授予事件管理员列出事件、创建时间轴事件、创建 OpsItems、关联相关项目 OpsItems、开始互动以及发布与事件相关的 CloudWatch指标的权限。

权限详细信息

该策略包含以下权限。

- ssm-incidents——允许主体列出事件清单并创建时间轴事件。这是必需的，这样响应人员才能在事件发生期间在事件控制面板上进行协作。
- ssm— 允许委托人创建 OpsItems 和关联相关项目。这是在事件开始 OpsItem 时创建父项所必需的。
- ssm-contacts——允许主体开始互动。这是 Incident Manager 在事件发生期间与联系人联系所必需的。

- `cloudwatch`— 允许委托人发布 CloudWatch 指标。这是 Incident Manager 发布与事件相关的指标所必需的。

```
{
    "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"
                }
            }
```

```
        }
    ]
}
```

要查看有关策略的更多详细信息，包括最新版本的JSON策略文档，请参阅AWSIncidentManagerServiceRolePolicy《AWS 托管策略参考指南》。

AWS 托管策略：**AWSIncidentManagerResolverAccess**

您可以附加AWSIncidentManagerResolverAccess到您的IAM实体，以允许它们启动、查看和更新事件。这也使他们能够在事件控制面板中创建客户时间轴事件和相关项目。您也可以将此政策附加到 AWS Chatbot 服务角色或直接附加到与用于事件协作的任何聊天渠道关联的客户托管角色。要详细了解中的IAM策略 AWS Chatbot，请参阅《AWS Chatbot 管理员指南》 AWS Chatbot中的 “使用管理运行命令的权限”。

权限详细信息

该策略包含以下权限。

- ssm-incidents——您可以启动事件、列出响应计划、列出事件、更新事件、列出时间轴事件、创建自定义时间轴事件、更新自定义时间轴事件、删除自定义时间轴事件、列出相关项目、创建相关项目和更新相关项目。

```
{
    "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": "*"
        }
    ]
}
```

要查看有关策略的更多详细信息，包括最新版本的JSON策略文档，请参阅AWSIncidentManagerResolverAccess《AWS 托管策略参考指南》。

事件管理器对 AWS 托管策略的更新

查看自该服务开始跟踪事件 AWS 管理器托管策略变更以来这些更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 Incident Manager 文档历史记录页面上的订阅RSS源。

更改	描述	日期
AWSIncidentManagerIncidentAccessServiceRolePolicy	事件管理器为AWSIncidentManagerIncidentAccessServiceRolePo	2024 年 2 月 20 日

更改	描述	日期
— 政策更新	licy 支持调查结果功能添加了一项新权限，允许其检查EC2实例是否属于 Auto Scaling 组。	
AWSIncidentManagerIncidentAccessServiceRolePolicy：新策略	事件管理器添加了一项新政策，该策略授予事件管理员在管理事件时致电其他 AWS 服务 人的权限。	2023 年 11 月 17 日
AWSIncidentManagerServiceRolePolicy — 政策更新	事件管理器添加了一项新权限，允许事件管理员将指标发布到您的账户。	2022 年 12 月 16 日
AWSIncidentManagerResolverAccess ——新策略	Incident Manager 添加了一项新政策，允许启动事件、列出响应计划、列出事件、更新事件、列出时间轴事件、创建自定义时间轴事件、更新自定义时间轴事件、删除自定义时间轴事件、列出相关项目、创建相关项目和更新相关项目。	2021 年 4 月 26 日
AWSIncidentManagerServiceRolePolicy：新策略	事件管理器添加了一项新政策，授予事件管理员列出事件、创建时间轴事件 OpsItems、创建、关联相关项目以及启动与事件相关的活动的权限。 OpsItems	2021 年 4 月 26 日
Incident Manager 开始跟踪更改	事件管理器开始跟踪其 AWS 托管策略的变更。	2021 年 4 月 26 日

对 AWS Systems Manager Incident Manager 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用事件管理器时可能遇到的常见问题，以及IAM。

主题

我无权在 Incident Manager 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当mateojacksonIAM用户尝试使用控制台查看虚构*my-example-widget*资源的详细信息但没有虚构权限时，就会出现以下示例错误。ssm-incidents:*GetWidget*

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

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 ssm-incidents:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到错误提示，表明您无权执行 iam:PassRole 操作，则您必须更新策略以允许将角色传递给 Incident Manager。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的IAM用户marymajor尝试使用控制台在事件管理器中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我希望允许我的 Amazon Web Services 账户以外的人访问我的 Incident Manager 资源

您可以创建一个角色，以便其他账户的用户或组织外的人员可以使用该角色访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Incident Manager 是否支持这些特征，请参阅 AWS Systems Manager Incident Manager 如何使用 IAM。
- 要了解如何提供对您拥有的资源的访问权限，请参阅《IAM用户指南》中的 AWS 账户 向其他IAM用户提供访问权限。 AWS 账户
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅IAM用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的向经过外部身份验证的用户提供访问权限（联合身份验证）。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。

在 Incident Manager 中使用共享的联系人和响应计划

通过联系人共享，作为联系人所有者，您可以与其他人 AWS 账户 或 AWS 组织内部共享联系人信息、升级计划和互动。您可以集中创建和管理联系人和上报计划，并确保其他人能在事件发生时联系到正确的联系人。

通过共享响应计划，作为响应计划所有者，您可以与其他人 AWS 账户 或 AWS 组织内部共享响应计划和相关事件。您可以集中创建和管理响应计划，这样使用者账户中的响应人员就能在事件发生时与之互动。

联系人或响应计划所有者可以与以下人员共享联系人和响应计划：

- 具体在其组织 AWS 账户 内部或外部 AWS Organizations
- 其组织内部的组织单位 AWS Organizations
- 它的整个组织都在 AWS Organizations

内容

共享联系人和响应计划的先决条件

要通过以下方式与您的组织或 AWS Organizations中的组织单位共享联系人或响应计划，请执行以下操作：

- 您必须拥有自己的资源 AWS 账户。您不能共享已与您共享的联系认或响应计划。
- 您必须启用与共享 AWS Organizations。有关更多信息，请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations 共享。

相关服务

联系人和响应计划共享与 AWS Resource Access Manager (AWS RAM) 集成。使用 AWS RAM，您可以与任何人 AWS 账户 或通过任何人共享您的 AWS 资源 AWS Organizations。您可以通过创建资源共享来共享自己拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。消费者可以是个人 AWS 账户、组织单位或中的整个组织 AWS Organizations。

有关的更多信息 AWS RAM，请参阅《AWS RAM 用户指南》。

共享联系人或响应计划

共享响应计划后，使用者可以访问使用该响应计划创建的所有过去、当前和将来的事件。

共享联系人后，使用者可以访问联系人信息、互动计划、上报计划以及事件发生期间的互动情况。使用者还可以在事件发生时与联系认或上报计划互动。

如果您是组织中的一员， AWS Organizations 并且启用了组织内部共享，则组织中的消费者将自动获得访问共享联系人或回应计划的权限。否则，使用者将会收到加入资源共享的邀请，并在接受邀请后为其授予共享联系人或响应计划的访问权限。

您可以使用 AWS RAM 控制台或共享您拥有的联系人或回复计划 AWS CLI。

使用 AWS RAM 控制台共享您拥有的联系计划或回复计划

请参阅《AWS RAM 用户指南》中的创建资源共享。

要共享您拥有的联系计划或回复计划，请使用 AWS CLI

使用create-resource-share命令。

停止共享联系人或响应计划

当资源所有者停止与使用者共享联系人或响应计划时，联系人、响应计划、上报计划、互动和事件将不再显示在使用者的控制台中。

> **Note**
>
> 如果使用者在控制台中查看联系人、响应计划、上报计划、互动或事件，则会继续看到这些内容，但不会更新，直到他们刷新页面或离开页面。

要停止共享您拥有的共享联系人或响应计划，您必须将其从资源共享中删除。您可以使用 AWS RAM 控制台或 AWS CLI.

要使用 AWS RAM 控制台停止共享您拥有的共享联系人或响应计划

请参阅《AWS RAM 用户指南》中的更新资源共享。

要使用 AWS CLI停止共享您拥有的共享联系人或响应计划

使用disassociate-resource-share命令。

识别共享的联系人或响应计划

所有者和使用者可以使用 Incident Manager 控制台和 AWS CLI识别共享联系人和响应计划。

要使用 Incident Manager 控制台识别共享的联系人或响应计划

> **Note**
>
> 在 Incident Manager 控制台中，联系人、响应计划、上报计划、互动和事件一般都不能被识别为共享资源。在可见 Amazon 资源名称 (ARN) 的地方，ARN包含所有者的账户 ID。

要确定共享的联系人或回应计划，请使用 AWS CLI

使用ListResponsePlans或ListContacts命令。该命令将返回您拥有的联系人和响应计划，以及与您共享的联系人和响应计划。ARN显示了联系人或回应计划所有者的 AWS 账户 ID。

共享的联系人和响应计划权限

所有者的权限

所有者可以更新、查看、共享、停止共享以及使用联系人和响应计划。联系人和响应计划包括相关的互动和事件。

使用者的权限

使用者只能使用和查看响应计划和联系人。联系人和响应计划包括相关的互动和事件。

计费和计量

资源所有者需支付资源费用。使用者无需为共享资源付费。共享资源不会产生额外的费用。

实例限制

共享资源不会影响资源所有者或使用者账户中的资源限制。仅使用所有者的账户来计算资源限制。

合规性验证 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 作为多个合规计划的一部分，第三方审计师对安全性和 AWS 合规性进行评估。这些包括SOC、PCIRAMPHIPAA、美联储等。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。

- 在 Amazon Web Services 上进行HIPAA安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《HIPAA符合条件的服务参考》。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Systems Manager Incident Manager

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

Incident Manager 是一项全球区域服务，目前不支持可用区。

除了 AWS 全球基础架构外，Incident Manager 还提供多项功能来帮助支持您的数据弹性和备份需求。在准备就绪向导中，系统会要求您设置复制集。该区域复制集可确保您的数据和资源可从多个区域访

问，从而使整个云网络的事件管理更易于管理。这种复制还可确保您的数据在其中一个区域出现故障时是安全且可访问的。

有关使用 Incident Manager 复制集的更多信息，请参阅 使用 Incident Manager 复制集。

基础设施安全 AWS Systems Manager Incident Manager

作为一项托管服务 AWS Systems Manager Incident Manager ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的API呼叫通过网络访问事件管理器。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如（Ephemeral Diffie-HellmanPFS）或（Elliptic C DHE urve Ephemeral Diffie-Hellman）。ECDHE大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与IAM委托人关联的私有访问密钥对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

使用 AWS Systems Manager Incident Manager 和接口VPC端点 (AWS PrivateLink)

您可以通过创建接口VPC终端节点在您的VPC和 AWS Systems Manager Incident Manager 之间建立私有连接。接口端点由 AWS PrivateLink提供支持。借 AWS PrivateLink助，您无需互联网网关、NAT 设备、VPN连接或 AWS Direct Connect 连接即可私密访问事件管理器API操作。您中的实例VPC不需要公有 IP 地址即可与事件管理器API操作进行通信。您VPC和事件管理器之间的流量保持在 Amazon 网络内。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 Amazon VPC 用户指南中的接口VPC终端节点 (AWS PrivateLink)。

事件管理器VPC端点注意事项

在为事件管理器设置接口VPC终端节点之前，请务必查看亚马逊VPC用户指南中的接口终端节点属性以及限制和AWS PrivateLink配额。

事件管理器支持从您调用其所有API操作VPC。要使用所有事件管理器，必须创建两个VPC端点：一个用于ssm-incidents，一个用于ssm-contacts。

为事件管理器创建接口VPC端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为事件管理器创建VPC终端节点。有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口终端节点。

使用以下服务名称为事件管理器创建VPC端点：

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

如果您使用私有DNS终端节点，则可以使用事件管理器在该区域的默认DNS名称向事件管理器API发出请求。例如，您可以使用名称 ssm-incidents.us-east-1.amazonaws.com 或 ssm-contacts.us-east-1.amazonaws.com。

有关更多信息，请参阅 Amazon VPC 用户指南中的通过接口终端节点访问服务。

为事件管理器创建VPC端点策略

您可以将终端节点策略附加到控制事件管理器访问权限的VPC终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行这些操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用VPC终端节点控制对服务的访问。

示例：事件管理器操作的VPC端点策略

下面是 Incident Manager 的端点策略示例。当附加到端点时，该策略会向所有资源上的所有主体授予对列出的 Incident Manager 操作的访问权限。

```
{
   "Statement":[
      {
         "Principal":"*",
```

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

Incident Manager 中的配置和漏洞分析

配置和 IT 控制由您（我们的客户）共同 AWS 负责。有关更多信息，请参阅责任 AWS 共担模型。

中的安全最佳实践 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实操是一般准则，并不代表完整的安全解决方案。这些最佳实操可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。

主题

- Incident Manager 的预防性安全最佳实践
- Incident Manager 的 Detective 安全最佳实践

Incident Manager 的预防性安全最佳实践

实施最低权限访问

在授予权限时，您可以决定谁获得哪些 Incident Manager 资源的哪些权限。您可以对这些资源启用希望允许的特定操作。因此，仅授予执行任务所需的权限。实施最低权限访问对于减小安全风险以及可能由错误或恶意意图造成的影响至关重要。

为实现最低权限访问，可以使用以下工具：

- 使用IAM实体的策略和权限边界控制对 AWS 资源的访问权限
- 服务控制策略

创建和管理联系人

激活联系人时，Incident Manager 会与设备联系以确认激活。激活设备前，请确保设备信息正确无误。这样可以减少 Incident Manager 在激活过程中联系错误设备或人员的可能性。

定期审查联系人和上报计划，确保在事件发生时只联系需要联系的联系人。定期查看联系人，删除过时或不正确的信息。如果事件发生时不应再通知联系人，则应将其从相关上报计划中删除或从 Incident Manager 中删除。

将聊天频道设为私人频道

您可以将事件聊天频道设为私人频道，以实现最低权限访问。考虑为每个响应计划模板使用不同的聊天频道和范围缩小的用户列表。这样可以确保只有正确的回复者才能进入可能包含敏感信息的聊天频道。

AWS Chatbot 启用的 Slack 频道继承用于配置 AWS Chatbot的IAM角色的权限。这使 AWS Chatbot 启用的 Slack 频道中的响应者可以调用任何允许列表中的操作，例如事件管理APIs器和检索指标图表。

让 AWS 工具保持最新

AWS 定期发布可在 AWS 操作中使用的工具和插件的更新版本。确保这些资源为最新可确保您账户中的用户和实例能够访问这些工具中的最新功能和安全特征。

- AWS CLI — AWS Command Line Interface (AWS CLI) 是一个开源工具，可让您使用命令行 shell 中的命令与 AWS 服务进行交互。要更新 AWS CLI，请运行安装 AWS CLI时使用的相同命令。我们建议您在本地计算机上创建计划任务，根据您的操作系统来相应运行命令，至少每两周一次。有关安装命令的信息，请参阅《 AWS 命令行界面用户指南》中的安装AWS命令行界面。
- AWS Tools for Windows PowerShell — Window PowerShell s 工具是一组 PowerShell 模块，它们建立在 for 公开的功能之 AWS SDK上。 NET。Windows 工具 PowerShell 允许您通过 PowerShell 命令行编写 AWS 资源操作脚本。随着适用于 Windows PowerShell 的工具的更新版本的发布，您应该定期更新在本地运行的版本。有关信息，请参阅AWS Tools for Windows PowerShell 在 Windows 上更新或在 Linux 或 macOS AWS Tools for Windows PowerShell 上更新。

相关内容

Systems Manager 的安全最佳实践

Incident Manager 的 Detective 安全最佳实践

识别和审计您的所有 Incident Manager 资源

确定您的 IT 资产是监管和安全性的一个至关重要的方面。识别 Systems Manager 资源，以评估它们的安保状况并对潜在的薄弱领域采取措施。为 Incident Manager 资源创建 Resource Groups。有关更多信息，请参阅《AWS Resource Groups 用户指南》中的什么是 Resource Groups？。

使用 AWS CloudTrail

AWS CloudTrail 提供用户、角色或 AWS 服务在事件管理器中采取的操作的记录。使用收集的信息 AWS CloudTrail，您可以确定向 Incident Manager 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。有关更多信息，请参阅 使用记录 AWS Systems Manager Incident Manager API 调用 AWS CloudTrail。

监控 AWS 安全公告

定期查看发布的安全公告，以备不时之 Trusted Advisor 需 AWS 账户。你可以使用describe-trusted-advisor-checks以编程方式执行此操作。

此外，请积极监控您每个人注册的主电子邮件地址 AWS 账户。 AWS 将使用此电子邮件地址就可能影响您的新出现的安全问题与您联系。

AWS 具有广泛影响的运营问题发布在 S AWS ervice Health Das hboard 上。操作性问题也通过 AWS Health Dashboard发布到各个账户。有关更多信息，请参阅 AWS Health 文档。

相关内容

Amazon Web Services：安全过程概述（白皮书）

入门：在配置 AWS 资源时遵循安全最佳实践（AWS 安全博客）

IAM最佳实践

中的安全最佳实践 AWS CloudTrail

在事件管理器中进行监控

AWS Systems Manager 事件管理器与以下提供监控和记录功能的服务集成：

CloudWatch 指标

使用 CloudWatch 指标来检索 S AWS ystems Manager 事件管理器操作的数据点统计信息，作为一组有序的时间序列数据，称为指标。您可使用这些指标来验证您的系统是否按预期运行。有关更多信息，请参阅 事件管理器中的 Amazon CloudWatch 指标。

CloudTrail 日志

AWS CloudTrail 用于捕获有关 AWS API 调用的详细信息。您可以将这些调用作为日志文件存储在 Amazon Simple Storage Service 中。您可以使用这些 CloudTrail 日志来确定拨打了哪个电话、呼叫来自哪个源 IP 地址、谁拨打了电话以及何时拨打了呼叫等信息。 CloudTrail 日志包含有关事件管理器 API 操作调用的信息。I有关更多信息，请参阅使用记录 AWS Systems Manager Incident Manager API 调用 AWS CloudTrail。

Trusted Advisor

AWS Trusted Advisor 可以帮助您监控 AWS 资源以提高性能、可靠性、安全性和成本效益。所有用户都可以使用四张 Trusted Advisor 支票；50多张支票可供拥有商业或企业支持计划的用户使用。对于 Incident Manager， Trusted Advisor 检查复制集的配置是否使用多个配置 AWS 区域 来支持区域故障转移和响应。有关更多信息，请参阅《AWS Support 用户指南》中的 AWS Trusted Advisor。

事件管理器中的 Amazon CloudWatch 指标

事件管理器提供您可以在 Amazon 中监控的汇总指标 CloudWatch。您可以使用这些指标来确定事件和响应计划的趋势。

这些指标包括：

- 在特定时间段内发生的事件数量
- 响应和解决这些事件的时间
- 已解决的事件数量

您可以监控 Incident Manager 的各项指标，以更好地了解您的运行状况，并采取有意义的措施来推动事件响应的卓越运行。Incident Manager 指标适用于所有 Incident Manager 区域。当您登录事件管理

器时，您将在复制集中指定的所有区域在 Amazon CloudWatch 中查看您的指标。您可以查看已采取事件措施的区域内已发布的指标。使用这些指标无需额外付费。

在 CloudWatch 控制台上，您可以使用这些指标构建仪表板，以：

- 测量并审查现有事件负载
- 跟踪事件负载是增加、减少还是保持不变
- 更有效地使用 Incident Manager 来减少事件的频率、持续时间和影响

本页描述了 CloudWatch 控制台上可用的事件管理器指标。

> **Important**
>
> 对于客户生成的事件，如果中的`TriggerDetails`源值使用非 ASCII 字符命名，则不会在不支持非 ASCII 文本的 Amazon CloudWatch 指标中报告该事件的指标。 `source`只能以编程方式提供，例如使用 SDK 或。 AWS CLI

事件管理器将以下指标发送到 CloudWatch。

指标	描述
`NumberOfCreateIncidents`	创建的事件数量。 有效维度：[]（空维度）、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan, Impact]、[ResponsePlan, Source] 单位：计数
`NumberOfResolveIncidents`	已解决的事件数量。 有效维度：[]（空维度）、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan, Impact]、[ResponsePlan, Source] 单位：计数
`TimeToFirstAcknowledgement`	事件创建时间与首次确认事件时间之间的时间差。

指标	描述
	有效维度：[]（空维度）、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan ，Impact]、[ResponsePlan ，Source] 单位：秒
TimeToResolveIncident	事件发生时间与解决时间之间的时间差。 有效维度：[]（空维度）、[ResponsePlan]、[Impact]、[Source]、[ResponsePlan ，Impact]、[ResponsePlan ，Source] 单位：秒

在 CloudWatch控制台上查看事件管理器指标

在 CloudWatch 控制台中查看事件管理器指标

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 选择 IncidentManager 命名空间。
4. 在指标选项卡上，选择一个维度，然后选择一个指标。

有关使用 CloudWatch 指标的更多信息，请参阅 Amazon CloudWatch 用户指南中的以下主题：

- 指标
- 使用亚马逊 CloudWatch 指标

指标的维度

Incident Manager 指标使用 IncidentManager 命名空间并为以下维度提供指标：

维度	描述
By Response Plan	按响应计划查看汇总指标。
By Impact Level	按严重性级别查看汇总指标。
By Source	查看手动、 CloudWatch 警报或 EventBridge 事件创建的事件的指标。
Across All Incidents	查看当前 AWS 区域所有事件的汇总指标。
Response Plan name and Source	查看响应计划和来源的每种组合的汇总指标。
Response Plan Name and Impact Level	查看响应计划和严重性级别的每种组合的汇总指标。

使用记录 AWS Systems Manager Incident Manager API 调用 AWS CloudTrail

AWS Systems Manager Incident Manager 与AWS CloudTrail一项服务集成，该服务提供用户、角色或. 所执行操作的记录 AWS 服务。 CloudTrail 将事件管理器的所有 API 调用捕获为事件。捕获的调用包括来自 Incident Manager 控制台的调用和对 Incident Manager API 操作的代码调用。使用收集的信息 CloudTrail，您可以确定向 Incident Manager 发出的请求、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS Management Console 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许您对事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅AWS CloudTrail 用户指南中的使用 AWS CloudTrail Lake。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

事件管理器管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制层面操作。默认情况下， CloudTrail 记录管理事件。

AWS Systems Manager Incident Manager 将所有事件管理器控制平面操作记录为管理事件。有关事件管理器记录的 AWS Systems Manager Incident Manager 控制平面操作的列表 CloudTrail，请参阅 AWS Systems Manager Incident Manager API 参考。

事件管理器事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

以下示例显示了演示该StartIncident操作的 CloudTrail 日志条目。

```
{
    "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"
}
```

以下示例显示了演示该DeleteContactChannel操作的 CloudTrail 日志条目。

```
{
    "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"
}
```


有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的CloudTrail录制内容。

产品和服务与 Incident Manager 集成

事件管理器是一项功能 AWS Systems Manager，可与以下产品、服务和工具集成。

与集成 AWS 服务

事件管理器与下表中所述的 AWS 服务 和工具集成。

AWS CDK	AWS CDK 是一个开发框架，用于使用代码来定义您的云基础架构并 AWS CloudFormation 用于配置。 AWS CDK 支持多种编程语言 TypeScript，包括、、 JavaScriptPythonJava、和 C#/Net。 有关将 AWS CDK 与事件管理器配合使用的信息，请参阅 AWS CDK API 参考中的以下部分： • @aws-cdk/aws-ssmincidents 模块 • @aws-cdk/aws-ssmcontacts 模块
AWS Chatbot	AWS Chatbot使 DevOps 软件开发团队能够使用消息传递程序聊天室来监控和响应其中的操作事件 AWS Cloud。 AWS Chatbot 使用 Incident Manager，您可以创建聊天频道，响应者可以使用这些频道来监控和响应事件。 AWS Chatbot 支持Slack聊天室、Microsoft Teams频道和 Amazon Chime 聊天室作为聊天频道。 在创建聊天频道的过程中，您还需要在 Amazon Simple Notification Service (Amazon SNS) 中创建主题。Amazon SNS 是一项托管服务，可将消息从发布者提供给订阅用户。在事件响应计划中，当您将创建的聊天频道与计划关联时，您还可以选择一个或多个与该聊天频道关联的主题。

	这些 SNS 主题用于向事件响应者发送有关事件的通知。 有关更多信息，请参阅在 Incident Manager 中使用聊天频道。
AWS CloudFormation	AWS CloudFormation 是一项服务，您可以使用它来创建包含应用程序所需的所有资源的模板，然后为您配置和配置资源。它还将配置所有依赖关系，因此您可以将更多精力放在应用程序上，而减少对资源管理的关注。 有关 AWS CloudFormation 与事件管理器配合使用的信息，请参阅《AWS CloudFormation 用户指南》中的以下主题： • Incident Manager 资源类型参考 • 联系人资源类型参考资源类型参考
Amazon CloudWatch	CloudWatch实时监控您的 AWS 资源和您运行 AWS 的应用程序。您可以使用 CloudWatch 来收集和跟踪指标，这些指标是您可以衡量资源和应用程序的变量。 您可以在事件管理器中配置 CloudWatch 警报以创建事件。 CloudWatch 当警报进入警报状态时，与 Systems Manager 和 Incident Manager 合作，根据响应计划模板创建事件。 有关更多信息，请参阅使用 CloudWatch 警报自动创建事件。

Amazon Chime	Amazon Chime 是一个集会议、聊天和业务电话于一体的在线工作场所。您可以使用 Amazon Chime 在组织内外开会、聊天和拨打业务电话。 您可以在 AWS Chatbot 中为 Amazon Chime 创建一个聊天频道，然后将该频道添加到响应计划中，从而将 Amazon Chime 聊天室集成到 Incident Manager 操作中。 有关更多信息，请参阅在 Incident Manager 中使用聊天频道。
Amazon EventBridge	EventBridge是一项无服务器服务，它使用事件连接应用程序组件，使您可以更轻松地构建可扩展的事件驱动应用程序。 您可以配置 EventBridge 规则以监视 AWS 资源中的事件模式，并在事件与您定义的模式匹配时在事件管理器中创建事件。您的规则可以监控数十种第三方应用程序 AWS 服务 和服务中的事件模式。 有关更多信息，请参阅使用 EventBridge 事件自动创建事件。
AWS Secrets Manager	借助 Secrets Manager，您可以在数据库凭证、应用程序凭证、OAuth 令牌、API 密钥和其他密钥的整个生命周期内对其进行管理、检索和轮换。 当你将 Incident Manager 与 PagerDuty 服务集成时，你会在 Secrets Manager 中创建一个包含你的 PagerDuty 凭据的密钥。 有关更多信息，请参阅将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中。

AWS Systems Manager	Systems Manager 是一个操作中心，可用于查看和控制您的应用程序基础架构，也是云环境的安全 end-to-end 管理解决方案。以下 Systems Manager 功能可直接与 Incident Manager 集成： • 自动化——自动化运行手册定义了 Systems Manager 在 AWS 资源上执行的操作。在 Incident Manager 中，运行手册定义了一系列用于解决事件的自动和手动步骤。 有关创建与 Incident Manager 一起使用的自动化运行手册的信息，请参阅 在 Incident Manager 中使用 Systems Manager Automation 运行手册。 • OpsCenter— OpsCenter 提供一个中心位置，运营工程师和 IT 专业人员可以在其中管理与 AWS 资源相关的运营工作项目（称为 OpsItems）。您可以 OpsItems直接根据事后分析进行创建，以跟进相关工作。 有关更多信息，请参阅在 Incident Manager 中执行事件后分析。
AWS Trusted Advisor	Trusted Advisor是一款可供购买基本或开发人员支持计划的 AWS 客户使用的工具。 Trusted Advisor 检查您的 AWS 环境，然后在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。 对于 Incident Manager， Trusted Advisor 检查复制集的配置是否使用多个配置 AWS 区域 来支持区域故障转移和响应。

与其他产品和服务的集成

您可以将 Incident Manager 与下表中所述的第三方服务集成或使用。

Jira Cloud	使用 AWS 服务管理连接器，您可以将事件管理器与基于云的第三方工作流程平台 Jira Cloud (Atlassian) 集成。 配置与 Jira Cloud 的集成后，当您在 Incident Manager 中创建新事件时，集成也会在 Jira Cloud 中创建事件。如果您在 Incident Manager 中更新了事件，则就会将这些更新添加到 Jira Cloud 中的相应事件中。如果您在 Incident Manager 或 Jira Cloud 中解决事件，则集成将根据您配置的首选项来解决这两项服务中的事件。 有关更多信息，请参阅《AWS 服务管理连接器管理员指南》中的集成 AWS Systems Manager Incident Manager （Jira Cloud）。
Jira Service Management	使用 AWS 服务管理连接器，您可以将事件管理器与基于云的第三方工作流平台 Jira Service Managem ent 集成。 配置与 Jira Service Management 的集成后，当您在 Incident Manager 中创建新事件时，集成也会在 Jira Service Management 中创建事件。如果您在 Incident Manager 中更新了事件，则就会将这些更新添加到 Jira Service Management 中的相应事件中。如果您在 Incident Manager 或 Jira Service Management 中解决事件，则集成将根据您配置的首选项来解决这两项服务中的事件。 有关更多信息，请参阅《AWS 服务管理连接器管理员指南》中的配置 Jira Service Managemen t。
Microsoft Teams	Microsoft Teams 提供基于云的协作工具，用于团队消息、音频和视频会议以及文件共享。

	您可以在 AWS Chatbot 中为 Microsoft Team 创建聊天频道，然后将该频道添加到响应计划中，从而将 Microsoft Teams 频道集成到 Incident Manager 操作中。 有关更多信息，请参阅在 Incident Manager 中使用聊天频道。
PagerDuty	PagerDuty是一款支持寻呼工作流程和升级策略的事件响应工具。 将事件管理器与集成后 PagerDuty，可以在响应计划中添加 PagerDuty 服务。之后，每当在事件管理器中创建事件 PagerDuty 时，都会在中创建相应的事件。中的事件除了在事件管理器中定义的寻呼工作流程和升级策略外，还 PagerDuty 使用您在其中定义的寻呼工作流程和升级策略。PagerDuty将事件管理器中的时间轴事件作为事件备注附上。 要将 Incident Manager 与集成 PagerDuty，您必须先在中创建一个 AWS Secrets Manager 包含您的 PagerDuty 凭据的密钥。 有关向中的密钥添加 PagerDuty REST API 密钥和其他所需详细信息的信息 AWS Secrets Manager，请参阅将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中。 有关将您的 PagerDuty 账户中的 PagerDuty 服务添加到事件管理器中的响应计划的信息，请参阅主题中将 PagerDuty 服务集成到响应计划的步骤制定响应计划。

ServiceNow	使用 AWS 服务管理连接器，您可以将 Incident Manager 与ServiceNow基于云的第三方工作流程平台集成。 配置集成后 ServiceNow，当您在事件管理器中创建新事件时，集成还会在中 ServiceNow 创建事件。如果您在 “事件管理器” 中更新事件，它会对中相应的事件进行这些更新 ServiceNow。如果您在事件管理器或中解决事件 ServiceNow，则集成将根据您配置的首选项来解决这两个服务中的事件。 有关更多信息，请参阅《AWS 服务管理连接器管理员指南》 AWS Systems Manager Incident Manager ServiceNow中的 “集成”。
Slack	Slack 提供基于云的协作工具，用于团队消息、音频和视频会议以及文件共享。 您可以在 AWS Chatbot 中为 Slack 创建聊天频道，然后将该频道添加到响应计划中，从而将 Slack 频道集成到 Incident Manager 操作中。 有关更多信息，请参阅在 Incident Manager 中使用聊天频道。

Terraform	HashiCorp Terraform 是一种开源基础设施即代码 (IaC) 软件工具，它提供命令行界面 (CLI) 工作流程来管理各种云服务。对于 Incident Manager，您可以使用 Terraform 来管理或提供以下内容： SSM 事件管理器联系人资源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • awssmcontacts_rotation SSM 联系人数据源 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • awssmcontacts_rotation SSM Incident Manager 资源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM Incident Manager 数据来源 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中

PagerDuty 为响应计划开启与集成后，事件管理器将按以下 PagerDuty 方式使用：

- PagerDuty 当您在事件管理器中创建新事件时，事件管理器会在中创建相应的事件。

- PagerDuty 环境中使用您在中 PagerDuty 创建的寻呼工作流程和升级策略。但是，事件管理器不会导入您的 PagerDuty 配置。
- 事件管理器将时间轴事件作为事件的注释发布 PagerDuty，最多 2,000 个注释。
- 在事件管理器中解决相关 PagerDuty 事件时，您可以选择自动解决事件。

要将 Incident Manager 与集成 PagerDuty，您必须先在中创建一个 AWS Secrets Manager 包含您的 PagerDuty 凭据的密钥。这些允许事件管理器与您的 PagerDuty服务进行通信。然后，您可以在事件管理器中创建的响应计划中包含 PagerDuty 服务。

您在 Secrets Manager 中创建的该密钥必须以正确的 JSON 格式包含以下内容：

- 来自您 PagerDuty 账户的 API 密钥。您可以使用通用访问 REST API 密钥，也可以使用用户令牌 REST API 密钥。
- 您的 PagerDuty 子域中的有效用户电子邮件地址。
- 您部署子域名的 PagerDuty 服务区域。

> **Note**
>
> PagerDuty 子域中的所有服务都部署到同一个服务区域。

先决条件

在 Secrets Manager 中创建密钥前，请确保您满足以下要求。

KMS 密钥

您必须使用在 AWS Key Management Service (AWS KMS) 中创建的客户托管密钥对您创建的密钥进行加密。您在创建存储 PagerDuty 凭证的密钥时指定此密钥。

> **Important**
>
> Secrets Manager 提供了使用加密密钥的选项 AWS 托管式密钥，但不支持这种加密模式。

客户托管式密钥必须满足以下要求：

- 密钥类型：选择对称。
- 密钥用法：选择加密和解密。

- 区域性：如果要将响应计划复制到多个区域 AWS 区域，请确保选择多区域密钥。

密钥策略

配置响应计划的用户必须拥有密钥基于资源的策略的 kms:GenerateDataKey 和 kms:Decrypt 权限。ssm-incidents.amazonaws.com 服务主体必须拥有密钥基于资源的策略的 kms:GenerateDataKey 和 kms:Decrypt 权限。

以下策略说明了这些权限。将每个*#######*替换为您自己的信息。

```
{
    "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": "*"
        }
    ]
}
```

有关创建客户托管式密钥的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建对称加密 KMS 密钥。有关 AWS KMS 密钥的更多信息，请参阅AWS KMS 概念。

如果现有的客户托管式密钥满足之前的所有要求，则可以编辑其策略以添加这些权限。有关在客户托管式密钥中更新策略的信息，请参阅《AWS Key Management Service 开发人员指南》中的更改密钥策略。

> **Tip**
>
> 您可以指定条件密钥来进一步限制访问权限。例如，以下策略允许通过 Secrets Manager 访问美国东部（俄亥俄州）区域 (us-east-2) 中的 Secrets Manager：
>
> ```
> {
>     "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` 许可

创建响应计划的 IAM 身份（用户、角色或群组）必须拥有 IAM 权限 `secretsmanager:GetSecretValue`。

将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中

1. 按照《AWS Secrets Manager 用户指南》中创建 AWS Secrets Manager 密钥中的步骤 3a 中的步骤进行操作。
2. 在步骤 3b 中，对于密钥/值对，请执行以下操作：
   - 选择纯文本选项卡。
   - 将方框中的默认内容替换为以下 JSON 结构：

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

   - 在您粘贴的 JSON 示例中，按如下方式替换####：
     - *pagerduty-token*：您账户中的通用访问权限 REST API 密钥或用户令牌 REST API 密钥的值。 PagerDuty

       有关相关信息，请参阅PagerDuty 知识库中的 API 访问密钥。
     - *pagerduty-re* gion：托管您的子域 PagerDuty 的数据中心的服务区域。 PagerDuty

       有关相关信息，请参阅PagerDuty 知识库中的服务区域。
     - *pagerduty-emai* l：属于您的子域的用户的有效电子邮件地址。 PagerDuty

       有关相关信息，请参阅PagerDuty 知识库中的管理用户。

     以下示例显示了包含所需 PagerDuty凭据的完整的 JSON 密钥：

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

3. 在步骤 3c 中，对于加密密钥，选择您创建的符合上一部分先决条件中所列要求的客户托管式密钥。
4. 在步骤 4c 中，对于资源权限，请执行以下操作：
   - 展开资源权限。

- 选择编辑权限。
- 将策略方框中的默认内容替换为以下 JSON 结构：

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

- 选择保存。

5. 在步骤 4d 中，对于复制密钥，如果将响应计划复制到多个 AWS 区域，请执行以下操作：
   - 展开复制密钥。
   - 对于 AWS 区域，选择在其中复制响应计划的区域。
   - 对于加密密钥，请选择在该区域创建或复制到该区域的符合先决条件部分所列要求的客户托管式密钥。
   - 对于每增加一个 AWS 区域，请选择添加区域，然后选择区域名称和客户托管密钥。
6. 完成《AWS Secrets Manager 用户指南》中创建 AWS Secrets Manager 密钥中的其余步骤。

有关如何将 PagerDuty 服务添加到 Incident Manager 事件工作流程的信息，请参阅主题中的将 PagerDuty 服务集成到响应计划中制定响应计划。

相关信息

如何使用 PagerDuty 和实现事件响应自动化 AWS Systems Manager Incident Manager（AWS Cloud 运营和迁移博客）

《AWS Secrets Manager 用户指南》中的在 AWS Secrets Manager 中的密钥加密

对 AWS Systems Manager Incident Manager 进行故障排除

如果您在使用 AWS Systems Manager Incident Manager 时遇到问题，则可使用以下信息根据最佳实践来解决问题。如果以下信息未涵盖您遇到的问题，或者在您尝试解决问题后问题仍然存在，请联系AWS Support。

主题

错误消息：ValidationException – We were unable to validate the AWS Secrets Manager secret

问题 1：创建响应计划的 AWS Identity and Access Management (IAM) 身份（用户、角色或群组）没有 `secretsmanager:GetSecretValue` IAM 权限。IAM 身份必须拥有此权限才能验证 Secrets Manager 密钥。

- 解决方案：将缺少的 `secretsmanager:GetSecretValue` 权限添加到创建响应计划的 IAM 身份的 IAM 策略中。有关信息，请参阅《IAM 用户指南》中的添加 IAM 身份权限（控制台）或添加 IAM 策略 (AWS CLI)。

问题 2：该密钥没有附加允许 IAM 身份运行`GetSecretValue`操作的基于资源的策略，或者基于资源的策略拒绝给予该身份权限。

- 解决方案：在密钥的基于资源的策略中创建或添加一条 `Allow` 声明，授予 IAM 身份的 `secrets:GetSecretValue` 权限。或者，如果使用的 `Deny` 语句包含 IAM 身份，则更新策略，以便该身份可以运行该操作。有关信息，请参阅《AWS Secrets Manager 用户指南》中的为 AWS Secrets Manager 密钥附加权限策略。

问题 3：这些密钥没有附加允许访问 Incident Manager 服务主体 `ssm-incidents.amazonaws.com` 的基于资源的策略。

- 解决方案：创建或更新密钥的基于资源的策略，并包含以下权限：

```
{
```

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

问题 4：选定加密密钥的 AWS KMS key 不是客户托管式密钥，或者选定客户托管式密钥不向 Incident Manager 服务主体提供 IAM 权限 `kms:Decrypt` 和 `kms:GenerateDataKey*`。或者，创建响应计划的 IAM 身份可能没有 IAM 权限`GetSecretValue`。

- 解决方案：确保您满足主题将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中中先决条件下所述的要求。

问题 5：包含通用访问 REST API 密钥或用户令牌 REST API 密钥的密钥 ID 无效。

- 解决方案：确保您正确输入了 Secrets Manager 密钥的 ID，不留空格。您必须在存储您要使用的密钥的同一个 AWS 区域 中工作。您不能使用已删除的密钥。

问题 6：在极少数情况下，Secrets Manager 服务可能会遇到问题，或者 Incident Manager 可能无法与其通信。

- 解决方案：请等待几分钟，然后重试。查看AWS Health Dashboard是否存在可能影响任一服务的问题。

对其他问题进行故障排除

如果前面的步骤未能解决您的问题，则可以从以下资源中获得更多帮助：

- 有关访问 Incident Manager 控制台时 Incident Manager 特有的 IAM 问题，请参阅 对 AWS Systems Manager Incident Manager 身份和访问进行故障排除。
- 有关访问 AWS Management Console 时的一般身份验证和授权问题，请参阅《IAM 用户指南》中的对 IAM 进行故障排除

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

Incident Manager 的文档历史记录

变更	说明	日期
更新托管策略 AWSIncidentManagerIncidentAccessServiceRolePolicy	事件管理器为AWSIncidentManagerIncidentAccessServiceRolePolicy 支持调查结果功能添加了一项新权限，允许其检查 EC2 实例是否属于 Auto Scaling 组。有关更多信息，请参阅事件管理器对 AWS 托管策略的更新。	2024年2月20日
其他 HashiCorp Terraform 支持：待命轮换	Terraform 增加了对事件管理器的支持。现在，您可以使用 Terraform 配置或管理事件管理器待命资源。有关此集成以及其他第三方与 Incident Manager 集成的信息，请参阅与其他产品和服务的集成。	2024 年 2 月 2 日
新功能：来自其他人的发现 AWS 服务	调查结果为您提供了与 AWS CloudFormation 堆栈和 AWS CodeDeploy 部署相关的更改的信息，这些更改是在事件管理器中创建事件的同时发生的。在 Incident Manager 控制台中，您可以查看有关这些更改的摘要信息，在许多情况下，还可以访问 CloudFormation 或 CodeDeploy 控制台的链接，以获取有关变更的完整详细信息。调查发现缩短了评估潜在事件原因所需的时间。它们还能降低响应者在调	2023 年 11 月 15 日

	查事件原因时访问错误账户或控制台的几率。此功能还引入了新的托管策略`AWSIncidentManagerIncidentAccessServiceRolePolicy` ，该策略允许事件管理员读取其他资源 AWS 服务 以识别与事件相关的发现。有关更多信息，请参阅以下主题： • 处理调查发现 • AWS 托管策略：AWSIncidentManagerIncidentAccessServiceRolePolicy	
更新了与 Incident Manager 的集成列表	产品和服务与 Incident Manager 的集成主题已扩展到列出并描述了您可以与 Incident Manager 集成到事件检测和响应操作中的所有 AWS 服务 和第三方工具。	2023 年 6 月 9 日

与集成 AWS Trusted Advisor	Trusted Advisor 现在可以检查复制集的配置是否使用多个复制集 AWS 区域 来支持区域故障转移和响应。对于由 CloudWatch警报或 EventBridge 事件创建的事件，事件管理器会创建与警报或事件规则 AWS 区域 相同的事件。如果 Incident Manager 暂时在该区域不可用，则系统会尝试在复制集中的另一个区域中创建事件。如果复制集仅包含一个区域，则在 Incident Manager 不可用时，系统将无法创建事件记录。为帮助避免这种情况，会在仅为一个区域配置复制集时进行 Trusted Advisor 报告。有关使用 Trusted Advisor 的信息，请参阅《AWS Support 用户指南》中的 AWS Trusted Advisor。	2023 年 4 月 28 日

在响应计划中使用 Microsoft Teams 作为聊天频道	通过与 Microsoft Teams 集成 AWS Chatbot，你现在可以在响应计划中使用微软 Teams 作为聊天频道。此外，还支持 Slack 和 Amazon Chime 聊天频道。事件发生期间，Incident Manager 将状态通知直接发送到聊天频道，让所有响应者随时了解情况。响应者还可以相互通信，并在 Microsoft Teams 应用程序 AWS CLI 中使用与事件相关的命令，以更新事件并与之交互。有关更多信息，请参阅在 Incident Manager 中使用聊天频道。	2023 年 4 月 4 日
新特征：待命时间表	Incident Manager 中的待命时间表定义了当发生需要操作员干预的事件时，谁会收到通知。待命时间表由您为该时间表创建的一个或多个轮换组成。每次轮换最多可包括 30 个联系人。创建待命时间表后，您可以将其作为上报纳入上报计划中。当发生与该上报计划相关的事件时，Incident Manager 会根据时间表通知待命的操作员（或多名操作员）。有关更多信息，请参阅在 Incident Manager 中使用待命时间表。	2023 年 3 月 28 日

打印格式化的事件分析或另存为 PDF	事件分析页面现在包含一个打印按钮，可生成格式适合打印的分析版本。使用为设备配置的打印机目的地，可以将事件分析保存为 PDF 格式，或发送到本地或网络打印机。有关更多信息，请参阅打印格式化 Incident Analysis。	2023 年 1 月 17 日
PagerDuty 集成：事件管理器现在可以将事件时间轴事件复制到 PagerDuty事件	当您在响应计划 PagerDuty 中启用与的集成时，事件管理器会将根据该计划创建的时间轴事件添加到中的相应事件记录中 PagerDuty。 PagerDuty 将时间轴事件添加为事件的注释，最多 2,000 个注释。要了解有关这些更改的更多信息，请参阅以下主题： • 将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中 • 将 PagerDuty 服务整合到响应计划中	2022 年 12 月 15 日
事件管理器与 CloudWatch 指标集成。	现在，您可以在中发布与事件相关的指标。 CloudWatch有关更多信息，请参阅CloudWatch指标。包含 AWSIncidentManagerServiceRolePolicy 一项额外的权限，允许我们的服务代表您发布指标。	2022 年 12 月 15 日

启动事件备注并更新事件详细信息屏幕	您可以使用事件备注与其他处理事件的用户进行协作和沟通。此外，您还可以从事件详细信息屏幕查看运行手册和互动状态。有关更多信息，请参阅事件详细信息。	2022 年 11 月 16 日
将 PagerDuty 上报计划和寻呼工作流程整合到事件管理器响应计划中	现在，您可以将事件管理器与响应计划集成， PagerDuty 并将 PagerDuty 服务添加到响应计划中。配置集成后，事件管理器可以在事件管理器中 PagerDuty 为每个新事件创建相应的事件。 PagerDuty 使用您在 PagerDuty 环境中定义的寻呼工作流程和升级策略。 有关更多信息，请参阅以下主题： • 产品和服务与 Incident Manager 集成 • 将 PagerDuty 访问凭证存储在 AWS Secrets Manager 密钥中 • 将 PagerDuty 服务集成到主题中的响应计划中 制定响应计划 • 故障排除	2022 年 11 月 16 日
启动事件备注并更新事件详细信息屏幕。	您可以使用事件备注与其他处理事件的用户进行协作和沟通。此外，您还可以从事件详细信息屏幕查看运行手册和互动状态。有关更多信息，请参阅事件详细信息。	2022 年 11 月 16 日

为复制集提供标记支持	现在，您可以在 AWS Systems Manager Incident Manager 中为复制集分配标签。这增加了对为复制集中 AWS 区域 指定的响应计划、事件记录和联系人分配标签的现有支持。有关信息，请参阅以下主题： • 准备向导 • 标记 Incident Manager 资源	2022 年 11 月 2 日
Incident Manager 与 Atlassian Jira Service Management 集成	您可以使用适用于 Jira 服务管理的服务管理连接器，将事件管理器与 Jira 服务管理集成。AWS 配置集成后，在 Incident Manager 中创建的新事件会在 Jira 中创建相应的事件。如果您在 Incident Manager 中更新事件，则更新会添加到 Jira 中的相应事件中。如果您在 Incident Manager 或 Jira 中解决事件，则相应的事件也会根据配置的首选项得到解决。有关更多信息，请参阅《AWS 服务管理连接器管理员指南》中的配置 Jira Service Management。	2022 年 10 月 6 日
增强标记支持	事件管理器支持为复制集中 AWS 区域 指定的响应计划、事件记录和联系人分配标签。Incident Manager 还支持自动为根据响应计划创建的事件分配标签。有关更多信息，请参阅标记 Incident Manager 资源。	2022 年 6 月 28 日

事件管理器与 ServiceNow	您可以使用 AWS 服务管理连接器将事件管理器与ServiceNow集成 ServiceNow。配置集成后，在事件管理器中创建的新事件将在中创建相应的事件 ServiceNow。如果您在事件管理器中更新事件，则更新将添加到中的相应事件中 ServiceNow。如果您在事件管理器或中解决事件 ServiceNow，则相应的事件也会根据配置的首选项得到解决。有关更多信息，请参阅中的集成 AWS Systems Manager 事件管理器 ServiceNow。	2022 年 6 月 9 日
导入联系人详细信息	创建事件后，Incident Manager 可以使用语音或短信通知来通知响应者。为确保响应者看到来电或短信通知来自 Incident Manager，我们建议所有响应者将 Incident Manager 虚拟卡片格式 (.vcf) 文件下载到其移动设备上的通讯录中。有关更多信息，请参阅将联系人详细信息导入通讯录。	2022 年 5 月 18 日

多项特征改进，可增强事件创建和补救能力	Incident Manager 推出了以下特征改进，以增强事件的创建和补救能力： • 在其他地区自动创建事件 AWS 区域：如果 Amazon CloudWatch 或 Amazon EventBridge 创建事件 AWS 区域 时事件管理器不可用，这些服务现在会自动在您的复制集中指定的可用区域之一创建事件。有关更多信息，请参阅跨区域事件管理。 • 使用事件元数据自动填充运行手册参数：现在，您可以将事件管理器配置为从事件中收集有关 AWS 资源的信息。然后，Incident Manager 可以用收集到的信息填充运行手册参数。有关更多信息，请参阅教程：将 Systems Manager Automation 运行手册与 Incident Manager 一起使用。 • 自动收集 AWS 资源信息：当系统创建事件时，事件管理器现在会自动收集有关事件中涉及的 AWS 资源的信息。然后，Incident Manager 将此信息添加到相关项目选项卡中。	2022 年 5 月 17 日

多个运行手册支持	Incident Manager 现在支持在事件发生期间为事件详细信息页面运行多个运行手册。	2022 年 1 月 14 日
事件管理器在新版本中推出 AWS 区域	Incident Manager 现在已在这些新区域可用：us-west-1、sa-east-1、ap-northeast-2、ap-south-1、ca-central-1、eu-west-2 和 eu-west-3。有关 Incident Manager 区域和配额的更多信息，请参阅《AWS 一般参考 参考指南》https://docs.aws.amazon.com/general/latest/gr/incident-manager.html。	2021 年 11 月 8 日
控制台互动确认	现在，您可以直接从 Incident Manager 控制台确认互动。	2021 年 8 月 5 日
属性选项卡	Incident Manager 在事件详细信息页面中引入了一个属性选项卡，提供了有关事件 OpsItem、父事件和相关事后分析的更多信息。	2021 年 8 月 3 日
Incident Manager 启动	事件管理器是一个事件管理控制台，旨在帮助用户缓解影响其 AWS 托管应用程序的事件并从中恢复过来。	2021 年 5 月 10 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。