AWS 事件检测及响应服务概念和程序

AWS 事件检测及响应服务用户指南

版本 May 26, 2026

AWS 事件检测及响应服务用户指南: AWS 事件检测及响应服务概念和程序

Table of Contents

什么是 AWS 事件检测及响应服务？ 1
注册 AWS 账户 1
使用条款 2
架构 2
角色和责任 3
区域可用性 4
开始使用 7
关于工作负载 7
关于警报 7
加入工作负载 7
使用 IDR CLI 加入 8
警报摄取 8
摄取警报的步骤 9
摄取警报的替代选项 9
预置访问权限 9
警报定义 10
警报优化 28
警报审核 29
警报上线 29
接入问卷（异常路径） 30
工作负载加入问卷 - 一般问题 30
工作负载加入问卷 - 架构问题 31
警报摄取问卷 - 概述 31
警报摄取问卷 - 运行手册问题 32
警报矩阵 33
管理工作负载 36
创建运行手册和响应计划 36
测试已加入的工作负载 41
测试选项 41
如何测试警报 42
关键成果 43
常见问题 44
请求对工作负载进行更改 44
抑制警报 45

在警报源抑制警报 46
提交工作负载更改请求来抑制警报 50
教程：使用指标数学函数抑制警报 51
教程：移除指标数学函数来抑制警报 52
移除工作负载 53
监控和可观测性 55
实施可观测性 55
事件管理 57
为应用程序团队预置访问权限 59
创建事件响应请求 59
通过 AWS Support Center Console创建请求 60
通过 AWS 支持 API 创建请求 61
通过 AWS Support App in Slack创建请求 61
使用 AWS Support App in Slack管理事件检测及响应服务支持案例 62
Slack 中的警报发起事件通知 63
在 Slack 中创建事件响应请求 63
报告 64
安全性与韧性 65
对您账户的访问权限 65
您的警报数据 66
文档历史记录 67

什么是 AWS 事件检测及响应服务？

AWS 事件检测及响应服务支持符合条件的 AWS Enterprise Support 客户主动参与事件，以降低发生故障的可能性，并加速恢复出现中断的关键工作负载。事件检测及响应服务有助于您与 AWS 协作，一同针对加入该服务的每项工作负载定制相应的运行手册和响应计划。

事件检测及响应服务具备以下关键特性：

- 提升可观测性：AWS 专家将为您提供指导，协助您在工作负载的应用程序层和基础设施层之间定义并关联指标和警报，从而尽早检测到中断行为。
- 5 分钟响应时间：事件管理工程师在收到警报后的 5 分钟内，根据您的工作负载或您提交的关键案例，主动与您联系。
- 加快事件解决速度：IME 使用专为您的工作负载制定的预定义和自定义运行手册，代表您创建支持案例，以及管理您工作负载的事件。IME 为事件提供单线程所有权，确保您与合适的 AWS 专家接洽，直到事件得到解决。
- 降低发生故障的可能性：事件得到解决后，IME 会应您的要求提供事后审查。而且，AWS 专家将会与您协作，运用相关的经验教训来完善事件响应计划和运行手册。您还可以利用 AWS Resilience Hub对您的工作负载进行持续的韧性跟踪。

主题

- 注册 AWS 账户
- 事件检测及响应服务的使用条款
- 事件检测及响应服务的架构
- 事件检测及响应服务中的角色和职责
- 事件检测及响应服务的区域可用性

注册 AWS 账户

要开始使用 AWS，您需要 AWS 账户。有关创建 AWS 账户的信息，请参阅《AWS 账户管理 参考指南》中的 AWS 账户入门指南。

事件检测及响应服务的使用条款

以下列表概述了使用 AWS 事件检测及响应服务的主要要求和限制。在使用该服务之前，请务必了解这些信息，因为它涵盖了支持计划要求、加入流程以及最短订阅期限等方面。

- AWS 事件检测及响应服务适用于直接账户和合作伙伴转售的 Enterprise Support 账户。
- AWS 事件检测及响应服务不适用于合作伙伴指导支持计划的账户。
- 在事件检测及响应服务期限内，您必须始终维护 AWS Enterprise Support。有关信息，请参阅 Enterprise Support。终止 Enterprise Support 会导致同时从 AWS 事件检测及响应服务中移除。
- AWS 事件检测及响应服务中的所有工作负载均须完成工作负载加入流程。
- 订阅 AWS 事件检测及响应服务账户的最短期限为九十（90）天。所有取消申请必须在目标取消生效日期前三十（30）天提交。
- AWS 会按照 AWS 隐私声明中的说明处理您的信息。

> **Note**
>
> 有关事件检测及响应服务计费相关的问题，请参阅获取 AWS 账单帮助。

事件检测及响应服务的架构

AWS 事件检测及响应服务与您的现有环境集成（如下图所示）。该架构包括以下服务：

- Amazon EventBridge：Amazon EventBridge 是您工作负载与 AWS 事件检测及响应服务之间的唯一集成点。警报是使用 AWS 管理的预定义规则，通过 Amazon EventBridge 从您的 Amazon CloudWatch 之类的监控工具摄取的。要让事件检测及响应服务能够构建和管理 EventBridge 规则，您需要安装服务相关角色。要详细了解这些服务，请参阅什么是 Amazon EventBridge 和 Amazon EventBridge 规则、什么是 Amazon CloudWatch，以及使用 AWS Health 的服务相关角色。
- AWS Health：AWS Health 可持续监控资源性能以及 AWS 服务和账户的可用性。事件检测及响应服务使用 AWS Health 跟踪您的工作负载所使用的 AWS 服务上的事件，并在收到来自您工作负载的警报时向您发送通知。要了解有关 AWS Health 的更多信息，请参阅什么是 AWS Health。
- AWS Systems Manager：Systems Manager 提供了一个统一的用户界面，用于跨 AWS 资源实现自动化和任务管理。AWS 事件检测及响应服务在 AWS Systems Manager 文档中托管有关您的工作负载的信息，包括工作负载架构详细信息、警报详细信息及其相应的事件管理运行手册（有关详细信

息，请参阅 AWS Systems Manager 文档）。要了解有关 AWS Systems Manager 的更多信息，请参阅什么是 AWS Systems Manager。

- 具体的运行手册：事件管理运行手册定义了 AWS 事件检测及响应服务在事件管理期间执行的操作。具体的运行手册会告知 AWS 事件检测及响应服务应联系谁、如何联系他们以及要共享哪些信息。

事件检测及响应服务中的角色和职责

AWS 事件检测及响应服务 RACI（负责、问责、咨询和知情）表概述了与事件检测及响应相关的各种活动的角色和职责。此表有助于针对诸如数据收集、运营准备就绪审查、账户配置、事件管理和事后审查等任务定义客户和 AWS 事件检测及响应服务团队的参与情况。

活动	Customer	Incident Detection and Response
数据收集		
客户和工作负载介绍	咨询	负责
架构	负责	问责
操作	负责	问责
确定要配置的 CloudWatch 警报	负责	问责
定义事件响应计划	负责	问责
运营准备就绪审查		
对工作负载执行 Well Architected 审查（WAR）	咨询	负责
验证事件响应	咨询	负责
验证警报矩阵	咨询	负责
确定工作负载所用的关键 AWS 服务	问责	负责

活动	Customer	Incident Detection and Response
账户配置		
在客户账户中创建 IAM 角色	负责	知情
使用创建的角色安装托管 EventBridge 规则	知情	负责
测试已加入的警报（CloudWatch 或 APM）	问责	知情
确认客户警报触发事件检测及响应	知情	负责
更新警报	负责	咨询
更新运行手册	咨询	负责
事件管理		
主动通知事件检测及响应服务检测到的事件	知情	负责
提供事件响应方案	知情	负责
提供事件解决方案/基础设施恢复方案	负责	咨询
事后审查		
请求事后审查	负责	知情
提供事后审查方案	知情	负责

事件检测及响应服务的区域可用性

对于托管在以下任一 AWS 区域中的 AWS Enterprise Support 账户，AWS 事件检测及响应服务提供英语、日语、普通话和韩语版本：

AWS 区域	名称
美国东部（弗吉尼亚北部）区域	us-east-1
美国东部（俄亥俄）区域	us-east-2
美国西部（北加利福尼亚）区域	us-west-1
美国西部（俄勒冈州）区域	us-west-2
加拿大（中部）区域	ca-central-1
Canada West（Calgary）Region	ca-west-1
南美洲（圣保罗）区域	sa-east-1
欧洲（法兰克福）区域	eu-central-1
欧洲地区（爱尔兰）区域	eu-west-1
欧洲（伦敦）区域	eu-west-2
欧洲（巴黎）区域	eu-west-3
欧洲地区（斯德哥尔摩）区域	eu-north-1
欧洲（苏黎世）	eu-central-2
欧洲地区（米兰）	eu-south-1
欧洲（西班牙）区域	eu-south-2
亚太地区（孟买）	ap-south-1
亚太地区（东京）	ap-northeast-1
亚太地区（首尔）	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2

AWS 区域	名称
亚太地区（香港）	ap-east-1
亚太地区（大阪）	ap-northeast-3
亚太地区（海得拉巴）	ap-south-2
亚太地区（雅加达）	ap-southeast-3
亚太地区（墨尔本）	ap-southeast-4
亚太地区（马来西亚）	ap-southeast-5
非洲（开普敦）	af-south-1
以色列（特拉维夫）	il-central-1
中东（阿联酋）	me-central-1
中东（巴林）	me-south-1
AWS GovCloud（美国东部）	us-gov-east-1
AWS GovCloud（美国西部）	us-gov-west-1

事件检测及响应服务入门

工作负载和警报是 AWS 事件检测及响应服务的核心。AWS 将与您密切合作，共同确定和监控对您的业务至关重要的特定工作负载。AWS 将协助您设置相关警报，以便将重大性能问题或客户影响通知给您的团队。正确配置警报对于在事件检测及响应服务中主动监控和快速响应事件而言至关重要。

关于事件检测及响应服务中的工作负载

您可以选择要用于使用 AWS 事件检测及响应服务进行监控和关键事件管理的具体工作负载。工作负载是一系列资源和代码，它们协同工作，共同致力于提供业务价值。工作负载可能是构成银行支付门户或客户关系管理（CRM）系统的所有资源和代码。您可以通过单个 AWS 账户或多个 AWS 账户来托管工作负载。

例如，您可以在单个账户中托管一个单体应用程序（例如，下图中的员工绩效应用程序）。或者，您也可以将一个应用程序（例如图中的 Storefront Webapp）细分成微服务托管在不同的账户中。工作负载可能会与其它应用程序或工作负载共享数据库等资源，如下图所示。

要开始进行工作负载接入，请参阅将工作负载加入到事件检测及响应服务。

关于事件检测及响应服务中的警报

警报是事件检测及响应服务的关键部分。警报可让您了解应用程序和底层 AWS 基础设施的性能。AWS 与您协作，共同确定适当的指标和警报阈值，只有当您受监控的工作负载受到严重影响时，才会触发这些指标和警报阈值。目标是让警报引起您指定的事件解决人员的注意，然后他们将会与事件管理团队协作，来快速为您缓解问题。将您的警报配置为仅在性能或客户体验显著降级而需要立即关注时才进入警报状态。一些主要警报类型包括指示业务影响的警报、Amazon CloudWatch 金丝雀警报和监控依赖关系的聚合警报等。

要开始进行警报摄取，请参阅警报摄取。

将工作负载加入到事件检测及响应服务

借助 AWS 事件检测及响应服务，可以对选择的工作负载进行监控和关键事件管理。工作负载是协同工作以交付业务价值的资源集合，例如支付门户或客户关系管理（CRM）系统。您可以将这些工作负载托管在单个 AWS 账户中，也可以将其分布在多个账户中，具体取决于您的架构。

目录

- 使用 IDR CLI 加入到事件检测及响应服务

- IDR CLI 的语言支持
- 接入工作负载的替代选项

使用 IDR CLI 加入到事件检测及响应服务

AWS 事件检测及响应服务客户命令行界面（IDR CLI）是一款命令行界面工具，可简化接入到 AWS 事件检测及响应服务的过程。

IDR CLI 在 AWS CloudShell 中运行以执行以下功能：

- 收集接入信息
- 通过资源组标记 API 收集 AWS 资源数据
- 管理 AWS 支持 案例
- 创建新的 Amazon CloudWatch 警报或摄取现有警报
- 通过 AWS CloudFormation 部署和测试基础设施，以支持第三方工具向事件检测及响应服务发送警报。

IDR CLI 可以在交互模式下运行以指导您完成接入步骤，也可以在离线模式下运行来处理批量或 DevOps 使用案例。

有关如何使用 IDR CLI 的更多信息，包括安装、先决条件和端到端示例，请参阅 AWS 事件检测及响应服务的 CLI。

IDR CLI 的语言支持

AWS 事件检测及响应服务提供英语、日语、普通话和韩语版本。如果您需要日语、普通话或韩语支持，请通过 IDR CLI 创建的 AWS 支持 案例联系 AWS，或者联系您的技术客户经理（TAM）。

接入工作负载的替代选项

如果您无法使用 IDR CLI 来接入，请咨询您的技术客户经理（TAM），了解替代选项。有关更多信息，请参阅 事件检测及响应服务中的工作负载接入问卷和警报摄取问卷（异常路径）。

警报摄取

AWS 事件检测及响应服务客户命令行界面（IDR CLI）可以创建新的 Amazon CloudWatch 警报或摄取现有警报，并可以通过 AWS CloudFormation 部署和测试基础设施，以支持第三方工具向 AWS 事件检测及响应服务发送警报。

AWS 事件检测及响应服务可以通过 Amazon EventBridge 从 Amazon CloudWatch 和第三方应用程序性能监控（APM）工具摄取警报：

- 摄取 CloudWatch 警报
- 摄取第三方应用程序性能监控警报

摄取警报的步骤

需要完成以下步骤才能摄取警报：

- 警报定义
- 使用 IDR CLI 摄取警报
- 警报审核和反馈
- 预调配将警报摄取到事件检测及响应服务所需的访问权限
- 警报上线

摄取警报的替代选项

如果您无法使用 IDR CLI 来摄取警报，请咨询您的技术客户经理（TAM），了解替代选项。有关更多信息，请参阅 事件检测及响应服务中的工作负载接入问卷和警报摄取问卷（异常路径）。

预调配将警报摄取到事件检测及响应服务所需的访问权限

> **Note**
>
> 如果您未在 IDR CLI 接入期间创建服务相关角色（SLR），请按照以下步骤手动预调配访问权限。

要让 AWS 事件检测及响应服务能够从您的账户摄取警报，请创建 `AWSServiceRoleForHealth_EventProcessor` SLR。AWS 代入此 SLR，以便在您的账户中创建托管式 EventBridge 规则。此托管式 EventBridge 规则将通知从您的账户发送到 AWS 事件检测及响应服务。有关此 SLR（包括关联的 AWS 托管式策略）的信息，请参阅《用户指南》中的使用服务相关角色。

您可以按照《AWS Identity and Access Management 用户指南》的创建服务相关角色中的说明，在您的账户中创建此服务相关角色。或者，您也可以使用以下 AWS Command Line Interface（AWS CLI）命令：

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

主要输出

- 在您的账户中成功创建服务相关角色。

> **Note**
>
> 需要在您将用来向 AWS 事件检测及响应服务发送警报的每个账户中创建服务相关角色 AWSServiceRoleForHealth_EventProcessor。

相关信息

有关更多信息，请参阅以下主题：

- 将服务关联角色用于
- 创建服务相关角色
- AWS 托管策略：AWSHealth_EventProcessorServiceRolePolicy

警报定义

在将警报接入到 AWS 事件检测及响应服务时，您负责定义指标和警报配置，以供了解应用程序的性能。作为此过程的一部分，您还必须确定组织内负责响应这些警报的团队。

在准备警报时，建议您遵循以下最佳实践：

- 仅当受监控的工作负载受到持续的严重影响而需要您的团队和 AWS 立即关注时，警报才会进入“警报”状态。对于已触发但未自动恢复的警报，需要您的团队加入 AWS 事件检测及响应服务发起的事件沟通会议。
- 确保您提供的联系信息，能让 AWS 事件检测及响应服务全天候、可靠地联系到贵组织内的相应团队，并邀请他们加入事件沟通会议。

主要输出

- 您使用 IDR CLI 向 AWS 事件检测及响应服务提供的警报和联系详细信息列表。

有关定义和摄取 Amazon CloudWatch 警报的更多信息，请参阅摄取 CloudWatch 警报。

有关摄取第三方应用程序性能监控警报的更多信息，请参阅摄取第三方应用程序性能监控警报。

摄取 CloudWatch 警报

AWS 事件检测及响应服务可以摄取 Amazon CloudWatch 警报，来为您的关键工作负载提供主动监控。通过摄取您的 Amazon CloudWatch 警报来进行监控，AWS 事件检测及响应服务可以：

- 自动检测警报何时进入“警报”状态。
- 与您的团队联系，以协同响应和解决事件。

为了确保您加入的警报有效，AWS 事件检测及响应服务建议采用以下最佳实践：

- 使用指标数学表达式配置警报，以便在定期维护或批处理作业执行期间对其进行抑制，从而避免出现误报联系情形。
- 根据预期的数据点交付频率设置警报的缺失数据处理。例如，生成连续数据点流的警报监控指标应将缺失的数据视为“Breaching”（不良），因为缺失数据点可能表明所监控的底层资源存在问题。相反，不经常报告数据点的警报监控指标（例如，仅在发生故障或错误时才记录数据点的警报监控指标）应将缺失的数据视为 NotBreaching（良好）。
- 定义当工作负载受到严重、持续的影响时进入“警报”状态的警报。例如，将警报配置为在自动替换运行状况不佳的资源所需的预期时间之后触发，而不是在首次检测到运行状况不佳的资源时触发。
- 识别自定义指标并为其创建警报，这些指标直接代表您的工作负载的客户体验。

有关常见 AWS 服务的建议 Amazon CloudWatch 警报的列表，请参阅 AWS re:Post 上的事件检测及响应服务最佳实践。

摄取第三方应用程序性能监控警报

AWS 事件检测及响应服务支持通过 Amazon EventBridge 从第三方应用程序性能监控（APM）工具摄取警报。这一集成通过摄取 APM 警报提供了灵活性，支持通过不同的 AWS 服务将 APM 事件路由到您账户中的 Amazon EventBridge 事件总线。

集成路径示例：

- 来源（APM）→ AWS 服务（示例：Amazon API Gateway 或 Amazon SNS）→ 转换 Lambda 函数 → 自定义 Amazon EventBridge 事件总线 → AWS 事件检测及响应服务
- 来源（APM）→ 合作伙伴 Amazon EventBridge 事件总线 → 转换 Lambda 函数 → 自定义 Amazon EventBridge 事件总线 → AWS 事件检测及响应服务

AWS 事件检测及响应服务在自定义事件总线上安装托管式规则，用于摄取转换 Lambda 函数发送给它的警报。值得注意的是，对于 SaaS Amazon EventBridge 集成，合作伙伴事件总线不是安装了托管式规则的事件总线。有关与 Amazon EventBridge 的合作伙伴集成的 APM 的完整列表，请参阅 Amazon EventBridge integrations。

使用合作伙伴事件总线或其它 AWS 事件总线源进行集成的示例

下图显示了使用合作伙伴事件总线或其它 AWS 事件总线源进行集成的示例。

有关与 Amazon EventBridge 的合作伙伴集成的 APM 的完整列表，请参阅 Amazon EventBridge integrations。

使用 Amazon API Gateway 进行集成的示例

下图显示了使用 API Gateway 进行集成的示例。

使用 Amazon Simple Notification Service 进行集成的示例

下图显示了使用 Amazon SNS 进行集成的示例。

为了简化集成过程，AWS 事件检测及响应服务为最常用的集成类型提供了 CloudFormation 模板。这些模板可以自动设置 AWS 资源和必要的 IAM 角色。

CloudFormation可以在下面的相应集成文档中找到手动创建各种集成类型的 模板和说明：

- 从与 EventBridge 直接集成的 APM 摄取警报
- 从未与 EventBridge 直接集成的 APM 摄取警报
- 从与 Amazon SNS 直接集成的 APM 摄取警报

> **Note**
>
> CloudFormation 模板需要修改。前面的主题中对这些修改进行了说明。有关向 AWS 事件检测及响应服务发送 APM 警报所需的有效载荷格式的更多信息，请参阅使用 EventBridge 摄取 APM 警报的有效载荷要求。

使用 EventBridge 摄取 APM 警报的有效载荷要求

事件检测及响应服务从哪里摄取 APM 警报？

AWS 事件检测及响应服务会将托管式规则安装在事件总线上，而您会将转换后的最终有效载荷发送到该事件总线上。最好是为此目的创建自定义事件总线。

有效载荷必须采用什么格式？

AWS 事件检测及响应服务摄取的事件总线事件中需要以下最小的 JSON 键值对：

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

以下示例显示了来自合作伙伴事件总线的事件在转换前后的情况。

转换前：

```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "alert_type": "error",
        "event_type": "query_alert_monitor",
```

```
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
<= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
```

```
    }
}
```

请注意，在转换事件之前，detail-type 和 source 指明警报源自的 APM 详细信息。必须在摄取之前对其进行修改。incident-detection-response-identifier 键尚不存在，也必须在摄取前添加。

Lambda 函数转换上述事件并将其放入目标自定义或默认事件总线中。转换后的有效载荷必须包含所需的键值对。

转换后：

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "UnHealthyHostCount",
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 <= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
```

```
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

请注意，detail-type 现在是 ams.monitoring/generic-apm，源现在是 GenericAPMEvent，在详细信息下有新的键值对：incident-detection-response-identifier。

incident-detection-response-identifier 值是根据您的 APM 发送的有效载荷从警报名称中提取的。APM 警报名称路径因 APM 而异。必须设置 Lambda 函数，以便从 Lambda 收到的 APM JSON 有效载荷中的正确路径获取警报名称，并将其用于 incident-detection-response-identifier 值。

对于发送到 AWS 事件检测及响应服务的每种警报类型，incident-detection-response-identifier 值必须是唯一的。incident-detection-response-identifier 上设置的每个唯一名称必须在加入期间提供给 AWS 事件检测及响应服务团队。不处理其 incident-detection-response-identifier 键的值未知或缺失的事件。

从与 EventBridge 直接集成的 APM 摄取警报

下面的主题显示了从与 Amazon EventBridge 直接集成的应用程序性能监控（APM）工具向 AWS 事件检测及响应服务发送警报的过程。有关与 Amazon EventBridge 直接集成的 APM 的完整列表，请参阅 Amazon EventBridge integrations。

您可以部署所提供的 CloudFormation 模板或手动设置此集成。在设置集成之前，请确认在您的账户中创建了 AWS 服务相关角色（SLR）`AWSServiceRoleForHealth_EventProcessor`。

选项 1：使用 CloudFormation

可以使用 CloudFormation 模板来简化创建集成基础设施的过程，该基础设施是从与 Amazon EventBridge 集成的 APM 中将警报摄取到 AWS 事件检测及响应服务所必需的。

> **Note**
>
> - 通过此 CloudFormation 模板部署的资源（例如 Lambda 和 EventBridge）会产生额外费用。有关这些服务的定价的更多信息，请参阅 AWS 定价。
> - 在 AWS 事件检测及响应服务需要摄取警报的每个 AWS 账户和区域中部署此 CloudFormation 模板。事件和支持案例是在从中收到 APM 警报的 AWS 账户上开立的。
> - 本文档以 New Relic 为例，但是 CloudFormation 模板可用于任何将 SaaS 与 Amazon EventBridge 集成的 APM。
> - 测试集成后，从 `TransformLambdaFunction` 中移除 logger.info() 语句，以防止有效载荷出现在 Amazon CloudWatch Logs 中。

部署此 CloudFormation 模板的先决条件：

- 必须在 Amazon EventBridge 中设置合作伙伴事件源。有关将 APM 设置为事件源的说明，请参阅《Amazon EventBridge 用户指南》中的使用 Amazon EventBridge 从 SaaS 合作伙伴接收事件。
- 必须根据 APM 有效载荷中警报名称的 JSON 路径来修改模板中的 `TransformLambdaFunction`（Lambda 函数），以便将 `["detail"]["incident-detection-response-identifier"]` 设置为所需的值。

先决条件步骤：

1. 打开 EventBridge 控制台。在集成菜单下，选择合作伙伴事件源。
   - 在 Amazon EventBridge 合作伙伴框中搜索您的 APM。

- 选择设置，然后按照提供的说明进行操作。
  - 注意：最后一步是在控制台中为合作伙伴事件源选择与事件总线关联。选择此选项会自动创建与合作伙伴事件源同名的合作伙伴事件总线（名称必须匹配）。
- 复制合作伙伴事件总线或源的名称。部署 CloudFormation 模板时，事件总线或源用作名为 `PartnerEventBusNameParameter` 的参数。
  - New Relic 的示例：`aws.partner/newrelic.com/1234567/source_name`
- 部署 CloudFormation 模板时，复制合作伙伴事件总线或源的第一部分以输入到 `PartnerEventBusPrefixParameter` 中。
  - New Relic 的示例为 `aws.partner/newrelic.com`

2. 下载并编辑 CloudFormation 模板。
   - 在模板中找到 `TransformLambdaFunction`
   - 在 `def lambda_handler(event, context)` 下，将 `event["detail"]["incident-detection-response-identifier"]` 设置为 json 路径，在该路径中，警报名称出现在 APM 警报的 json 有效载荷中。每个 APM 都将有不同的路径。下面可以看到一些示例，但您的具体有效载荷可能会有所不同。
     - New Relic 示例：`event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`。
     - Datadog 示例：`event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
     - Splunk 示例：`event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
   - 保存 CloudFormation 模板。

部署 CloudFormation 模板：

1. 在您的目标账户和区域中打开 CloudFormation 控制台。
2. 依次选择“创建堆栈”、“使用新资源（标准）”
   - 选择选择现有模板、上传模板文件、选择文件，然后上传您本地保存的 CloudFormation 模板。
3. 指定堆栈详细信息：
   - 输入堆栈名称（示例：`NewRelicIntegrationForIDR`）。
   - 指定在完成先决条件期间获得的参数值。
     - APMNameParameter（示例：`NewRelic`）

    - PartnerEventBusNameParameter（示例：`aws.partner/newrelic.com/1234567/source_name`）
    - PartnerEventBusPrefixParameter（示例：`aws.partner/newrelic.com`）
  - 选择下一步。
4. 配置堆栈选项：
  - 滚动到页面底部，然后选中支持 CloudFormation 使用自定义名称创建 IAM 资源的框。
5. 审核和创建：
  - 验证参数值是否正确配置，然后选择提交。
6. CloudFormation 堆栈会部署必要的资源，来将您的 APM 事件集成到 AWS 事件检测及响应服务。等待堆栈状态显示 `CREATE_COMPLETE`。
7. 假设示例值已输入到 New Relic 的参数中并在 US-EAST-1 区域中运行，CloudFormation 堆栈会创建以下资源。
  - CustomEventBus：NewRelic-AWSIncidentDetectionResponse-EventBus
  - EventBridgeRule：aws.partner/newrelic.com/1234567/source_name|NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
  - TransformLambdaExecutionRole：IDR-TransformLambdaExecutionRole-us-east-1
  - TransformLambdaFunction：NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
  - TransformLambdaPermission：NewRelicIntegrationForIDR-TransformLambdaPermission-[random_string]

集成测试

部署堆栈后，通过从 APM 发送测试有效载荷来测试集成：

1. 导航到 Lambda 控制台并选择 `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 函数。选择监控选项卡。
2. 在指标图表中寻找成功的调用。
3. 选择查看 Amazon CloudWatch Logs，以检查日志流中是否有您的测试有效载荷或是否存在任何错误。

与 AWS 事件检测及响应服务共享您的事件总线 ARN

1. 打开 Amazon EventBridge 控制台。选择事件总线。

2. 复制作为 CloudFormation 堆栈一部分创建的自定义事件总线的 ARN（示例：*arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus*）。
   - 将此 ARN 添加到警报摄取问卷 - 概述的“第三方 APM 警报”部分中的“EventBridge 事件总线 ARN”字段。
3. 在接入过程中，AWS 事件检测及响应服务会在此自定义事件总线上创建托管式 EventBridge 规则，以摄取您的 APM 警报。

选项 2：手动集成

为 AWS 事件检测及响应服务需要从中摄取警报的每个 AWS 账户和 AWS 区域完成以下步骤。AWS 事件检测及响应服务建议在与您的应用程序资源相同的 AWS 账户和区域中设置警报，以便更快地识别和调查受影响的资源。事件和支持案例是在从中收到 APM 警报的 AWS 账户上开立的。

1. 通过将 APM 设置为 Amazon EventBridge 合作伙伴事件源，创建 EventBridge 合作伙伴事件总线（例如 `aws.partner/apm_name/integrationName`）。有关将 APM 设置为事件源的指南，请参阅使用 Amazon EventBridge 接收来自 SaaS 合作伙伴的事件。
2. 执行下列操作之一：
   - （建议）创建名为 `$YourApmName-AWSIncidentDetectionResponse-EventBus` 的 EventBridge 自定义事件总线。
   - （替代）使用默认的 EventBridge 事件总线，而非自定义事件总线。

   AWS 事件检测及响应服务将通过 `AWSServiceRoleForHealth_EventProcessor` SLR，在自定义或默认事件总线上安装托管式规则 (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`)。规则源将是自定义或默认事件总线，规则目标将是 AWS 事件检测及响应服务，而规则将与用于摄取第三方 APM 事件的模式相匹配。
3. 创建名为 `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` 的 Lambda 函数来转换您的合作伙伴事件总线事件。转换后的事件将与托管式规则 `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` 相匹配。
   - 转换后的事件包括唯一的 AWS 事件检测及响应服务标识符，并将事件的来源和详细信息类型设置为所需的值。这样，转换后的 JSON 有效载荷结构就会与托管式规则模式相匹配。
   - 将 Lambda 函数的目标设置为在步骤 2 中创建的自定义事件总线（建议）或设置为您的默认事件总线。

4. 创建 EventBridge 规则，并定义与您要推送到 AWS 事件检测及响应服务的事件列表相匹配的事件模式。规则的源是您在步骤 1 中创建的合作伙伴事件总线 (`aws.partner/apm_name/integrationName`)。规则的目标是您在步骤 3 中创建的 Lambda 函数 (`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`)。有关定义 EventBridge 规则的指南，请参阅 Amazon EventBridge 规则。

有关如何使用 AWS 事件检测及响应服务手动设置合作伙伴事件总线集成的分步示例，请参阅集成来自 Datadog 和 Splunk 的通知。

从未与 EventBridge 直接集成的 APM 摄取警报

AWS 事件检测及响应服务支持使用 Webhook 从未与 Amazon EventBridge 直接集成的第三方 APM 摄取警报。

您可以部署 CloudFormation 模板或手动设置集成。在设置集成之前，请确认在您的账户中创建了 AWS 服务相关角色（SLR）`AWSServiceRoleForHealth_EventProcessor`。

选项 1：使用 CloudFormation 模板

可以使用 CloudFormation 模板来简化创建集成基础设施的过程，该基础设施是从未与 Amazon EventBridge 直接集成的 APM 中将警报摄取到 AWS 事件检测及响应服务所必需的。

部署此 CloudFormation 模板之前的注意事项

- 此解决方案使用 API Gateway Lambda 授权方，来将在 APM 的有效载荷中传递的密钥令牌与 AWS Secrets Manager 中的令牌进行比较。如果令牌不匹配，则将返回带有显式拒绝的策略。有关更多信息，请参阅 Lambda 授权方。
- 在 AWS 责任共担模式下，您有责任确保您使用的身份验证方法符合组织的安全要求。我们建议使用 AWS Secrets Manager 或类似的服务，而不是将 API 密钥或授权令牌等敏感信息存储为硬编码变量。有关更多信息，请参阅使用 AWS Secrets Manager 创建和管理密钥。
- 有关实施 HMAC 散列消息认证码（HMAC）的其它示例，请参阅 aws-samples Github 页面上的 receive-webhooks。有关实施令牌授权的更多信息，请参阅 API Gateway 文档中的 TOKEN 授权方 Lambda 函数示例。
- 该解决方案使用 API Gateway 中的 RateLimit、BurstLimit 和 Quota 来控制请求量。这些工具限制了在设定的时间内可以处理的请求数量。这有助于防止系统过载并保持服务稳定。有关节流的更多信息，请参阅 API Gateway 开发人员指南。
- 考虑使用 AWS Web 应用程序防火墙（WAF）来保护 API Gateway 免受已知的错误 IP 地址侵害。这降低了攻击者向 API 发出大量虚假请求以阻止真实日志事件的风险。

- AWS Secrets Manager 令牌值应作为 HTTP 标头存储在应用程序性能监控（APM）工具中。作为最佳安全实践，请确保定期轮换令牌。
- 通过此 CloudFormation 模板部署的资源（例如：Lambda 和 EventBridge）将产生额外费用。有关这些服务的定价的更多信息，请参阅 AWS 定价。
- 测试集成后，从 `TransformLambdaFunction`（Lambda 函数）中移除 logger.info() 语句，以防止有效载荷出现在 Amazon CloudWatch Logs 中。
- 在 AWS 事件检测及响应服务需要从中摄取警报的每个 AWS 账户和区域中部署此 CloudFormation 模板。

准备 CloudFormation 模板：

注意：集成步骤以 Dynatrace 为例，但是此模板可用于任何可以向 API Gateway 发送有效载荷的 APM。

1. 下载并打开 CloudFormation 模板。
2. 在模板中找到 `APIGWUsagePlan`。查看为 `RateLimit`、`BurstLimit` 和 `Quota Limit` 配置的值，这些值默认设置为 20、50 和 2000。调整这些值以满足您的要求。
3. 在模板中找到 `AuthorizerLambdaFunction`。此 Lambda 函数用作身份验证机制的示例。它从名为 `authorizationToken` 的标头中提取一个令牌值，该标头是从您的 APM 中传递的。您可以修改此代码，使其符合贵组织的安全策略和 APM 要求。
4. 在模板中找到 `TransformLambdaFunction`。将字典路径 `raw_json["detail"]["ProblemTitle"]` 替换为指向警报名称的路径（警报名称在 APM 的 JSON 有效载荷中发送）。对于 Dynatrace，将其保持原样。

部署 CloudFormation 模板：

1. 在目标账户和 AWS 区域中打开 CloudFormation 控制台。
2. 依次选择创建堆栈、使用新资源（标准）。
   - 选择选择现有模板、上传模板文件、选择文件，然后上传您本地保存的 CloudFormation 模板。
3. 指定堆栈详细信息：
   - 输入堆栈名称（示例：*`DynatraceIntegrationForIDR`*。）
   - APMNameParameter（示例：*`Dynatrace`*。）
   - 选择下一步。
4. 配置堆栈选项：

- 滚动到页面底部，然后选中支持 CloudFormation 使用自定义名称创建 IAM 资源的框。

5. 审核和创建：
   - 验证参数值是否正确配置，然后选择“提交”。
6. CloudFormation 堆栈会部署必要的资源，来将您的 APM 事件集成到 AWS 事件检测及响应服务。等待直到 CloudFormation 堆栈状态变为 CREATE_COMPLETE。
7. 假设示例值 `Dynatrace` 输入到参数中并在 US-EAST-1 区域中执行，CloudFormation 堆栈会创建以下资源。
   - 密钥名称：DynatraceMySecretTokenName（将针对密钥 APMSecureToken 创建随机密钥值）
   - API Gateway 资源:
     - API 名称：Dynatrace-AWSIncidentDetectionResponse-APIGW
     - 阶段名称：Dynatrace-Stage-Prod
     - 授权方：Dynatrace-APIGW-Authorizer
     - 使用计划：APIGW_Throttling_Plan
   - Lambda 函数：
     - 用于授权的函数：Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - 用于转换的函数：Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - 自定义事件总线名称：Dynatrace-AWSIncidentDetectionResponse-EventBus
   - IAM 角色：
     - TransformLambdaExecutionRole：IDR-TransformLambdaExecutionRole-us-east-1
     - AuthorizerLambdaExecutionRole：IDR-AuthorizerLambdaExecutionRole-us-east-1
8. 记录 Webhook URL 和令牌值：
   - 打开 API Gateway 控制台，然后选择作为 CloudFormation 堆栈一部分创建的 API 名称。
   - 从左侧导航栏中选择“阶段”，使用 + 号展开阶段名称，然后选择 POST。记录调用 URL。将 APM 中的此 URL 配置为发送警报事件的 Webhook 的目标。
   - 打开 AWS Secrets Manager 控制台并选择作为 CloudFormation 堆栈一部分创建的密钥名称。（示例：DynatraceMySecretTokenName。）
     - 在“密钥值”选项卡中，选择检索密钥值。您将看到“密钥”为 APMSecureToken。记录密钥值。请勿与任何人分享此密钥值。

集成测试

部署堆栈后，通过从 APM 发送测试有效载荷来测试集成：

1. 导航到 Lambda 控制台并选择 APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform 函数。选择监控选项卡。
2. 在指标图表中寻找成功的调用。
3. 选择查看 Amazon CloudWatch Logs，以检查日志流中是否有您的测试有效载荷或是否存在任何错误。

与 AWS 事件检测及响应服务共享您的事件总线 ARN

1. 打开 Amazon EventBridge 控制台。选择事件总线。
2. 复制作为 CloudFormation 堆栈一部分创建的自定义事件总线的 ARN，示例：*arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus*。
   - 将此 ARN 添加到警报摄取问卷 - 概述的“第三方 APM 警报”部分中的“EventBridge 事件总线 ARN”字段。
3. 在接入过程中，AWS 事件检测及响应服务将在此自定义事件总线上创建托管式 EventBridge 规则，以摄取您的 APM 警报。

选项 2：手动集成

使用以下步骤设置与 AWS 事件检测及响应服务的集成。

1. 创建 Amazon API Gateway 以接受来自 APM 的有效载荷。
2. 定义 Lambda 函数，以便使用身份验证令牌进行授权。
3. 执行下列操作之一：
   - （建议）创建名为 $YourApmName-AWSIncidentDetectionResponse-EventBus 的 EventBridge 自定义事件总线。
   - （替代）使用默认的 EventBridge 事件总线，而非自定义事件总线。
4. 定义转换 Lambda 函数来将 AWS 事件检测及响应服务标识符附加到您的有效载荷。您还可以使用此函数筛选要发送到 AWS 事件检测及响应服务的事件。
   - API Gateway 必须调用转换 Lambda 函数，该函数将转换由 API Gateway 传递的有效载荷。
   - 转换 Lambda 函数必须在上面第 3 点定义的事件总线中写入转换后的事件。
5. 将您的 APM 设置为向 API Gateway 生成的 URL 发送通知。

从与 Amazon SNS 直接集成的 APM 摄取警报

如果您的 APM 支持向 Amazon SNS 主题发送警报，则您可以按照本指南将您的 APM 警报摄取到 AWS 事件检测及响应服务。

您可以部署所提供的 CloudFormation 模板或手动设置此集成。在设置集成之前，请确认在您的账户中创建了 AWS 服务相关角色（SLR）`AWSServiceRoleForHealth_EventProcessor`。

选项 1：使用 CloudFormation

可以使用 CloudFormation 模板来简化创建集成基础设施的过程，该基础设施是从与 Amazon SNS 集成的 APM 中将警报摄取到 AWS 事件检测及响应服务所必需的。

> **Note**
>
> - 通过此 CloudFormation 模板部署的资源（例如：Lambda 和 EventBridge）将产生额外费用。有关这些服务的定价的更多信息，请参阅 AWS 定价。
> - 此 CloudFormation 模板必须部署在 AWS 事件检测及响应服务需要从中摄取警报的每个 AWS 账户和区域中。
> - 本文档中提供的示例适用于 Grafana，但是此模板可用于与 Amazon Simple Notification Service 直接集成的任何 APM。
> - 出于安全考虑，AWS 建议从 `TransformLambdaFunction` 中移除 `logger.info()` 语句，以防止将有效载荷记录在 Amazon CloudWatch Logs 中。

部署此 CloudFormation 模板的先决条件：

- 必须创建标准 Amazon Simple Notification Service 主题，才能接收来自 APM 的警报事件。在 Amazon Simple Notification Service 控制台中创建 SNS 主题。
- 必须根据所使用的 APM 来修改模板中的 `TransformLambdaFunction`，以便将 `["detail"]["incident-detection-response-identifier"]` 设置为所需的值。

完成先决条件：

1. 打开 Amazon SNS 控制台，然后选择“主题”。复制为接收来自 APM 的警报事件而创建的标准 Amazon SNS 主题的 ARN。
   - 示例：`arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`

2. 下载并打开 CloudFormation 模板
   - 在模板中找到 `TransformLambdaFunction`
     - 在 `def lambda_handler(event, context)` 下，将 `event["detail"]["incident-detection-response-identifier"]` 设置为 json 路径，在该路径中，警报名称出现在 SNS 记录的 json 有效载荷中。
       - 通过 SNS 发送到 `TransformLambdaFunction` 的任何事件都有一个父有效载荷结构，即 `event["Records"][n]["Sns"]["Message"]`。来自源的实际有效载荷来源（APM）封装在父结构内。
       - Grafana 的示例：`event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

部署 CloudFormation 模板：

1. 在您需要在其中设置集成的账户和区域中导航到 CloudFormation 控制台。
2. 导航到 CloudFormation。
   - 依次选择“创建堆栈”、“使用新资源（标准）”
     - 选择“选择现有模板”、“上传模板文件”、“选择文件”，然后上传您本地保存的 CloudFormation 模板。
3. 指定堆栈详细信息：
   - 输入堆栈名称（示例：`<your-apm-name>IntegrationForIDR`）
   - 指定在完成先决条件期间获得的参数值
     - APMNameParameter（示例：`Grafana`）
     - TriggerSNSParameter（示例：`arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`）
   - 选择下一步。
4. 配置堆栈选项：
   - 滚动到页面底部，然后确认支持 CloudFormation 使用自定义名称创建 IAM 资源的复选框。
5. 审核和创建：
   - 验证参数值是否正确配置，然后选择“提交”。
6. CloudFormation 堆栈将部署必要的资源，来将您的 APM 事件集成到 AWS 事件检测及响应服务。等待直到 CloudFormation 堆栈状态变为 CREATE_COMPLETE。
7. 假设示例值已输入到 Grafana 的参数中并在 EU-WEST-1 区域中执行，CloudFormation 堆栈会创建以下资源。

- CustomEventBus：Grafana-AWSIncidentDetectionResponse-EventBus
- SNSSubscription：arn:aws:sns:eu-west-1:012345678912:grafana-sns:[random_string]
- TransformLambdaExecutionRole：IDR-TransformLambdaExecutionRole-eu-west-1
- TransformLambdaFunction：Grafana-AWSIncidentDetectionResponse-Lambda-Transform
- TransformLambdaPermission：GrafanaIntegrationForIDR-TransformLambdaPermission-[random_string]

集成测试

成功部署 CloudFormation 堆栈后，您可以通过从 APM 发送测试有效载荷来验证集成。从 APM 发送测试有效载荷后：

1. 导航到 Lambda 控制台并选择 `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 函数。然后，选择“监控”选项卡。
2. 应在指标图表中观察到成功的调用。
3. 选择“查看 Amazon CloudWatch Logs”。您可以从日志流中的日志事件进行验证，以确认从 APM 发送的测试有效载荷是否存在，或者是否遇到了任何错误。

与 AWS 事件检测及响应服务共享您的事件总线 ARN

1. 导航到 Amazon EventBridge 控制台。选择“事件总线”。
2. 记录作为 CloudFormation 堆栈一部分部署的自定义事件总线的 ARN，例如：`arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`。
   - 在警报摄取问卷 - 概述的“第三方 APM 警报”部分的“EventBridge 事件总线 ARN”字段中，将此自定义事件总线的 ARN 提供给 AWS 事件检测及响应服务。
3. 在接入过程中，AWS 事件检测及响应服务将在此自定义事件总线上创建托管式 EventBridge 规则，以摄取您的 APM 警报。

选项 2：手动集成

1. 打开 Amazon SNS 控制台并创建一个标准 Amazon SNS 主题（名为 `[apm_name]-sns`），以接收来自 APM 的警报事件。确保选择标准（而不是 FIFO）作为主题类型。记下所创建的 Amazon SNS 主题的 ARN。

2. 执行下列操作之一：
   - （建议）创建名为 [apm_name]-AWSIncidentDetectionResponse-EventBus 的 EventBridge 自定义事件总线。
   - （替代）使用默认的 EventBridge 事件总线，而非自定义事件总线。

   AWS 事件检测及响应服务将通过 AWSServiceRoleForHealth_EventProcessor SLR，在自定义或默认事件总线上安装托管式规则 (AWSHealthEventProcessorEventSource-DO-NOT-DELETE)。规则源将是自定义或默认事件总线，规则目标将是 AWS 事件检测及响应服务，而规则将与用于摄取第三方 APM 事件的模式相匹配。
3. 创建名为 $YourApmName-AWSIncidentDetectionResponse-LambdaFunction 的 Lambda 函数以转换您的 SNS 有效载荷。
   - 转换后的事件必须满足在使用 EventBridge 摄取 APM 警报的有效载荷要求中规定的有效载荷要求
   - 将 Lambda 函数的目标设置为在步骤 2 中创建的自定义事件总线（建议）或设置为您的默认事件总线。
4. 将 SNS 主题设置为 Lambda 函数 $YourApmName-AWSIncidentDetectionResponse-LambdaFunction 的触发器。
   - 在“添加触发器”页面中，搜索“SNS”。
   - 添加在步骤 1 中创建的专用 SNS 主题的 ARN。
   - 选择“添加”。
5. 按照您的 APM 文档，为需要由 AWS 事件检测及响应服务摄取的 APM 有效载荷设置 SNS 目标。

AWS 事件检测及响应服务将通过 AWSServiceRoleForHealth_EventProcessor SLR，在自定义或默认事件总线上安装托管式规则 (AWSHealthEventProcessorEventSource-DO-NOT-DELETE)。规则源将是自定义或默认事件总线，规则目标将是 AWS 事件检测及响应服务，而规则将与用于摄取第三方 APM 事件的模式相匹配。

警报优化和监控调整

为了确保最佳的事件检测准确性，我们的事件管理工程师会根据您的关键工作负载持续评估警报性能。我们提供建议的警报配置更改（您需要进行这些更改），并主动与您和您的技术客户经理（TAM）协作以完善这些设置。

当监控数据表明警报可能与您的业务关键型操作不一致时，例如警报触发但并没有对客户造成相应影响，或者警报状态频繁波动，我们建议取消非关键警报，并接入能更准确反映关键工作负载影响的警报。这有助于保持事件响应覆盖范围的整体有效性。

警报审核和反馈

AWS 事件检测及响应服务在接入警报以进行监控之前，会对警报进行全面审核。将根据技术验收标准评估警报，包括配置参数、数据质量和警报有效性。

根据此审核，可提供两种类型的反馈：

- 强制性配置要求：必须实施这些更改才能验收警报。
- 可选的改进建议：这些更改可增强警报的有效性，但不是验收警报的必备条件。

收到此反馈后，您可以决定只处理接入已验收的警报和需要可选改进的警报，同时并行处理具有强制性配置要求的警报的配置更改。

或者，您可以在上线之前实施所有更改。这种方法根据需要调整的警报数量延长了接入时间表。

警报上线

警报摄取完成后，AWS 事件检测及响应服务将对工作负载启用监控。从此刻开始，已加入的警报将受到主动监控，当已加入的警报进入警报状态时，AWS 事件检测及响应服务将根据工作负载的运行手册与您联系。

主要输出

- AWS 事件检测及响应服务确认您的工作负载已上线且受到监控。

后续步骤：

- 要验证加入的警报是否按预期联系 AWS 事件检测及响应服务，请参阅测试已加入事件检测及响应服务的工作负载。
- 要更改已加入的警报、运行手册或工作负载信息，请参阅请求更改已加入事件检测及响应服务的工作负载。

事件检测及响应服务中的工作负载接入问卷和警报摄取问卷（异常路径）

> **Note**
>
> 如果您无法使用 IDR CLI 来加入工作负载，请使用以下问卷来处理工作负载和警报加入。

本主题提供了在将工作负载加入 AWS 事件检测及响应服务以及配置要摄取到该服务的警报时需要填写的问卷。工作负载加入问卷涵盖有关您工作负载、其架构详细信息以及事件响应联系人的一般信息。在警报摄取问卷中，您需要为您的工作负载指定会触发在事件检测及响应服务中创建事件的关键警报，并指定运行手册信息，说明要联系哪些人以及要采取哪些措施。正确填写这些问卷是为您的 AWS 工作负载设置监控和事件响应流程的关键步骤。

下载工作负载接入问卷：

- 英文版
- 日文版

下载警报摄取问卷：

- 英文版
- 日文版

工作负载加入问卷 - 一般问题

一般问题

问题	响应示例
企业名称	Amazon Inc.
此工作负载的名称（含任何缩写）	Amazon Retail Operations（ARO）
此工作负载的主要最终用户和功能。	此工作负载是一个电子商务应用程序，最终用户可通过它购买各种物品。此工作负载是我们业务的主要收入来源。

工作负载加入问卷 - 架构问题

架构问题

问题	响应示例
AWS 资源标签列表，用于定义属于此工作负载的资源。AWS 将使用这些标签来标识此工作负载的资源，以便在事件发生期间迅速为您提供支持。 **Note** 标签区分大小写。如果您提供多个标签，则此工作负载使用的所有资源都必须具有相同的标签。	应用程序名称：Optimax 环境：生产
此工作负载使用的 AWS 服务的列表，以及它们所在的 AWS 账户和 AWS 区域。	AWS 服务：Route 53、ALB、ECS、... 账户：123456789101、123456789102、... 区域：US-EAST-1、US-WEST-2、...

警报摄取问卷 - 概述

在警报摄取问卷中，您需要为您的工作负载指定要参与 AWS 事件检测及响应服务的关键警报，以及您希望事件管理工程师在这些警报触发时进行联系的联系人。

警报摄取问卷分为以下几个部分：

- 联系人部分：首先，请指定警报触发时，要包含在 AWS 事件检测及响应服务所创建的 支持 案例中的主要联系人，以及您首选的事件沟通会议应用程序。如果未提供沟通会议首选项，AWS 事件检测及响应服务将在事件期间创建事件沟通会议。接下来，指定上报联系人以及在无法联系到主要联系人时与他们联系的时间间隔。最后，列出在事件期间应通过支持案例接收定期事件状态更新的任何联系人。
- 警报矩阵：列出一组警报，这些警报在触发时将联系 AWS 事件检测及响应服务。在选择警报以便接入时，请参阅 AWS 事件检测及响应服务定义的“关键警报标准”。有关更多信息，请参阅 警报定义。
  - Amazon CloudWatch 警报（如果您没有 Amazon CloudWatch 警报，请将此部分留空）

- 第三方 APM 警报（如果您没有第三方 APM 警报，请将此部分留空）
  - EventBridge 事件总线 ARN：这是您在从与 EventBridge 直接集成的 APM 摄取警报或从未与 EventBridge 直接集成的 APM 摄取警报中创建的自定义事件总线 ARN 的 ARN。
  - 警报标识符：共享 APM 警报的账号、区域和名称。

警报摄取问卷 - 运行手册问题

运行手册问题

问题	响应示例
AWS 通过 支持 案例与工作负载联系人联系。当针对此工作负载触发警报时，谁是主要联系人？ 指定您的首选会议应用程序，AWS 将在事件发生期间要求提供这些详细信息。 **Note** 如果未提供首选的会议应用程序，则 AWS 会在事件发生期间与您联系，并提供 Chime 桥供您加入。	应用程序团队 app@example.com +61 2 3456 7890
如果事件发生期间联系不到主要联系人，请按首选的通信顺序提供上报联系人和时间表。	1. 10 分钟后，如果主要联系人没有回复，请联系： John Smith - 应用程序主管 john.smith@example.com +61 2 3456 7890 2. 10 分钟后，如果 John Smith 没有回复，请联系： Jane Smith - 运维经理 jane.smith@example.com

问题	响应示例
	+61 2 3456 7890

警报矩阵

提供以下信息以确定一组警报，这些警报将触发 AWS 事件检测及响应服务代表您的工作负载创建事件。AWS 事件检测及响应服务的工程师查看您的警报后，将提供额外的加入步骤。

AWS 事件检测及响应服务关键警报标准：

- AWS 事件检测及响应服务警报应仅在受监控的工作负载遭受重大业务影响（收入损失/客户体验降级）且需要运维人员立即给予关注时才会进入“警报”状态。
- AWS 事件检测及响应服务警报还必须在联系的同时或联系之前与您工作负载的事件解决人员联系。AWS事件经理将会在风险缓解流程中与您的事件解决人员协作，而非充当第一响应者然后再上报给您。
- AWS 事件检测及响应服务警报阈值必须设置为适当的阈值和持续时间，以便每当警报触发时，都会介入调查。如果警报介于“警报”和“正常”状态之间，会产生足够的影响以确保得到运维人员的响应和关注。

AWS 事件检测及响应服务标准违规策略：

只有当发生事件时，才能根据具体案例评估这些标准。事件管理团队会与您的技术客户经理（TAM）协作来调整警报，并且在极少数情况下，如果怀疑客户警报不符合此标准，且不必要地定期与事件管理团队联系，则会禁用监控。

> **Important**
>
> 在提供联系人地址时提供群组分发电子邮件地址，这样您就可以控制收件人的添加和删除而无需更新运行手册。
> 如果您希望 AWS 事件检测及响应服务团队在发送初始互动电子邮件后给您的站点可靠性工程（SRE）团队打电话，请提供他们的联系电话。

CloudWatch 警报的警报矩阵表

CloudWatch 警报 ARN	此警报的主要联系人。 （如果与工作负载主要联系人不同）	指定该警报最相关的 AWS 服务，以联系合适的工程师。如果不需要，请输入 N/A。
示例： `arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response`	示例： Sam Smith - 应用程序管理员 sam.smith@example.com +61 2 3456 7890	示例： ECS

第三方 APM 警报的警报矩阵表

EventBridge 事件总线 ARN
 	
（这是作为第三方 APM 集成的一部分创建的，用于将警报发送到 AWS 事件检测及响应服务。）
		示例：（每个账户/区域组合将有一个事件总线）
		
		`arn:aws:events:us-east-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`
		
		`arn:aws:events:us-west-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`	

警报标识符	这个指标表示什么？ 为什么此警报很重要？	此警报的主要联系人。 （如果与工作负载主要联系人不同）	指定该警报最相关的 AWS 服务，以联系合适的工程师。如果不需要，请输入 N/A。
示例： ALB_5xx_Target_Response	示例： 该指标表示来自 ALB 背后的目标的事务响	示例： Sam Smith - 应用程序管理员	示例： ECS

账户 ID：123456789012 区域：us-east-1	应。如果 5XX 错误数超过阈值，则表示发生严重故障，而无法处理业务事务。	sam.smith@example.com +61 2 3456 7890	

管理事件检测及响应服务中的工作负载

有效的事件管理的一个关键部分就是建立适当的流程和程序，来加入、测试和维护监控的工作负载。本节介绍了基本步骤，包括创建全面的运行手册和响应计划来指导您的团队应对事件，对新的工作负载进行全面的测试和验证，请求更改以更新工作负载监控，以及根据需要适当地移除工作负载等。

主题

- 创建运行手册和响应计划来应对事件检测及响应服务中的事件
- 测试已加入事件检测及响应服务的工作负载
- 请求更改已加入事件检测及响应服务的工作负载
- 抑制警报触发事件检测及响应服务
- 从事件检测及响应服务中移除工作负载

创建运行手册和响应计划来应对事件检测及响应服务中的事件

AWS 事件检测及响应服务会依据您在 IDR CLI 加入过程中捕获的信息来创建运行手册，以便管理对工作负载造成影响的事件。运行手册记录了事件经理在应对事件时采取的步骤。响应计划会至少映射到您的一个工作负载。事件管理团队会根据您在工作负载接入期间提供的信息创建这些模板。

主要输出：

- 完成您工作负载在 AWS 事件检测及响应服务中的定义。
- 完成 AWS 事件检测及响应服务中的警报和运行手册。

您也可以下载 AWS 事件检测及响应服务运行手册示例：aws-idr-runbook-example.zip。

示例运行手册

Example示例运行手册

说明

本文档适用于 [CustomerName] - [WorkloadName]。

步骤：优先级

Priority 操作

1. 向买家发送有关 支持 案例的第一封信函，如下所示。

```
Hello,

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

Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
```

步骤：信息

互动计划

本节介绍适用于本运行手册的互动计划，仅包含联系详细信息。互动计划将在分步沟通计划中进行引用。

- 初始互动

  AWS 事件检测及响应服务团队向 支持 案例中添加了以下客户利益相关者地址。AWS 利益相关者是指可能需要让他们意识到任何问题的其它利益相关者。

  - 客户利益相关者：customeremail1；customeremail2；mobile1
  - AWS 利益相关者：aws-idr-oncall@amazon.com；tam-team-email；等等
  - 仅限一次性联系人：这些是仅包含在第一次沟通中的电子邮件联系人。在第一次沟通结束后，移除这些联系人。这些可能是客户的寻呼电子邮件地址，例如 Pager-duty，不得对每封信函进行寻呼。在“优先级”部分的“沟通计划”中明确添加说明，说明仅当仅限一次性联系人可用时如何使用这些信息。
- 事件呼叫设置

  指明客户是否需要 AWS 事件检测及响应服务来创建桥，客户是否使用静态桥，或者客户是否会在事件发生时提供桥。

  （根据客户偏好选择一个选项）

  - AWS 事件检测及响应服务创建 Amazon Chime/Zoom 桥
  - 客户提供的静态桥
    - 会议号码：<插入会议号码>

- 客户通过回复 AWS 事件检测及响应服务团队发出的沟通内容，为每个事件提供桥详情。
- 其它 - 指定详细信息。

- 互动升级

  当初始互动计划中的联系人未对事件做出回应时，AWS 事件检测及响应服务将联系以下联系人。

  对于每位升级联系人，请指明是必须将他们添加到 支持 案例、致电，或者同时采用这两种方式。

  - 在升级之前，请确保您已致电初始互动联系人（如果适用）。
  - 第一个升级联系人：[escalationEmailAddress#1]/[PhoneNumber] - 等待 XX 分钟后再升级到该联系人。
    - [将联系人添加到案例/电话] 此联系人。
  - 第二个升级联系人：[escalationEmailAddress#2]/[PhoneNumber] - 等待 XX 分钟后再升级到该联系人。
    - [将联系人添加到案例/电话] 此联系人。
  - 等等

沟通计划

本节介绍事件管理工程师如何与除事件呼叫和沟通渠道之外的指定利益相关者进行沟通。

- 影响沟通计划

  当 AWS 事件检测及响应服务从分类步骤中确定警报会对客户造成潜在影响时，该计划即启动。

  AWS 事件检测及响应服务将要求客户加入预先确定的桥，如互动计划 - 事件呼叫设置中所述。

  （根据仅限一次性联系人是否可用，选择一个。）

  1. 确保互动计划 - 初始互动中的客户利益相关者已添加到案例 CC 中。

  或

  1. 确保互动计划 - 初始互动中的客户利益相关者和仅限一次性联系人已添加到案例 CC 中。
  2. 根据以下模板向客户发送互动通知：

     （请选择一个）

     影响模板 - Amazon Chime 桥

```
The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
    Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
Please join the Amazon Chime Bridge below so we can start the steps outlined in
 your Runbook:
    Amazon Chime Meeting ID: <insert_Meeting_ID_here>
    Link to Amazon Chime Bridge: <insert_Link_here>
    International dial-in numbers: https://chime.aws/dialinnumbers/
```

影响模板 - 客户提供的桥

```
The following alarm has engaged AWS Incident Detection and Response:
    Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025 3:30 PM UTC>
Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
```

影响模板 - 客户静态桥

```
The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
    Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
Please join the Bridge below so we can start the steps outlined in your Runbook:
    Conference Number: <insert_conference_number>
    Conference URL: <insert_bridge_URL>
```

3. 将案例设置为“待处理的客户操作”。
4. 发送上述影响沟通后，从案例中移除仅限一次性联系人。（如果仅限一次性联系人可用。）
5. 按照上面提到的互动升级计划进行操作。
6. 如果客户未在 30 分钟内做出回应，请断开互动并继续监控，直到警报恢复。

- 无影响沟通计划

  当警报在事件检测及响应服务完成初始分类之前恢复时，启动此计划。

1. 在发送无影响通知之前，请根据互动计划 - 初始互动互动计划中列出的联系人，从 支持 案例 CC 中移除和/或添加客户联系人。

   [“请勿添加仅限一次性联系人。”]（如果仅限一次性联系人可用，则适用。）

2. 根据以下模板向客户发送不互动通知：

   无影响模板

   ```
   AWS Incident Detection and Response received an alarm that has recovered for your
    workload.
       Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
       Alarm State Change Reason - <insert_state_change_reason>
       Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
       Alarm End Time - <Example: 1 January 2025, 3:35 PM UTC>
   This may indicate a brief customer impact that is currently not ongoing.
   If there is an ongoing impact to your workload, please let us know and we will
    engage to assist.
   ```

3. 将案例置于待处理的客户操作。
4. 如果客户未在 30 分钟内回应，请解决案例。

应用程序架构概述

本节概述了事件管理工程师和运营工程师意识的应用程序/工作负载架构。

- 提供关键服务的 AWS 账户和区域：支持此应用程序的 AWS 账户及区域的列表。协助工程师评测支持应用程序的底层基础设施。
  - 123456789012
    - US-EAST-1：酌情简要描述
      - Amazon EC2：酌情简要描述
      - DynamoDB：酌情简要描述
      - 等等
    - US-WEST-1：酌情简要描述
      - 等等
  - 另一个账户
    - 等等

测试已加入事件检测及响应服务的工作负载

警报摄取完成后，AWS 事件检测及响应服务将对工作负载启用监控，并发送上线确认。从现在起，您的工作负载将受到积极监控。

警报测试验证已加入的警报是否按预期与 AWS 事件检测及响应服务互动，触发相应的运行手册以及任何其它所需的操作，例如，如果您在警报摄取期间选择了自动创建案例。

测试是可选的，但强烈建议使用它。您有责任在实际事件发生之前验证您的响应安排。

测试选项

AWS 事件检测及响应服务提供了两种测试选项。

选项 1：预定的游戏日演练（推荐）

预定的游戏日演练是对真实事件中可能发生的情况进行的实况端到端模拟。AWS 事件检测及响应服务会按照您规定的运行手册步骤，让您深入了解真实事件会如何发展。游戏日演练可为您提供机会来提出问题或完善说明，进而改进互动效果。

要预定游戏日演练，请完成以下步骤：

1. 使用首选日期和 1 小时的时段（包括时区）通知 AWS 事件检测及响应服务。提供至少 48 小时的提前期。
2. 为游戏日演练计划资源，包括您的 SRE/运营团队和升级联系人。

游戏日演练安排：

1. 您和 AWS 事件检测及响应服务加入呼叫。
2. 如果适用，您可以禁用警报操作。
3. 您可以按照如何测试警报中的说明，手动将警报设置为警报状态。
4. AWS 事件检测及响应服务确认收到警报通知。
5. AWS 事件检测及响应服务对警报做出响应，并加入运行手册中规定的桥。
6. 您和 AWS 事件检测及响应服务确认游戏日演练结果。

选项 2：离线警报测试

您可以随时独立地测试警报，而无需安排呼叫。触发警报会根据您的运行手册与 AWS 事件检测及响应服务互动，就像在真实事件期间一样。

要执行离线警报测试，请完成以下步骤：

1. 为防止意外操作，请禁用任何 Amazon CloudWatch 警报操作。
2. 按照如何测试警报中的说明触发警报。
3. 在 5 分钟内，将代表您创建支持案例，AWS 事件检测及响应服务将按照运行手册中的规定与您互动。
4. 告知 Incident Manager 您正在进行离线警报测试。
5. Incident Manager 确认收到了哪些警报状态变更并验证响应安排。

如果未在 5 分钟内创建支持案例，请提交事件请求，以便手动与 AWS 事件检测及响应服务互动来排查故障。

如何测试警报

Amazon CloudWatch 警报

> **Note**
>
> 您用于警报测试的 AWS Identity and Access Management 用户或角色必须具有 `cloudwatch:SetAlarmState` 权限。

使用 AWS Command Line Interface或 AWS CloudShell 手动将警报设置为警报状态。这些命令可在不影响工作负载的情况下更改警报状态。

为防止意外的操作（例如 Amazon EC2 实例重启），请在更改警报状态之前禁用任何 CloudWatch 警报操作。测试完成后，您可以重新启用 CloudWatch 警报操作。要了解有关禁用或启用警报操作的更多信息，请参阅《Amazon CloudWatch API 参考》中的 DisableAlarmActions 和 EnableAlarmActions。

禁用警报操作。

```
aws cloudwatch disable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

将警报状态设置为“警报”：

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

测试后重新启用警报操作：

```
aws cloudwatch enable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

警报状态将在几秒钟内自动恢复为正常。

复合警报

`set-alarm-state` 命令不能保证复合警报恢复为正常状态。作为最佳实践，请在测试后验证复合警报的状态。要手动重置复合警报，请使用以下命令：

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

要详细了解有关手动更改 CloudWatch 警报的状态，请参阅《Amazon CloudWatch API 参考》中的 SetAlarmState。

要了解有关 CloudWatch API 操作所需权限的更多信息，请参阅 Amazon CloudWatch 权限参考。

第三方 APM 警报

使用第三方应用程序性能监控（APM）工具（例如 Datadog、Splunk、New Relic 或 Dynatrace）的工作负载需要不同的说明来模拟警报。

1. 在 APM 中禁用警报操作以防止意外操作。
2. 修改您的警报阈值或比较运算符，以强制警报进入警报状态。这会触发 AWS 事件检测及响应服务的有效载荷。
3. 测试完成后，回滚阈值或比较运算符更改，以便将警报还原为正常状态。

关键成果

成功测试后：

- 警报摄取得以确认，并且警报配置正确无误。
- AWS 事件检测及响应服务手收到警报。

- 系统创建支持案例，并通知您指定的联系人。
- AWS 事件检测及响应服务会通过您规定的会议方式与您互动。
- 在测试期间产生的所有警报和支持案例均得以解决。

常见问题

是否必须进行警报测试？

否。测试是可选的，但强烈建议您在真实事件发生前验证您的端到端响应安排。

我的工作负载会受到影响吗？

不会。但是，在测试期间，在警报上配置的任何警报操作都会触发，除非您将其禁用。在测试之前禁用警报操作，以防止意外影响。

在测试期间会通知谁？

在预定的游戏日演练期间，我们会联系您运行手册中的所有联系人和升级路径来进行验证。在离线警报测试期间，仅通知在警报加入期间指定的初始联系人。

我能否通过电子邮件回复案例更新？

否。支持 案例信函的电子邮件副本是从一个不回复的地址发送的。要更新案例，请使用 AWS Support Center Console。

如何在上线后请求游戏日演练？

回复您现有的加入支持案例（如果存在），或者创建请求更改已加入事件检测及响应服务的工作负载。

请求更改已加入事件检测及响应服务的工作负载

要请求更改已加入的工作负载，请完成以下步骤，通过 AWS 事件检测及响应服务创建支持案例。

1. 转到AWS 支持 中心，然后选择创建案例，如以下示例所示：

2. 选择技术。
3. 对于服务，选择事件检测和响应。
4. 对于类别，选择工作负载更改请求。
5. 对于严重性，选择一般指导。

6. 为此更改输入主题。例如：

   AWS 事件检测及响应服务 - *workload_name*

7. 为此更改输入描述。例如，输入“此请求是为了更改已加入 AWS 事件检测及响应服务的现有工作负载”。请确保在请求中包含以下信息：

   - 工作负载名称：您的工作负载名称。
   - 账户 ID：ID1、ID2、ID3 等。
   - 更改详细信息：输入关于您请求的更改的详细信息。

8. 在其他联系人 - 可选部分中，输入您希望接收有关此更改的通信信息的所有电子邮件 ID。

   以下是其他联系人 - 可选部分的示例。

   > **Important**
   >
   > 未能在其他联系人 - 可选部分中添加电子邮件 ID 可能会延误更改流程。

9. 选择提交。

   提交更改请求后，您可以添加组织中的其它电子邮件。要添加电子邮件，请在案例详细信息中选择回复，如以下示例中所示：

   然后，在其他联系人 - 可选部分中添加电子邮件 ID。

   以下是回复页面的示例，您可以在其中输入其它电子邮件。

抑制警报触发事件检测及响应服务

通过暂时或按计划抑制已加入的工作负载的警报，指定哪些警报可以触发 AWS 事件检测及响应服务的监控。例如，在计划维护期间，您可以暂时抑制工作负载警报，以防警报触发事件检测及响应服务。或者，如果您每天都有重启活动，则可以按计划抑制警报。您可以在警报源（例如 Amazon CloudWatch）抑制警报，也可以提交工作负载更改请求。

主题

- 在警报源抑制警报

- 提交工作负载更改请求来抑制警报
- 教程：使用指标数学函数抑制警报
- 教程：移除指标数学函数来抑制警报

在警报源抑制警报

通过在警报源抑制警报，指定哪些警报可触发事件检测及响应服务以及何时触发。

主题

- 使用指标数学函数抑制 CloudWatch 警报
- 移除指标数学函数以取消抑制 CloudWatch 警报
- 指标数学函数示例及相关的使用案例
- 抑制来自第三方 APM 的警报

使用指标数学函数抑制 CloudWatch 警报

要抑制事件检测及响应服务监控 Amazon CloudWatch 警报，请使用指标数学函数来阻止 CloudWatch 警报在指定时段内进入 ALARM 状态。

> **Note**
>
> 对 CloudWatch 警报禁用警报操作不会抑制事件检测及响应服务监控警报。警报状态的变化是通过 Amazon EventBridge 摄取的，而非通过 CloudWatch 警报操作摄取。

要使用指标数学函数来抑制 CloudWatch 警报，请完成以下步骤：

1. 登录 AWS 管理控制台并打开 CloudWatch 控制台（https://console.aws.amazon.com/cloudwatch/）。
2. 选择警报，然后找到要向其添加指标数学函数的警报。
3. 选择操作，然后单击编辑以更改警报。
4. 选择编辑指标以修改警报的指标。
5. 选择添加数学、从空表达式开始。
6. 输入您的数学表达式，然后选择应用。
7. 取消选择警报监控的现有指标。

8. 选择您刚刚创建的表达式，然后选择选择指标。
9. 选择跳到查看并创建。
10. 查看您的更改，确保您的指标数学函数已按预期应用，然后选择更新警报。

有关使用指标数学函数抑制 CloudWatch 警报的分步示例，请参阅教程：使用指标数学函数抑制警报。

有关语法和可用函数的更多信息，请参阅《Amazon CloudWatch 用户指南》中的指标数学语法和函数。

移除指标数学函数以取消抑制 CloudWatch 警报

通过移除指标数学函数来取消抑制 CloudWatch 警报。要从警报中移除指标数学函数，请完成以下步骤：

1. 登录AWS 管理控制台并打开 CloudWatch 控制台 (https://console.aws.amazon.com/cloudwatch/)。
2. 选择警报，然后找到要从中移除指标数学表达式的一个或多个警报。
3. 在指标数学部分中，选择编辑。
4. 要从警报中移除该指标，请在指标上选择编辑，然后选择指标数学表达式旁边的 x 按钮。
5. 选择原始指标，然后选择选择指标。
6. 选择跳到查看并创建。
7. 查看您的更改，确保您的指标数学函数已按预期应用，然后选择更新警报。

指标数学函数示例及相关的使用案例

下表给出了一些指标数学函数示例，相关的使用案例以及对每个指标组成部分的解释。

指标数学函数	使用案例	说明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	通过将世界标准时间每周二凌晨 1:00 至凌晨 3:00 期间的实际数据点替换为 0，抑制该时段内的警报。	• DAY(m1) == 2：确保是星期二（星期一 = 1，星期日 = 7）。 • HOUR(m1) >= 1 && HOUR(m1) > 3：指定从世界标准时间凌晨 1 点到凌晨 3 点的时间范围。

指标数学函数	使用案例	说明
		• IF(condition, value_if_true, value_if_false)如果条件为 true，则将该指标值替换为 0。否则，返回原始值 (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	通过将世界标准时间每天午夜 11:00 至次日凌晨 4:00 期间的实际数据点替换为 0，抑制该时段内的警报。	• HOUR(m1) >= 23：捕获从世界标准时间 23:00 开始的时间。 • HOUR(m1) < 4：捕获截至（但不包括）世界标准时间凌晨 04:00 的时间。 • ||：逻辑运算符 OR 确保条件应用于两个范围：深夜和凌晨。 • IF(condition, value_if_true, value_if_false)：在指定时间范围内返回 0。该范围之外则保留原始指标值 m1。
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	通过将世界标准时间每天上午 11:00 至下午 1:00 期间的实际数据点替换为 0，抑制该时段内的警报。	• HOUR(m1) >= 11 && HOUR(m1) < 13：捕捉世界标准时间 11:00 到 13:00 之间的时间范围。 • IF(condition, value_if_true, value_if_false)：如果条件为 true（例如，时间介于世界标准时间 11:00 到 13:00 之间），则返回 0，如果条件为 false，则保留原始指标值 (m1)。

指标数学函数	使用案例	说明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	通过将世界标准时间每周二凌晨 1:00 至凌晨 3:00 期间的实际数据点替换为 99，抑制该时段内的警报。	• DAY(m1) == 2：确保是星期二（星期一 = 1，星期日 = 7）。 • HOUR(m1) >= 1 && HOUR(m1) < 3：指定从世界标准时间凌晨 1 点到凌晨 3 点的时间范围。 • IF(condition, value_if_true, value_if_false)如果条件为 true，则将该指标值替换为 99。否则，返回原始值 (m1)。
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	通过将世界标准时间每天午夜 11:00 至次日凌晨 4:00 期间的实际数据点替换为 100，抑制该时段内的警报。	• HOUR(m1) >= 23：捕获从世界标准时间 23:00 开始的时间。 • HOUR(m1) < 4：捕获截至（但不包括）世界标准时间凌晨 04:00 的时间。 • ||：逻辑运算符 OR 确保条件应用于两个范围：深夜和凌晨。 • IF(condition, value_if_true, value_if_false)：在指定时间范围内返回 100。该范围之外则保留原始指标值 m1。

指标数学函数	使用案例	说明
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	通过将世界标准时间每天上午 11:00 至下午 1:00 期间的实际数据点替换为 99，抑制该时段内的警报。	• HOUR(m1) >= 11 && HOUR(m1) < 13：捕捉世界标准时间 11:00 到 13:00 之间的时间范围。 • IF(condition, value_if_true, value_if_false)：如果条件为 true（例如，时间介于世界标准时间 11:00 到 13:00 之间），则返回 99。如果条件为 false，则保留原始指标值 (m1)。

抑制来自第三方 APM 的警报

有关如何抑制警报的说明，请参阅您的第三方 APM 供应商的文档。第三方 APM 供应商的例子有 New Relic、Splunk、Dynatrace、Datadog 和 SumoLogic。

提交工作负载更改请求来抑制警报

如果您无法按照上一节所述在警报源抑制警报，那么请提交工作负载更改请求，指示事件检测及响应服务手动抑制对工作负载部分或全部警报的监控。

有关如何创建工作负载更改请求的详细说明，请参阅请求更改已加入事件检测及响应服务的工作负载。在提出工作负载更改请求以请求抑制警报时，请务必提供以下必要信息

- 工作负载名称：您的工作负载名称。
- 账户 ID：ID1、ID2、ID3 等。
- 更改详细信息：警报抑制
- 抑制开始时间：日期、时间和时区。
- 抑制结束时间：日期、时间和时区。
- 要抑制的警报：要抑制的 CloudWatch 警报 ARN 或第三方 APM 事件标识符的列表。

创建警报抑制工作负载更改请求后，您将收到来自事件检测及响应服务的以下通知：

- 工作负载更改请求确认。
- 警报被抑制时发送的通知。
- 重新启用警报以进行监控时发送的通知。

教程：使用指标数学函数抑制警报

以下教程将引导您完成如何使用指标数学来抑制 CloudWatch 警报的过程。

示例方案

即将到来的星期二凌晨 1:00 到凌晨 3:00 之间（世界标准时间）有计划的活动。您想要创建一个 CloudWatch 指标数学函数来将这段时间内的实际数据点替换为 0（低于设定阈值的数据点）。

1. 评估导致警报触发的标准。以下屏幕截图提供了警报标准示例：

   上面的屏幕截图中显示的警报将会监控应用程序负载均衡器目标组的 UnHealthyHostCount 指标。当 5/5 个数据点的 UnHealthyHostCount 指标大于或等于 3 时，此警报便会进入 ALARM 状态。该警报将缺失数据视为不良数据（超出配置的阈值）。
2. 创建指标数学函数。

   在此示例中，即将到来的星期二凌晨 1:00 到凌晨 3:00 之间（世界标准时间）有计划的活动。因此，需要创建一个 CloudWatch 指标数学函数来将这段时间内的实际数据点替换为 0（低于设定阈值的数据点）。

   请注意，您要配置的替换数据点因警报配置而异。例如，如果您有一个用于监控 HTTP 成功率的警报，其阈值小于 98，则将计划活动期间的实际数据点替换为高于配置阈值 100 的值。以下是该情景的指标数学函数示例。

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

   上面的指标数学函数包含以下元素：

   - DAY(m1) == 2：确保是星期二（星期一 = 1，星期日 = 7）。
   - HOUR(m1) >= 1 && HOUR(m1) < 3：指定从世界标准时间凌晨 1 点到凌晨 3 点的时间范围。
   - IF(condition, value_if_true, value_if_false)如果条件为 true，则该函数将指标值替换为 0。否则，将返回原始值 (m1)。

有关语法和可用函数的更多信息，请参阅《Amazon CloudWatch 用户指南》中的指标数学语法和函数。

3. 登录 AWS 管理控制台并打开 CloudWatch 控制台（https://console.aws.amazon.com/cloudwatch/）。
4. 选择警报，然后找到要向其添加指标数学函数的警报。
5. 在指标数学部分中，选择编辑。
6. 选择添加数学、从空表达式开始。
7. 输入您的数学表达式，然后选择应用。

   警报监控的现有指标自动变为 m1，您的数学表达式为 e1，如以下示例所示：

8. （可选）编辑指标数学表达式的标签，以便他人可以了解它是一个函数及其创建的原因，如以下示例所示：

9. 取消选择 m1，选择 e1，然后选择选择指标。这会将警报设置为监控数学表达式，而非直接监控底层指标。
10. 选择跳到查看并创建。
11. 验证是否按预期配置警报，然后选择更新警报以保存更改。

在上面的示例中，若未应用指标数学函数，则实际 `UnHealthyHostCount` 指标将在计划活动期间报告。这将导致 CloudWatch 警报进入 `ALARM` 状态并触发事件检测及响应服务，如以下示例所示：

创建指标数学函数后，活动期间实际数据点会被替换为 0，警报保持 `OK` 状态，从而抑制触发事件检测及响应服务。

教程：移除指标数学函数来抑制警报

如果您针对单次活动抑制了 CloudWatch 警报，那么在活动结束后从警报中移除指标数学函数，就能恢复对警报的定期监控。要定期抑制警报，例如，如果您计划的每周例行修补导致实例每周在同一天和同一时间重启，那么请保留指标数学函数。

以下教程将引导您完成如何移除指标数学来取消抑制 CloudWatch 警报的过程

1. 登录 AWS 管理控制台并打开 CloudWatch 控制台（https://console.aws.amazon.com/cloudwatch/）。
2. 选择警报，然后找到要向其添加指标数学函数的警报。
3. 在指标数学部分中，选择编辑。
4. 要从警报中移除抑制，请选择指标数学表达式旁边的 x 按钮。
5. 选择要恢复实际指标监控的指标。然后选择选择指标。
6. 选择跳到查看并创建。
7. 验证是否按预期配置警报，然后选择更新警报以保存更改。

从事件检测及响应服务中移除工作负载

要从 AWS 事件检测及响应服务中移除工作负载，请为每个工作负载创建一个新的支持案例。在创建支持案例时，请记住以下几点：

- 要移除单个 AWS 账户中的工作负载，请从该工作负载的账户或付款人账户创建支持案例。
- 要移除跨多个 AWS 账户的工作负载，请从您的付款人账户创建支持案例。在支持案例的正文中，列出要移除工作负载的所有账户 ID。

> **Important**
>
> 如果您从不正确的账户创建移除工作负载的支持案例，则在工作负载被移除之前，您可能会遇到延误且可能会要求您提供更多信息。

请求移除工作负载

1. 进入 AWS 支持 中心，然后选择创建案例。
2. 选择技术。
3. 对于服务，选择事件检测和响应。
4. 对于类别，选择工作负载移除。
5. 对于严重性，选择一般指导。
6. 为此更改输入主题。例如：

[移除] AWS 事件检测及响应服务 - *workload_name*

7. 为此更改输入描述。例如，输入“此请求是为了移除已加入 AWS 事件检测及响应服务的现有工作负载”。请确保在请求中包含以下信息：

   - 工作负载名称：您的工作负载名称。
   - 账户 ID：ID1、ID2、ID3 等。
   - 移除原因：提供移除工作负载的原因。

8. 在其他联系人 - 可选部分中，输入您希望接收有关此移除请求的通信信息的所有电子邮件 ID。
9. 选择提交。

AWS 事件检测及响应服务的监控和可观测性

AWS 事件检测及响应服务可为您提供专家级指导，协助您定义从应用程序层到底层基础设施的所有工作负载的可观测性。监控能够让您知晓工作负载存在问题。可观测性利用数据收集来告诉您问题出在哪里以及问题发生的原因。

事件检测及响应系统通过利用 Amazon CloudWatch 和 Amazon EventBridge 等原生 AWS 服务来检测可能影响您工作负载的事件，从而监控您的 AWS 工作负载是否面临故障和性能下降的问题。监控将针对即将出现的、正在进行的、即将消退的或潜在的故障或性能下降向您提供通知。将账户加入事件检测及响应服务时，您可以选择账户中的哪些警报应由事件检测及响应监控系统进行监控，并将这些警报与事件管理期间使用的应用程序和运行手册相关联。

事件检测及响应服务使用 Amazon CloudWatch 和其它 AWS 服务工具来为您构建可观测性解决方案。AWS 事件检测及响应服务通过两种方式协助您实施可观测性：

- 业务结果指标：AWS 事件检测及响应服务的可观测性首先要定义用于监控工作负载结果或最终用户体验的关键指标。AWS 专家将与您协作，了解您的工作负载目标、可能影响用户体验的主要输出或因素，并定义用于捕捉这些关键指标中的任何降级情况的指标和警报。例如，移动呼叫应用程序的关键业务指标是呼叫建立成功率（监控用户呼叫尝试的成功率），而网站的关键指标是页面速度。事件参与是基于业务结果指标触发的。
- 基础设施级别指标：在此阶段，我们会确定支持您的应用程序的底层 AWS 服务和基础设施，并定义指标和警报来跟踪这些基础设施服务的性能。其中可能包括诸如应用程序负载均衡器实例的 `ApplicationLoadBalancerErrorCount` 之类的指标。该指标将在加入工作负载并设置监控后开始运行。

基于 AWS 事件检测及响应服务实施可观测性

由于可观测性是一个持续的过程，可能无法在一次演练或单个时间范围内完成，因此 AWS 事件检测及响应服务分两个阶段实施可观测性：

- 加入阶段：加入期间的可观测性侧重于检测应用程序的业务结果何时受到损害。为此，加入阶段的可观测性侧重于定义应用程序层的关键业务结果指标，以将您的工作负载中断情况通知给 AWS。这样，AWS 就能迅速应对这些中断，并协助您进行恢复。要了解有关使用 AWS 事件检测及响应服务命令行界面来协助自动执行这些步骤的更多信息，请参阅 AWS 事件检测及响应服务的 CLI。
- 加入后阶段：AWS 事件检测及响应服务针对可观测性提供了诸多主动服务，包括基础设施级别指标的定义、指标调整以及根据客户的成熟度设置跟踪和日志等。这些服务的实施可能需要几个月，涉及

多个团队。AWS 事件检测及响应服务提供有关可观测性设置的指导，客户需要在其工作负载环境中实施所需的更改。如需亲自实施可观测性功能的协助，请向您的技术客户经理（TAM）提出请求。

通过事件检测及响应服务进行事件管理

AWS 事件检测及响应服务通过指定的事件经理团队为您提供每周 7 天、每天 24 小时的主动监控和事件管理。下图概述了应用程序警报触发事件后的标准事件管理流程，包括警报生成、AWS 事件经理参与、事件解决以及事后审查。

1. 警报生成：您工作负载上触发的警报将通过 Amazon EventBridge 推送给 AWS 事件检测及响应服务。AWS 事件检测及响应服务会自动调出与您的警报相关的运行手册并通知事件经理。如果您的工作负载上发生了严重事件，但 AWS 事件检测及响应服务监控的警报未检测到，则您可以创建支持案例来发送事件响应请求。有关发送事件响应请求的更多信息，请参阅创建事件响应请求。
2. AWS 事件经理参与：事件经理会对警报做出回应，并与您进行电话会议或按照运行手册中规定的其它方式与您取得联系。事件经理会验证 AWS 服务的运行状况，以确定警报是否是关于工作负载所使用的 AWS 服务的问题，并就底层服务的状态提供建议。如果需要，事件经理会代表您创建案例，并联系相应的 AWS 专家来提供支持。由于 AWS 事件检测及响应服务专门针对您的应用程序监控 AWS 服务，因此 AWS 事件检测及响应服务可能会在宣布 AWS 服务事件之前确定事件与 AWS 服务问题有关。在这种情况下，事件经理会就 AWS 服务的状态向您提供建议，触发 AWS 服务事件管理工作流程，并跟进服务团队的事件解决情况。所提供的信息让您有机会尽早实施恢复计划或解决办法，以减轻 AWS 服务事件的影响。

   有时警报会触发并迅速恢复。在这种情况下，事件经理会发送一封案例信函，说明警报已恢复，但不会与您接洽。但是，如果警报在 15 分钟内多次触发，则即使警报恢复，事件经理也会按照运行手册的说明与您接洽。
3. 事件解决：事件经理会在所需的 AWS 团队之间协调事件，并确保您与合适的 AWS 专家保持联系，直到事件得到缓解或解决。
4. 事后审查（根据请求）：事件发生后，AWS 事件检测及响应服务会根据您的请求进行事后审查，并生成事后报告。事后报告包括问题描述、事件造成的影响、参与的团队以及为缓解或解决事件而采取的解决办法或措施。事故后报告可能包含如何降低事件再次发生的可能性或如果未来再发生类似事件如何改进管理的信息。事故后报告不是根本原因分析（RCA）。除了事后报告外，您还可以请求 RCA。下面提供了事后报告的示例。

> **Important**
>
> 以下报告模板仅供参考。

Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS ## case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-impaired-useast1-P95

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

Incident Summary:

Summary of the incident in chronological order and steps taken by AWS Incident Managers to direct the incident to a path to mitigation.
At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical incident for the workload. AWS Incident Detection and Response Managers responded to the alarm, checking AWS service health and steps outlined in the workload’s runbook.
At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the Incident Management team sent the engagement email to the customer’s Site Reliability Team (SRE) team, created a troubleshooting bridge, and an ## support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and ## Engineering joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to services the workload depends on. The investigation shifted to the specific resources in the customer account.
At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase in traffic volume was causing a drop in connections. The customer confirmed this ALB was newly provisioned to handle an increase in workload traffic for an on-going promotional event.
At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The Incident Manager worked with the Cloud Support Engineer to raise an escalation a higher support level to quickly scale the ALB per the runbook.

```
 At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The
back-off/retry logic yields mild recovery but timeouts are still being seen for some
clients.
By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to
pre-incident levels. Connection timeouts subside.
 At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes
of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

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

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

主题

- 为应用程序团队预置 AWS Support Center Console的访问权限
- 创建事件响应请求
- 使用 AWS Support App in Slack管理事件检测及响应服务支持案例

为应用程序团队预置 AWS Support Center Console的访问权限

AWS 事件检测及响应服务会在事件发生期间通过 支持 案例与您进行沟通。要与事件经理进行通信，您的团队必须有权访问 支持 中心。

有关预置访问权限的更多信息，请参阅《支持 用户指南》中的管理对 支持 中心的访问权限。

创建事件响应请求

如果您的工作负载上发生了严重事件，但 AWS 事件检测及响应服务监控的警报未检测到，您可以创建支持案例来发送事件响应请求。对于订阅了 AWS 事件检测及响应服务的任何工作负载（包括正在执行加入流程的工作负载），您都可以使用 AWS Support Center Console、AWS 支持 API 或 AWS Support App in Slack来创建事件响应请求。

下图演示了 AWS 客户请求事件检测及响应服务团队协助解决事件的端到端工作流程，详细说明了从最初发送请求一直到调查、缓解并解决的步骤。

要针对切实影响您工作负载的事件创建事件响应请求，请创建 支持 案例。在提出支持案例后，AWS 事件检测及响应服务会让您与相应的 AWS 专家进行会谈，以便加速恢复工作负载。

使用 AWS Support Center Console创建事件响应请求

要创建事件响应请求，请完成以下步骤：

1. 打开 AWS Support Center Console以创建新的支持案例。
2. 对于主题，输入事件的简短摘要。例如 `AWS Incident Detection and Response - Active Incident - workload_name`。
3. 对于描述，输入事件的详细信息。我们建议您在支持案例中包括以下详细信息：
   - 受影响的 AWS 资源 ARN、工作负载名称及其功能
   - 业务影响描述
   - （可选）您的首选会议桥 URL。如果您未提供桥详细信息，AWS 事件检测及响应服务会创建一个 AWS 会议桥，并向您发送包含桥 URL 的邀请。
4. （可选）附加有助于描述事件的文件，例如屏幕截图或日志摘录。
5. 配置以下案例分类字段：
   - 案例类型：技术
   - 服务：事件检测及响应服务
   - 类别：活动的事件
   - 严重性：业务关键系统停机
6. 提供更多背景信息来协助 AWS 事件检测及响应服务更快地联系 AWS 专家，例如受影响的 AWS 服务、受影响的 AWS 区域、业务影响、影响开始时间和受影响的资源。
7. 选择提交。
8. AWS 事件检测及响应服务会在五分钟内确认您的案例，并会为您提供会议桥，让您与相应的 AWS 专家接触。

使用 AWS 支持 API 创建事件响应请求

您可以使用 AWS 支持 API 以编程方式创建支持案例。有关更多信息，请参阅《AWS 支持 用户指南》中的关于 AWS 支持 API。

使用 AWS Support App in Slack创建事件响应请求

要使用 AWS Support App in Slack创建事件响应请求，请完成以下步骤：

1. 打开您在其中配置 AWS Support App in Slack的 Slack 频道。
2. 输入以下命令：

```
/awssupport create
```

3. 输入此事件的主题。例如，输入 AWS 事件检测及响应服务 - 活动事件 - workload_name。
4. 输入此事件的问题描述。添加以下详细信息：

   技术信息：

   受影响的服务：

   受影响的资源：

   受影响的区域：

   工作负载名称：

   业务信息：

   业务影响描述：

   [可选] 客户桥详细信息：
5. 选择下一步。

6. 对于问题类型，选择技术支持。
7. 对于服务，选择事件检测和响应。
8. 对于类别，选择活动事件。
9. 对于严重性，选择关键业务系统停机。

10.（可选）在要通知的其他联系人字段中输入最多 10 个其他联系人，以逗号分隔。这些其他联系人将会收到有关此事件的电子邮件通信信息的副本。

11选择审核。

12Slack 频道中会出现一条只有您才能看到的新消息。查看案例详细信息，然后选择创建案例。

13您的案例 ID 会在来自 AWS Support App in Slack的新消息中提供。

14事件检测及响应服务会在 5 分钟内确认您的案例，并会为您提供会议桥，让您与相应的 AWS 专家接触。

15案例话题中会更新来自事件检测及响应服务的通信信息。

使用 AWS Support App in Slack管理事件检测及响应服务支持案例

借助 AWS Support App in Slack，您可以在 Slack 中管理您的 支持 案例，接收有关您 AWS 事件检测及响应服务工作负载的新警报发起事件的通知，以及创建事件响应请求。

要配置 AWS Support App in Slack，请按照 支持 用户指南中提供的说明进行操作。

> **Important**
>
> - 要在 Slack 中接收有关您工作负载的所有警报发起事件的通知，您必须为所有已加入 AWS 事件检测及响应服务的工作负载账户配置 AWS Support App in Slack。支持案例是在出现工作负载警报的账户中创建的。
> - 事件发生期间，会代表您创建多个高严重性支持案例来通知 支持 事件解决人员。关于在事件期间创建的所有支持案例，您都会在 Slack 中收到符合您 Slack 频道通知配置的通知。
> - 您通过 AWS Support App in Slack收到的通知并不会取代事件发生期间 AWS 事件检测及响应服务通过电子邮件或电话联系的工作负载初始联系人和上报联系人。

主题

- Slack 中的警报发起事件通知
- 在 Slack 中创建事件响应请求

Slack 中的警报发起事件通知

在 Slack 频道中配置 AWS Support App in Slack后，针对您由 AWS 事件检测及响应服务监控的工作负载，将会收到有关警报发起的事件的通知。

以下示例演示了关于警报发起事件的通知在 Slack 中的显示方式。

示例通知：

当 AWS 事件检测及响应服务确认您的警报发起事件后，Slack 中便会生成类似于以下内容的通知：

要查看 AWS 事件检测及响应服务添加的完整通信信息，请选择查看详细信息。

AWS 事件检测及响应服务的更多更新将显示在该案例的话题中。

选择查看详细信息，可查看 AWS 事件检测及响应服务添加的完整通信信息。

在 Slack 中创建事件响应请求

有关如何通过 AWS Support App in Slack创建事件响应请求的说明，请参阅创建事件响应请求。

事件检测及响应服务中的报告

AWS 事件检测及响应服务提供了运维和性能数据，有助于您了解服务的配置方式、事件历史记录以及事件检测及响应服务的性能。本页介绍了可用的数据类型，包括配置数据、事件数据和性能数据等。

配置数据

- 所有加入的账户
- 所有应用程序的名称
- 与每个应用程序关联的警报、运行手册和支持配置文件

事件数据

- 每个应用程序的事件的日期、数量和持续时间
- 与特定警报关联的事件的日期、数量和持续时间
- 事件后报告

性能数据

- 服务级别目标（SLO）性能

请联系您的技术客户经理，来获取您可能需要的运维和性能数据。

事件检测及响应服务安全性与韧性

AWS 责任共担模式会应用于 支持 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础结构。您负责维护对托管在此基础架构上的内容的控制。此内容包括您所使用的 AWS 服务 的安全配置和管理任务。

有关数据隐私的更多信息，请参阅数据隐私常见问题。

有关欧洲数据保护的信息，请参阅 AWS 安全性博客上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护AWS账户凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予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）。
- 使用安全套接字层/传输层安全性（SSL/TLS）证书与 AWS 资源通信。建议使用 TLS 1.2 或更高版本。如欲了解相关信息，请参阅什么是 SSL/TLS 证书？。
- 使用 AWS CloudTrail 设置 API 和用户活动日记账记录。有关信息，请参阅。AWS CloudTrail
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 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 中的个人数据。有关 Amazon Macie 的信息，请参阅 Amazon Macie。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的信息，请参阅 Federal Information Processing Standard (FIPS) 140-2。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理 支持 或其它 AWS 服务时。您在用于名称的标签或自由格式字段中输入的任何数据都可能会用于计费或诊断日志。当您向外部服务器提供 URL 时，强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

AWS 事件检测及响应服务对您账户的访问权限

AWS Identity and Access Management (IAM) 是一种 Web 服务，可以帮助您安全地控制对 AWS 资源的访问。可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（具有相应权限）来使用资源。

AWS 事件检测及响应服务和您的警报数据

默认情况下，事件检测及响应服务会收到您账户中每个 CloudWatch 警报的 Amazon 资源名称（ARN）和状态，然后在您加入的警报变为“警报”状态时启动事件检测及响应流程。如果您想自定义事件检测及响应服务从您账户接收有关警报的哪些信息，请联系您的技术客户经理。

文档历史记录

下表介绍了自本 IDR 指南上一次发布以来对文档所做的重要改动。

更改	描述	日期
澄清了 APM 集成的标准 Amazon SNS 主题	澄清了在将第三方 APM 警报与 AWS 事件检测及响应服务集成时，客户应创建标准的 Amazon Simple Notification Service 主题（而不是 FIFO）。 有关更多信息，请参阅 从与 Amazon SNS 直接集成的 APM 摄取警报。	2026 年 5 月 26 日
游戏日演练现在是可选的，简化了加入问卷，并更新了运行手册开发	更新了警报测试（游戏日演练），使其在上线后变为可选的，并具有两个测试选项：预定的游戏日演练或离线警报测试。简化了工作负载加入和警报摄取问卷。更新了运行手册制作以移除对 AWS Systems Manager 文档的引用。 有关更多信息，请参阅 测试已加入事件检测及响应服务的工作负载、事件检测及响应服务中的工作负载接入问卷和警报摄取问卷（异常路径）和 创建运行手册和响应计划来应对事件检测及响应服务中的事件。	2026 年 5 月 26 日
更新了“创建事件响应请求”过程	更新了“创建事件响应请求”过程以匹配当前的 AWS Support Center Console 用户界面，添加了桥 URL 指南，并移除了过时的屏幕截图。 有关更多信息，请参阅 使用 AWS Support Center Console创建事件响应请求。	2026 年 5 月 12 日
更新了接入过程以采用 CLI 优先的方法	更新了“入门”一章，以便将 AWS 事件检测及响应服务客户命令行界面提升为主要的接入方法，并弃用了工作负载接入问卷和警报摄取问卷作为默认的接入路径。对于无法使用 IDR CLI 的客户，问卷仍可作为例外选项提供。	2026 年 5 月 12 日

更改	描述	日期
	有关更多信息，请参阅将工作负载加入到事件检测及响应服务和警报摄取。	
添加了日语问卷链接	为工作负载接入问卷和警报摄取问卷添加了日语下载链接。 有关更多信息，请参阅 事件检测及响应服务中的工作负载接入问卷和警报摄取问卷（异常路径）。	2026 年 4 月 20 日
更新了架构引用	移除了对架构图的引用，代之以架构详细信息。 有关更多信息，请参阅事件检测及响应服务的架构和关于事件检测及响应服务中的工作负载。	March 31, 2026
更新了“测试已加入事件检测及响应服务的工作负载”	添加了有关在测试期间更改警报状态之前禁用 CloudWatch 警报操作的信息。 有关更多信息，请参阅 测试已加入事件检测及响应服务的工作负载。	2026 年 3 月 2 日
更新了“通过事件检测及响应服务进行事件管理”	添加了有关重复警报行为和事件经理接洽的信息。 有关更多信息，请参阅 通过事件检测及响应服务进行事件管理。	2026 年 3 月 2 日
“使用指标数学函数抑制 CloudWatch 警报”部分中更新的步骤	“使用指标数学函数抑制 CloudWatch 警报”部分中更新的步骤。 有关更多信息，请参阅 在警报源抑制警报。	2026 年 2 月 3 日
添加了韩语作为支持的语言	添加了韩语作为支持的语言。 有关更多信息，请参阅 事件检测及响应服务的区域可用性。	2026 年 1 月 22 日

更改	描述	日期
添加了普通话作为支持的语言	添加了普通话作为支持的语言。 有关更多信息，请参阅 事件检测及响应服务的区域可用性。	2026 年 1 月 13 日
添加了新的部分：AWS 事件检测及响应服务客户命令行界面	添加了 IDR CLI 部分，并更新了入门一章，以包含有关 AWS 事件检测及响应服务客户命令行界面的信息。 有关更多信息，请参阅 AWS 事件检测及响应服务的 CLI。	2025 年 12 月 8 日
更新了多个部分：事件检测及响应服务中的工作负载加入和警报摄取问卷以及事件检测及响应服务入门	AWS 服务事件处理流程不再是 AWS 事件检测及响应服务的一部分。本用户指南的相关章节已更新，删除了对此流程的引用。您将继续通过 AWS 服务运行状况控制面板接收服务事件通知。AWS 事件检测及响应服务的客户可以根据需要使用事件响应请求在服务事件期间获得帮助。有关更多信息，请参阅 创建事件响应请求。	2025 年 10 月 14 日
删除了以下部分：服务事件的事件管理	AWS 服务事件处理流程不再是 AWS 事件检测及响应服务的一部分。为了反映此更改，用户指南已经删除了这一部分。您将继续通过 AWS 服务运行状况控制面板接收服务事件通知。AWS 事件检测及响应服务的客户可以根据需要使用事件响应请求在服务事件期间获得帮助。有关更多信息，请参阅 创建事件响应请求。	2025 年 10 月 14 日
更新了以下部分：事件检测及响应服务的区域可用性	AWS 事件检测及响应服务现已在 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）推出。有关更多信息，请参阅 事件检测及响应服务的区域可用性。	2025 年 10 月 5 日

更改	描述	日期
更新了以下部分：事件检测及响应服务中的工作负载加入和警报摄取问卷	更新了警报矩阵表的示例电子邮件地址。	2025 年 8 月 26 日
更新了以下部分：为工作负载订阅 AWS 事件检测及响应服务	在创建案例窗口的描述部分中删除了对订阅开始日期字段的引用。 更新了以下部分：为工作负载订阅 AWS 事件检测及响应服务	2025 年 8 月 4 日
新功能：抑制警报触发事件检测及响应服务	在托管工作负载中新增了几个部分，提供了有关如何暂时或按计划抑制警报的信息 新增的部分：抑制警报触发事件检测及响应服务	2025 年 4 月 9 日
更新了使用 AWS Support Center Console创建事件响应请求的说明	添加了有关在问题描述字段中输入哪些信息的详细信息。 更新了以下部分：创建事件响应请求	2025 年 2 月 6 日
添加了更多 AWS 区域	已在事件检测及响应服务的可用性部分添加了更多 AWS 区域。 更新了以下部分：事件检测及响应服务的区域可用性	2024 年 11 月 1 日
更新了使用 AWS Support App in Slack管理事件检测及响应服务支持案例页面	将页面移至事件管理下，修改了文本，并更换了屏幕截图。 更新了以下部分：使用 AWS Support App in Slack管理事件检测及响应服务支持案例	2024 年 10 月 10 日
添加了一个关于 AWS Support App in Slack的新页面 更新了“通过 AWS 事件检测及响应服务进行事件管理”	添加了一个关于 AWS Support App in Slack的新页面 更新了“通过 AWS 事件检测及响应服务进行事件管理”，新增了“使用 AWS Support App in Slack 创建事件响应请求”这一部分。	2024 年 9 月 10 日

更改	描述	日期
更新了账户订阅	更新了账户订阅部分，增加了关于申请订阅账户时如何创建支持案例的详细说明。 更新了以下部分：为工作负载订阅 AWS 事件检测及响应服务	2024 年 6 月 12 日
新增了以下部分：移除工作负载	在入门中增加了移除工作负载这一部分，纳入了关于移除工作负载的信息 有关更多信息，请参阅 从事件检测及响应服务中移除工作负载。	2024 年 3 月 28 日
更新了账户订阅	更新了账户订阅部分，增加了有关移除工作负载的信息 有关更多信息，请参阅“为工作负载订阅 AWS 事件检测及响应服务”	2024 年 3 月 28 日
更新了“测试”部分	更新了测试部分，增加了有关加入流程的最后一步“游戏日演练测试”的信息。 更新了以下部分：测试已加入事件检测及响应服务的工作负载	2024 年 2 月 29 日
更新了“什么是 AWS 事件检测及响应服务”部分	更新了什么是 AWS 事件检测及响应服务部分。 更新了以下部分：什么是 AWS 事件检测及响应服务？	2024 年 2 月 19 日
更新了“问卷”部分	更新了“工作负载加入问卷”部分，增加了“警报摄取问卷”。将该部分从加入问卷更名为工作负载加入和警报摄取问卷。	2024 年 2 月 2 日

更改	描述	日期
更新了 AWS Service Event 和加入信息	更新了几个部分，其中增加了有关加入的新信息。 更新了以下部分： • 将工作负载加入到事件检测及响应服务 • 为工作负载订阅 AWS 事件检测及响应服务 新增的部分 • 为应用程序团队预置 AWS Support Center Console的访问权限	2024 年 1 月 31 日
增加了“相关信息”部分	在预置访问权限中增加了相关信息部分。 更新了以下部分：预调配将警报摄取到事件检测及响应服务所需的访问权限	2024 年 1 月 17 日
更新了示例步骤	更新了示例：集成来自 Datadog 和 Splunk 的通知中步骤 2、3 和 4 的程序。 更新了部分：“示例：集成来自 Datadog 和 Splunk 的通知”	2023 年 12 月 21 日
更新了介绍图片和文字	更新了从与 Amazon EventBridge 直接集成的 APM 摄取警报中的图片。 更新了以下部分：创建运行手册和响应计划来应对事件检测及响应服务中的事件	2023 年 12 月 21 日
更新了运行手册模板	更新了创建 AWS 事件检测及响应服务运行手册中的运行手册模板。 更新了以下部分：创建运行手册和响应计划来应对事件检测及响应服务中的事件	2023 年 12 月 4 日

更改	描述	日期
更新了警报配置	更新了警报配置，新增了有关 CloudWatch 警报配置的详细信息。 新增的部分：在事件检测及响应服务中创建符合您业务需求的 CloudWatch 警报 新增的部分：使用 CloudFormation 模板在事件检测及响应服务中构建 CloudWatch 警报 新增的部分：事件检测及响应服务中的 CloudWatch 警报使用案例示例	2023 年 9 月 28 日
更新了“入门”部分	更新了“入门”部分，新增了有关工作负载更改请求的信息。 新增的部分：请求更改已加入事件检测及响应服务的工作负载 更新了以下部分：为工作负载订阅 AWS 事件检测及响应服务	2023 年 9 月 5 日
“入门”中新增一个部分	增加了，提供了有关如何将警报摄取到 AWS 事件检测及响应服务的信息。	2023 年 6 月 30 日
原始文档	首次发布的《AWS 事件检测及响应服务》	2023 年 3 月 15 日