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 February 3, 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？

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（IME）将全天候对您加入该服务的工作负载进行监控，全面检测严重事件。IME 会在警报触发后的 5 分钟内做出响应，或者对您向事件检测及响应服务团队提出的关键业务支持案例做出响应。
- 加快事件解决速度：IME 使用专为您的工作负载创建的预定义和自定义运行手册，在 5 分钟内做出响应，代表您创建 Support 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

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 文档中托管有关您工作负载的信息，包括工作负载架构图、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
填写加入问卷	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
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

活动	Customer	Incident Detection and Response
测试 CloudWatch 警报	负责	问责
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

AWS 区域	名称
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
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

AWS 区域	名称
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，快速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。

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。

要了解如何开始加入工作负载，请参阅工作负载加入和工作负载加入问卷。

警报

警报是事件检测及响应服务的关键部分，因为它们可以让您了解应用程序和底层 AWS 基础设施的性能。AWS 将与您协作，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，来快速为您解决所有问题。应将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。

要了解如何摄取警报，请参阅警报摄取和警报摄取问卷。

> **Note**
>
> 要更改您的运行手册、工作负载信息或 AWS 事件检测及响应服务中监控的警报，请参阅请求更改已加入事件检测及响应服务的工作负载。

加入事件检测及响应服务

AWS 与您协作，来将您的工作负载和警报加入到 AWS 事件检测及响应服务。您可以使用事件检测及响应服务客户命令行界面（CLI）工具或在事件检测及响应服务中的工作负载加入和警报摄取问卷中，向 AWS 提供有关工作负载和您要加载的警报的关键信息。

下图显示了事件检测及响应服务中的工作负载加入和警报摄取流程：

工作负载加入

在加入工作负载期间，AWS 将与您协作，了解您的工作负载以及在事件发生期间如何为您提供支持。您需要提供有关工作负载的关键信息，以便我们协助您减轻业务影响。

主要输出：

- 一般工作负载信息
- 包括图表在内的架构详情
- 运行手册信息
- 客户发起的事件

警报摄取

AWS 将与您协作，协助您加入警报。AWS 事件检测及响应服务可以通过 Amazon EventBridge 接收来自 Amazon CloudWatch 和第三方应用程序性能监控（APM）工具的警报。加入警报可实现主动事件检测及自动事件参与。有关更多信息，请参阅从与 Amazon EventBridge 直接集成的 APM 摄取警报。

主要输出：

- 警报矩阵

下表列出了将工作负载加入到 AWS 事件检测及响应服务所需的步骤。下表显示的是每项任务的持续时间示例。每项任务的实际日期需要根据团队的空闲时间和日程表来确定。

事件检测及响应服务中的工作负载加入和警报摄取问卷

本页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，说明应联系哪些人以及应采取哪些措施。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。

下载工作负载加入问卷。

下载警报摄取问卷。

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。
此工作负载适用的合规性和/或监管要求，以及事件发生后需要 AWS 采取的任何措施。	该工作负载主要处理需要确保安全性和机密性的患者医疗记录。

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。	应用程序名称：Optimax 环境：生产

问题	响应示例
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。	
此工作负载使用的 AWS 服务的列表，以及运行这些服务的 AWS 账户和区域。 Note 每项服务要新建一行。	Route 53：将互联网流量路由到 ALB。 账户：123456789101 区域：US-EAST-1、US-EAST-2
此工作负载使用的 AWS 服务的列表，以及运行这些服务的 AWS 账户和区域。 Note 每项服务要新建一行。	ALB：将传入流量路由到一组目标 ECS 容器。 账户：123456789101 区域：不适用
此工作负载使用的 AWS 服务的列表，以及运行这些服务的 AWS 账户和区域。 Note 每项服务要新建一行。	ECS：主业务逻辑队列的计算基础设施。负责处理传入的用户请求并向持久层进行查询。 账户：123456789101 区域：US-EAST-1
此工作负载使用的 AWS 服务的列表，以及运行这些服务的 AWS 账户和区域。 Note 每项服务要新建一行。	RDS：Amazon Aurora 集群存储由 ECS 业务逻辑层访问的用户数据。 账户：123456789101 区域：US-EAST-1

问题	响应示例
此工作负载使用的 AWS 服务的列表，以及运行这些服务的 AWS 账户和区域。 **Note** 每项服务要新建一行。	S3：存储网站静态资产。 账户：123456789101 区域：不适用
详细说明未加入但出现中断时可能会对此工作负载造成影响的任何上游/下游组件。	身份验证微服务：将阻止用户在未经身份验证的情况下加载医疗记录。
是否有适用于此工作负载的本地或非 AWS 组件？ 如果有，那么是什么组件？执行哪些功能？	所有进出 AWS 的互联网流量均通过我们的本地代理服务进行路由。
在可用区和区域级别提供任何手动或自动失效转移/灾难恢复计划的详细信息。	暖备用。成功率持续下降期间自动失效转移到 US-WEST-2。

警报摄取问卷

运行手册问题

问题	响应示例
AWS 将通过 支持 案例与工作负载联系人接洽。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

问题	响应示例
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 +61 2 3456 7890
在整个事件期间，AWS 会定期通过支持案例传达更新内容。是否还需要向其他联系人传达这些更新内容？	john.smith@example.com，jane.smith@example.com

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政策：

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。

警报矩阵表

指标名称/ARN/阈值	说明	备注	请求的操作
工作负载数量/ *CW Alarm ARN*/ 5 分钟内 5 个数据点的 CallCount < 100000，将缺失数据处理为缺失	该指标表示进入工作负载的传入请求数，在应用程序负载均衡器级别进行衡量。 此警报很重要，因为传入请求大量减少可能表明上游网络连接存在问题，或者我们的 DNS 实现存在问题，导致用户无法访问工作负载。	该警报在上周进入“警报”状态 10 次。此警报存在误报的风险。已计划进行阈值审核。 存在问题？ “否”或“是”（如果为“否”，则留空）：在执行特定的批处理作业期间，此警报频繁翻转。 解决人员：站点可靠性工程师	发送电子邮件至 *SRE@example.com* ，联系站点可靠性工程团队 为我们的 ELB 和 Amazon Route 53 服务创建 AWS 支持 案例。 如果需要立即采取措施：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知##团队重启实例，或者刷新日志。（如果不需要立即采取措施，请留空）

指标名称/ARN/阈值	说明	备注	请求的操作
工作负载请求延迟/ *CW Alarm ARN*/ 5 分钟内 5 个数据点的 p90 延迟 > 100 毫秒，将缺失数据处理为缺失	此指标表示工作负载完成 HTTP 请求的 p90 延迟。 此警报表示延迟（衡量网站客户体验的重要指标）。	该警报在上周进入“警报”状态 0 次。 存在问题？“否”或“是”（如果为“否”，则留空）：在执行特定的批处理作业期间，此警报频繁翻转。 解决人员：站点可靠性工程师	发送电子邮件至 *SRE@example.com* ，联系站点可靠性工程团队 为我们的 ECW 和 RDS 服务创建 AWS 支持 案例。 如果需要立即采取措施：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知##团队重启实例，或者刷新日志。（如果不需要立即采取措施，请留空）
工作负载请求可用性/ *CW Alarm ARN*/ 5 分钟内 5 个数据点的可用性 < 95%，将缺失数据处理为缺失。	此指标表示工作负载完成 HTTP 请求的可用性。每个时段的 HTTP 200 数量除以请求数。 此警报表示工作负载的可用性。	该警报在上周进入“警报”状态 0 次。 存在问题？“否”或“是”（如果为“否”，则留空）：在执行特定的批处理作业期间，此警报频繁翻转。 解决人员：站点可靠性工程师	发送电子邮件至 *SRE@example.com* ，联系站点可靠性工程团队 为我们的 ELB 和 Amazon Route 53 服务创建 AWS 支持 案例。 如果需要立即采取措施：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知##团队重启实例，或者刷新日志。（如果不需要立即采取措施，请留空）

指标名称/ARN/阈值	说明	备注	请求的操作
New Relic 警报示例			
端到端集成测试/ *CW Alarm ARN*/ 3 分钟持续时间内 1 分钟指标的失败率为 3%，将缺失数据处理为缺失 工作负载标识符：端到端测试工作流程，AWS 区域：US-EAST-1，AWS 账户 ID：012345678910	此指标用于测试请求是否可以遍历工作负载的每一层。如果该测试失败，则表示存在严重故障，无法处理业务交易。 此警报表示处理工作负载业务交易的能力。	该警报在上周进入“警报”状态 0 次。 存在问题？“否”或“是”（如果为“否”，则留空）：在执行特定的批处理作业期间，此警报频繁翻转。 解决人员：站点可靠性工程师	发送电子邮件至 *SRE@example.com* ，联系站点可靠性工程团队 为我们的 Amazon Elastic Container Service 和 Amazon DynamoDB 服务创建 AWS 支持 案例。 如果需要立即采取措施：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知##团队重启实例，或者刷新日志。（如果不需要立即采取措施，请留空）

事件检测及响应服务中的工作负载发现

AWS 将与您协作，尽可能多地了解有关您工作负载的背景信息。AWS 事件检测及响应服务团队会使用这些信息来创建运行手册，以便在发生事件时为您提供支持。所需的信息已在事件检测及响应服务中的工作负载加入和警报摄取问卷填写。最好是在 AppRegistry 中注册您的工作负载。有关更多信息，请参阅 AppRegistry 用户指南。

主要输出：

- 工作负载信息，例如工作负载说明、架构图、联系信息和上报详细信息等。
- 工作负载如何使用每个 AWS 区域的 AWS 服务的详细信息。

- 您的团队使用的警报，用于检测重大的工作负载影响。

为工作负载订阅事件检测及响应服务

为您要订阅 AWS 事件检测及响应服务的每个工作负载创建支持案例。

- 对于单账户工作负载：通过工作负载的账户或您的付款人账户提交。
- 对于多账户工作负载：通过您的付款人账户提交并列出所有账户 ID。

> **Important**
>
> 为工作负载订阅事件检测及响应服务时，如果使用错误的账户提交支持案例，可能会导致延迟并且需要提供更多信息。

要订阅工作负载，请完成以下步骤：

1. 打开 AWS 支持 中心，然后选择创建案例。您只能通过已经注册 Enterprise Support 的账户订阅工作负载。下图是 Support 中心控制台的示例。

2. 要填写支持案例表，请输入以下信息：
   - 选择技术支持。
   - 对于服务，选择事件检测和响应。
   - 对于类别，选择加入新工作负载。
   - 对于严重性，选择一般指导。
3. 为此更改输入主题。例如，您可以输入 [加入] AWS 事件检测及响应服务 - *workload_name*。
4. 为此更改输入描述。例如，您可以输入此请求是为了将工作负载加入到 AWS 事件检测及响应服务。

   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。这些账户是您想要加入 AWS 事件检测及响应服务的账户
   - 语言：有关事件检测及响应服务支持的语言的列表，请参阅事件检测及响应服务的区域可用性。
5. 在其他联系人 - 可选部分中，输入您希望接收有关此请求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 可能会延迟 AWS 事件检测及响应服务的加入流程。

6. 选择提交。

   提交请求后，您可以添加组织中的其它电子邮件。要添加电子邮件，请回复案例，然后在其他联系人 - 可选部分中添加电子邮件 ID。

   以下是回复按钮和其他联系人 - 可选部分的示例。

为订阅请求创建支持案例后，请准备好以下两个文档，以继续工作负载加入流程：

- AWS 工作负载架构图。
- 事件检测及响应服务中的工作负载加入和警报摄取问卷：在该问卷中填写与您要加入的工作负载有关的所有信息。如果您要加入多个工作负载，请为每个工作负载都创建一个新的加入问卷。如果您对填写加入问卷有疑问，请联系您的技术客户经理（TAM）。

> **Note**
>
> 请勿使用附加文件选项来将这两个文档附加到案例中。AWS 事件检测及响应服务团队回复案例时将会提供一个 Amazon Simple Storage Service 上传程序链接，供您上传文档。

有关如何通过 AWS 事件检测及响应服务创建案例以请求更改已加入的现有工作负载的信息，请参阅请求更改已加入事件检测及响应服务的工作负载。有关如何移除工作负载的信息，请参阅从事件检测及响应服务中移除工作负载。

在事件检测及响应服务中定义和配置警报

AWS 将与您协作，一起定义指标和警报，让您能够了解应用程序及其底层 AWS 基础设施的性能。我们要求警报在定义和配置阈值时符合以下标准：

- 警报只在受监控的工作负载遭受重大影响（收入损失/客户体验降级导致性能显著下降）且需要运维人员立即给予关注时才进入“警报”状态。
- 警报还必须在与事件管理团队联系的同时或联系之前，与您工作负载的指定事件解决人员联系。事件管理工程师会在风险缓解流程中与您指定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。
- 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。如果警报在“警报”和“正常”状态之间摇摆，会产生足够的影响以确保得到运维人员的响应和关注。

警报类型：

- 可描述业务影响程度并传递相关信息以进行简单故障检测的警报。
- Amazon CloudWatch 金丝雀警报。有关更多信息，请参阅金丝雀和 X-Ray 跟踪以及 X-Ray。
- 聚合警报（监控依赖关系）

下表提供了警报示例，所有警报均使用 CloudWatch 监控系统。

指标名称/警报阈值	警报 ARN 或资源 ID	如果此警报触发	如果已联系，请为这些服务提出高级支持案例
API 错误/ 10 个数据点的错误数 >= 10	arn:aws:cloudwatch:us-west-2:000000000000:alarm:E2MPmimLambda-Errors	工单转给数据库管理员（DBA）团队	Lambda、API Gateway
ServiceUnavailable（HTTP 状态代码 503）	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	工单转给服务团队	Lambda、API Gateway

指标名称/警报阈值	警报 ARN 或资源 ID	如果此警报触发	如果已联系，请为这些服务提出高级支持案例
5 分钟窗口内 10 个数据点（不同客户端）的错误数 >=3			
ThrottlingException（Http 状态码 400） 5 分钟窗口内 10 个数据点（不同客户端）的错误数 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	工单转给服务团队	EC2、Amazon Aurora

有关更多详细信息，请参阅AWS 事件检测及响应服务的监控和可观测性。

如果您更喜欢使用自动化工具来加载警报，则事件检测及响应服务命令行界面（CLI）有助于您部署和加载警报。有关更多详细信息，请参阅AWS 事件检测及响应服务 CLI。

主要输出：

- 工作负载警报的定义和配置。
- 加入问卷上填写警报详情。

主题

- 在事件检测及响应服务中创建符合您业务需求的 CloudWatch 警报
- 使用 CloudFormation 模板在事件检测及响应服务中构建 CloudWatch 警报
- 事件检测及响应服务中的 CloudWatch 警报使用案例示例

在事件检测及响应服务中创建符合您业务需求的 CloudWatch 警报

在创建 Amazon CloudWatch 警报时，您可以采取几个步骤来确保警报尽可能满足您的业务需求。

> **Note**
>
> 有关推荐要加入事件检测及响应服务的 AWS 服务 CloudWatch 警报示例，请参阅 AWS re:Post 上的事件检测及响应服务警报最佳实践。

查看您提出的 CloudWatch 警报

查看您提出的警报，以确保这些警报只在受监控的工作负载遭受重大影响（收入损失或客户体验降级导致性能显著下降）时才进入“警报”状态。例如，您是否认为此警报严重到在它进入“警报”状态后必须立即做出响应？

以下是可能表示重大业务影响的建议指标，例如影响最终用户使用应用程序的体验：

- CloudFront：有关更多信息，请参阅查看 CloudFront 和边缘函数指标。
- 应用程序负载均衡器：如果可能，最好为应用程序负载均衡器创建以下警报：
  - HTTPCode_ELB_5XX_Count
  - HTTPCode_Target_5XX_Count

  通过上述警报，您可以监控来自应用程序负载均衡器背后或其它资源背后的目标的响应。这样就可以更轻松地确定 5XX 错误的来源。有关更多信息，请参阅应用程序负载均衡器的 CloudWatch 指标。
- Amazon API Gateway：如果您在 Elastic Beanstalk 中使用 WebSocket API，那么可以考虑使用以下指标：
  - 集成错误率（筛选 5XX 错误）
  - 集成延迟
  - 执行错误

  有关更多信息，请参阅使用 CloudWatch 指标监控 WebSocket API 执行。
- Amazon Route 53：监控 EndPointUnhealthyENICount 指标。此指标是处于自动恢复状态的弹性网络接口数。此状态表示解析程序尝试恢复一个或多个与端点（通过 EndpointId 指定）关联的 Amazon Virtual Private Cloud 网络接口。在恢复过程中，端点会正常运行，但容量有限。并且在完全恢复之前，端点无法处理 DNS 查询。有关更多信息，请参阅使用 Amazon CloudWatch 监控 Amazon Route 53 Resolver 端点。

验证警报配置

确认您提出的警报符合自己的业务需求后，请验证警报的配置和历史记录：

- 根据指标的图表趋势，验证支持指标进入“警报”状态的阈值。
- 验证用于轮询数据点的时间段。在 60 秒时对数据点进行轮询有助于及早检测事件。
- 验证 DatapointToAlarm 配置。在大多数情况下，最佳做法是将其设置为 3/3 或 5/5。在事件中，如果设置为 [60 秒指标，DatapointToAlarm 为 3/3]，则警报在 3 分钟后触发；如果设置为 [60 秒指标，DatapointToAlarm 为 5/5]，则警报会在 5 分钟后触发。使用这一组合可以消除嘈杂的警报。

> **Note**
>
> 上述建议可能会因您使用服务的方式不同而有所差异。每项 AWS 服务在工作负载中的运行方式各不相同。而且，在多个地方使用同一服务时，其运行方式可能会有所不同。您必须确保了解自己的工作负载是如何利用提供警报的资源的，以及上游和下游的影响。

验证您的警报如何处理缺失数据

某些指标源不会定期向 CloudWatch 发送数据。对于这些指标，最好是将缺失数据处理为 notBreaching。有关更多信息，请参阅配置 CloudWatch 告警处理缺失数据的方式和避免提前转换到告警状态。

例如，如果某个指标用于监控错误率，然后没有错误，则该指标会报告无数据（零）数据点。如果您将警报配置为将缺失数据处理为缺失，则单个超出阈值的数据点后跟两个无数据（零）数据点会导致该指标进入“警报”状态（3/3 个数据点）。这是因为缺失数据配置会对评估周期内最后一个已知数据点进行评估。

对于指标监控错误率的情况，如果没有出现服务降级，您可以假设没有数据是一件好事。最佳做法是将缺失数据处理为 notBreaching，这样缺失数据就会被视为“正常”，该指标便不会基于单个数据点进入“警报”状态。

查看每个警报的历史记录

如果某个警报的历史记录显示其经常进入“警报”状态而后又快速恢复，那么该警报可能存在问题。确保调整警报以防出现噪音或误报警报。

验证底层资源的指标

确保您的指标查看有效的底层资源并使用正确的统计数据。如果警报配置为查看无效的资源名称，则警报可能无法跟踪底层数据。这可能会导致警报进入“警报”状态。

创建复合警报

如果您向事件检测及响应服务运维团队提供大量要加入的警报，则可能会要求您创建复合警报。复合警报可减少需要加入的警报总数。

使用 CloudFormation 模板在事件检测及响应服务中构建 CloudWatch 警报

为了更快地加入 AWS 事件检测及响应服务，并减少构建警报所需的工作，AWS 为您提供了 CloudFormation 模板。这些模板为常见的加入服务提供了优化的警报设置，例如应用程序负载均衡器、网络负载均衡器以及 Amazon CloudFront 等。

使用 CloudFormation 模板构建 CloudWatch 警报

1. 使用提供的链接下载模板：

NameSpac	指标	Compariso nOperator （阈值）	周期	Datapoint sToAlarm	TreatMiss ingData	统计数据	模板链接
应用程序弹性负载均衡器	(m1+m2)/(m1+m2+m m4)*100 m1=HTTP(de_Target _2XX_Cou t m2=HTTP(de_Target _3XX_Cou t m3=HTTP(de_Target _4XX_Cou t m4=HTTP(de_Target	LessThanT hreshold(95)	60	3/3	missing	总和	模板 –

NameSpac	指标	ComparisonOperator（阈值）	周期	DatapointsToAlarm	TreatMissingData	统计数据	模板链接
	_5XX_Count						
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3/3	notBreaching	平均值	模板 –
应用程序弹性负载均衡器	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3/3	notBreaching	最大值	模板 –
网络弹性负载均衡器	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3/3	notBreaching	最大值	模板 –

2. 查看下载的 JSON 文件，确保其符合贵组织的运营和安全流程。
3. 创建 CloudFormation 堆栈：

> **Note**
>
> 以下步骤使用标准的 CloudFormation 堆栈创建流程。有关详细步骤，请参阅通过 CloudFormation 控制台创建堆栈。

a. 打开 AWS CloudFormation 控制台，地址：https://console.aws.amazon.com/cloudformation。

b. 选择创建堆栈。

c. 选择模板已就绪，然后从本地文件夹上传模板文件。

以下是创建堆栈屏幕的示例。

d. 选择下一步。

e. 输入以下必要信息：

- AlarmNameConfig 和 AlarmDescriptionConfig：输入警报的名称和描述。
- ThresholdConfig：根据您应用程序的要求修改阈值。
- DistributionIDConfig：确保分发 ID 指向您创建 CloudFormation 堆栈的账户中的正确资源。

f. 选择下一步。

g. 查看 PeriodConfig、EvalutionPeriodConfig 以及 DatapointsToAlarmConfig 字段中的默认值。最好是使用这些字段的默认值。如有必要，您可以根据应用程序的要求进行相应调整。

h. （可选）根据需要输入标签和 SNS 通知信息。最好开启终止保护，以防警报被意外删除。要开启终止保护，请选中已激活单选按钮，如以下示例所示：

i. 选择下一步。

j. 检查您的堆栈设置，然后选择创建堆栈。

k. 创建堆栈后，您会看到警报已在 Amazon CloudWatch 警报列表中列出，如以下示例所示：

4. 在正确的账户和 AWS 区域创建所有警报后，请通知您的技术客户经理（TAM）。AWS 事件检测及响应服务团队会审核您新警报的状态，然后继续加入流程。

事件检测及响应服务中的 CloudWatch 警报使用案例示例

以下使用案例提供了如何在事件检测及响应服务中使用 Amazon CloudWatch 警报的示例。这些示例演示了如何配置 CloudWatch 警报来监控各项 AWS 服务的关键指标和阈值，从而使您能够识别和应对可能会影响您应用程序和工作负载可用性及性能的潜在问题。

使用案例示例 A：应用程序负载均衡器

您可以创建以下 CloudWatch 警报来指示潜在的工作负载潜在影响。为此，您需要创建一个指标数学表达式，当成功连接数降至特定阈值以下时，便会发出警报。有关可用的 CloudWatch 指标，请参阅[应用程序负载均衡器的 CloudWatch 指标]

指
标：`HTTPCode_Target_3XX_Count;HTTPCode_Target_4XX_Count;HTTPCode_Target_5XX_Count`

`(m1+m2)/(m1+m2+m3+m4)*100 m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 = HTTP Code 4xx || m4 = HTTP Code 5xx`

命名空间：AWS/ApplicationELB

ComparisonOperator(阈值)：小于 x (x = 客户的阈值) 。

时间段：60 秒

DatapointsToAlarm：3/3

缺失数据处理：将缺失数据处理为 breaching。

统计数据：Sum

下图显示了使用案例 A 的流程：

示例使用案例 B：Amazon API Gateway

您可以创建以下 CloudWatch 警报来指示潜在的工作负载潜在影响。为此，您需要创建一个复合指标，当 API Gateway 中存在高延迟或 4XX 错误平均数量较高时发出警报。有关可用的指标，请参阅 Amazon API Gateway 维度和指标

指标：`compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))`

命名空间：AWS/API Gateway

ComparisonOperator(阈值)：大于客户的阈值 x 或 y。

时间段：60 秒

DatapointsToAlarm：1/1

缺失数据处理：将缺失数据处理为 notBreaching。

统计数据 – 。

下图显示了使用案例 B 的流程：

示例使用案例 C：Amazon Route 53

您可以通过创建 Route 53 运行状况检查来监控您的资源，这些检查使用 CloudWatch 收集原始数据并将其处理为近乎实时的可读指标。您可以创建以下 CloudWatch 警报来指示潜在的工作负载潜在影响。您可以使用 CloudWatch 指标创建警报，以便在超出既定阈值时触发该警报。有关可用的 CloudWatch 指标，请参阅 Route 53 运行状况检查的 CloudWatch 指标

指标：R53-HC-Success

命名空间：AWS/Route 53

阈值 HealthCheckStatus：3 分钟内 3 个数据点的 HealthCheckStatus < x（x 是客户的阈值）

时间段：1 分钟

DatapointsToAlarm：3/3

缺失数据处理：将缺失数据处理为 breaching。

统计数据：Minimum

下图显示了使用案例 C 的流程：

示例使用案例 D：使用自定义应用程序监控工作负载

在这种情况下，花点时间定义适当的运行状况检查至关重要。如果您仅验证应用程序的端口是打开的，则说明您并未验证该应用程序是否正常运行。此外，调用应用程序的主页不一定是确定该应用程序是否正常运行的正确方法。例如，如果应用程序同时依赖一个数据库和 Amazon Simple Storage Service（Amazon S3），则运行状况检查必须验证所有元素。一种方法是创建一个监控网页，例如 /monitor。监控网页会调用数据库，以确保它可以连接并获取数据。而且，监控网页会调用 Amazon S3。然后，您再将负载均衡器上的运行状况检查指向 /monitor 页面。

下图显示了使用案例 D 的流程：

将警报摄取到 AWS 事件检测及响应服务

AWS 事件检测及响应服务支持通过 Amazon EventBridge 摄取警报。本节介绍如何将 AWS 事件检测及响应服务与不同的应用程序性能监控（APM）工具集成，包括 Amazon CloudWatch、与 Amazon EventBridge 直接集成的 APM（例如 Datadog 和 New Relic），以及没有与 Amazon EventBridge

直接集成的 APM。有关直接与 Amazon EventBridge 集成的 APM 的完整列表，请参阅 Amazon EventBridge integrations。

要了解有关使用事件检测及响应服务命令行界面（CLI）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 CLI。

主题

预置将警报摄取到事件检测及响应服务所需的访问权限

要让 AWS 事件检测及响应服务能够从您的账户摄取警报，请安装 `AWSServiceRoleForHealth_EventProcessor` 服务相关角色（SLR）。AWS 认为 SLR 可以创建 Amazon EventBridge 托管的规则。这些托管规则会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 托管策略）的信息，请参阅《AWS Health 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》中的创建服务相关角色中的说明在您的账户中安装此服务相关角色。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

- 在您的账户中成功安装服务相关角色。

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 AWS Health
- 创建服务相关角色

- AWS 托管策略：AWSHealth_EventProcessorServiceRolePolicy

将事件检测及响应服务与 Amazon CloudWatch 集成

AWS 事件检测及响应服务使用您在预置访问权限期间开启的服务相关角色（SLR）在名为 AWSHealthEventProcessor-DO-NOT-DELETE 的 AWS 账户中创建 Amazon EventBridge 托管的规则。事件检测及响应服务使用此规则来从您的账户中摄取 Amazon CloudWatch 警报。无需执行其它步骤即可从 CloudWatch 摄取警报。

从与 Amazon EventBridge 直接集成的 APM 摄取警报

下图演示了从与 Amazon EventBridge 直接集成的应用程序性能监控（APM）工具（例如 Datadog 和 Splunk）向 AWS 事件检测及响应服务发送通知的过程。有关与 EventBridge 直接集成的 APM 的完整列表，请参阅 Amazon EventBridge integrations。

要了解有关使用事件检测及响应服务命令行界面（CLI）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 CLI。

使用以下步骤设置与 AWS 事件检测及响应服务的集成。在执行这些步骤之前，请确认您的账户中已安装 AWS 服务相关角色（SLR）AWSServiceRoleForHealth_EventProcessor。

设置与 AWS 事件检测及响应服务的集成。

您必须针对每个 AWS 账户和 AWS 区域完成以下步骤。警报必须来自应用程序资源所在的 AWS 账户和 AWS 区域。

1. 将每个 APM 设置为 Amazon EventBridge 合作伙伴事件源（例如 aws.partner/my_apm/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。这样就会在您的账户中创建一个合作伙伴事件总线。
2. 请执行以下操作之一：
   - （推荐方法）创建自定义 EventBridge 事件总线。AWS 事件检测及响应服务通过 AWSServiceRoleForHealth_EventProcessor SLR 安装托管规则（AWSHealthEventProcessorEventSource-DO-NOT-DELETE）总线。规则源是自定义事件总线。规则目标是 AWS 事件检测及响应服务。该规则与摄取第三方 APM 事件的模式相匹配。
   - （替代方法）使用默认的事件总线，而非自定义事件总线。默认事件总线要求托管规则向 AWS 事件检测及响应服务发送 APM 警报。

3. 创建一个 AWS Lambda 函数（例如 My_APM-AWSIncidentDetectionResponse-LambdaFunction）来转换您的合作伙伴事件总线事件。转换后的事件与托管规则 AWSHealthEventProcessorEventSource-DO-NOT-DELETE 相匹配。

   a. 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。模式与托管规则相匹配。

   b. 将 Lambda 函数的目标设置为步骤 2 中创建的自定义事件总线（推荐方法）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 中定义的合作伙伴事件总线（例如，aws.partner/my_apm/integrationName）。规则的目标是您在步骤 3 中定义的 Lambda 函数（例如 My_APM-AWSIncidentDetectionResponse-LambdaFunction）。有关定义 EventBridge 规则的指南，请参阅 Amazon EventBridge 规则。

有关如何设置合作伙伴事件总线集成以用于 AWS 事件检测及响应服务的示例，请参阅示例：集成来自 Datadog 和 Splunk 的通知。

示例：集成来自 Datadog 和 Splunk 的通知

此示例提供了将 Datadog 和 Splunk 中的通知集成到 AWS 事件检测及响应服务的详细步骤。

主题

- 步骤 1：将您的 APM 设置为 Amazon EventBridge 中的事件源
- 步骤 2：创建自定义事件总线
- 步骤 3：创建用于转换的 AWS Lambda 函数
- 步骤 4：创建自定义 Amazon EventBridge 规则

步骤 1：将您的 APM 设置为 Amazon EventBridge 中的事件源

在您的 AWS 账户中将每个 APM 设置为 Amazon EventBridge 中的事件源。有关将您的 APM 设置为事件源的说明，请参阅 Amazon EventBridge 合作伙伴中针对您工具的事件源设置说明。

通过将 APM 设置为事件源，您可以将来自 APM 的通知摄取到您 AWS 账户中的事件总线中。设置完成后，AWS 事件检测及响应服务可在事件总线收到事件时启动事件管理流程。此流程会在您的 APM 中将 Amazon EventBridge 添加为目标。

步骤 2：创建自定义事件总线

最好是使用自定义事件总线。AWS 事件检测及响应服务使用自定义事件总线来摄取转换后的事件。AWS Lambda 函数将转换伙伴事件总线事件，并将其发送至自定义事件总线。AWS 事件检测及响应服务会安装托管规则，用于从自定义事件总线摄取事件。

您可以使用默认的事件总线，而非自定义事件总线。AWS 事件检测及响应服务会修改托管规则，以便从默认事件总线而非自定义事件总线摄取事件。

在 AWS 账户中创建自定义事件总线：

1. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
2. 选择总线、事件总线。
3. 在自定义事件总线下，选择创建。
4. 在名称下为您的事件总线提供一个名称。推荐采用以下格式：APMName-AWSIncidentDetectionResponse-EventBus。

   例如，如果您使用的是 Datadog 或 Splunk，请使用以下对应的格式：

   - Datadog：Datadog-AWSIncidentDetectionResponse-EventBus
   - Splunk：Splunk-AWSIncidentDetectionResponse-EventBus

步骤 3：创建用于转换的 AWS Lambda 函数

Lambda 函数将在步骤 1 中的合作伙伴事件总线和步骤 2 中的自定义（或默认）事件总线之间转换事件。Lambda 函数转换符合 AWS 事件检测及响应服务托管规则。

在 AWS 账户中创建 AWS Lambda 函数

1. 打开 AWS Lambda 控制台的 Functions (函数) 页面。
2. 选择创建函数。
3. 选择从头开始创作选项卡。
4. 对于函数名称，输入一个采用 `APMName-AWSIncidentDetectionResponse-LambdaFunction` 格式的名称。

   以下是 Datadog 和 Splunk 的示例：

   - Datadog：Datadog-AWSIncidentDetectionResponse-LambdaFunction
   - Splunk：Splunk-AWSIncidentDetectionResponse-LambdaFunction

5. 对于运行时，选择 Python 3.10。
6. 将其余字段保留默认值。选择创建函数。
7. 在代码编辑页面上，将默认的 Lambda 函数内容替换为以下代码示例中的函数。

   请注意以下代码示例中以 # 开头的注释。这些注释指出了要更改的值。

   Datadog 转换代码模板：

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example 'Datadog-AWSIncidentDetectionResponse-EventBus'
EventBusName = "Datadog-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # Replace the dictionary path, event["detail"]["meta"]["monitor"]["name"], with
 the path to your alert name based on your APM payload.
    # This example is for finding the alert name for Datadog.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["meta"]["monitor"]["name"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
     Entries=[
              {
               'Detail': json.dumps(event["detail"], indent=2),
               'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
               'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
               'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
```

```
            }
     ]
    )
    print(response['Entries'])
```

Splunk 转换代码模板：

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example Splunk-AWSIncidentDetectionResponse-EventBus
EventBusName = "Splunk-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # replace the dictionary path event["detail"]["ruleName"] with the path to your
 alert name based on your APM payload.
    # This example is for finding the alert name in Splunk.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["ruleName"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
    Entries=[
             {
              'Detail': json.dumps(event["detail"], indent=2),
              'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
              'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
              'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
            }
```

```
        ]
    )
    print(response['Entries'])
```

8. 选择部署。
9. 为要接收转换后数据的事件总线的 Lambda 执行角色添加 PutEvents 权限：
   a. 打开 AWS Lambda 控制台的 Functions (函数) 页面。
   b. 选择函数，然后在配置选项卡上选择权限。
   c. 在执行角色下，选择角色名称以在 AWS Identity and Access Management 控制台中打开执行角色。
   d. 在权限策略下，选择现有的策略名称以打开策略。
   e. 在此策略中定义的权限下，选择编辑。
   f. 在策略编辑器页面上，选择添加新语句：
   g. 策略编辑器会添加一个新的空白语句，类似于以下内容

   h. 将自动生成的新语句替换为以下内容：

```
{
  "Sid": "AWSIncidentDetectionResponseEventBus0",
  "Effect": "Allow",
  "Action": "events:PutEvents",
  "Resource": "arn:aws:events:{region}:{accountId}:event-bus/{custom-eventbus-name}"
}
```

   i. 资源是您在步骤 2：创建自定义事件总线中创建的自定义事件总线的 ARN，或者，如果您在 Lambda 代码中使用默认事件总线，则为默认事件总线的 ARN。
10. 查看并确认已为角色添加所需权限。
11. 选择将此新版本设为默认版本，然后选择保存更改。

有效载荷转换需要什么？

AWS 事件检测及响应服务摄取的事件总线事件中需要以下 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。

```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "alert_type": "error",
      "event_type": "query_alert_monitor",
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
```

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

请注意，在转换事件之前，`detail-type` 表示发出警报的 APM，源来自合作伙伴 APM，`incident-detection-response-identifier` 键不存在。

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。转换后的有效载荷目前包含所需的键值对。

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "incident-detection-response-identifier": "UnHealthyHostCount",
      "alert_type": "error",
      "event_type": "query_alert_monitor",
```

```
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
          "metadata": {
            "monitor_id": 222222,
            "metric": "aws.applicationelb.un_healthy_host_count"
          }
        },
        "transition": {
          "trans_name": "Triggered",
          "trans_type": "alert"
        },
        "states": {
          "source_state": "OK",
          "dest_state": "Alert"
        },
        "duration": 0
      },
      "priority": "normal",
      "source_type_name": "Monitor Alert",
      "tags": [
        "aws_account:123456789012",
        "monitor"
      ]
```

```
    }
}
```

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。

在上面的示例中，incident-detection-response-identifier 值取自路径 $.detail.meta.monitor.name 下的警报名称。APM 警报名称路径因 APM 而异。Lambda 函数必须修改为从正确的合作伙伴事件 JSON 路径中获取警报名称并将其用于 incident-detection-response-identifier 值。

incident-detection-response-identifier 上设置的每个唯一名称会在加入期间提供给 AWS 事件检测及响应服务团队。不会处理 incident-detection-response-identifier 名称未知的事件。

步骤 4：创建自定义 Amazon EventBridge 规则

步骤 1 中创建的合作伙伴事件总线需要您创建的 EventBridge 规则。该规则将所需的事件从合作伙伴事件总线发送到步骤 3 中创建的 Lambda 函数。

有关定义 EventBridge 规则的指南，请参阅 Amazon EventBridge 规则。

1. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
2. 选择规则，然后选择与您的 APM 关联的合作伙伴事件总线。以下是合作伙伴事件总线示例：
   - Datadog：aws.partner/datadog.com/eventbus-name
   - Splunk：aws.partner/signalfx.com/RandomString
3. 选择创建规则，创建新的 EventBridge 规则。
4. 对于规则名称，请按 APMName-AWS Incident Detection and Response-EventBridgeRule 格式输入名称，然后选择下一步。名称示例如下：
   - Datadog：Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk：Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. 对于事件源，选择 AWS 事件或 EventBridge 合作伙伴事件。
6. 将示例事件和创建方法保留为默认值。
7. 对于事件模式，请选择以下内容：

a. 事件源：EventBridge 合作伙伴。
b. 合作伙伴：选择您的 APM 合作伙伴。
c. 事件类型：所有事件。

以下是示例事件模式：

Datadog 事件模式示例

Splunk 事件模式示例

8. 对于目标，请选择以下内容：
   a. 目标类型：AWS 服务
   b. 选择目标：选择 Lambda 函数。
   c. 函数：您在步骤 2 中创建的 Lambda 函数的名称。
9. 选择下一步、保存规则。

使用 Webhook 从未与 Amazon 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。要了解有关使用事件检测及响应服务命令行界面（CLI）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 CLI。

有关与 Amazon EventBridge 直接集成的 APM 的列表，请参阅 Amazon EventBridge integrations。

使用以下步骤设置与 AWS 事件检测及响应服务的集成。在执行这些步骤之前，请确认您的账户中已安装 AWS 托管规则 AWSHealthEventProcessorEventSource-DO-NOT-DELETE

使用 Webhook 摄取事件

1. 定义 Amazon API Gateway 以接受来自您 APM 的有效载荷。
2. 使用身份验证令牌定义用于授权的 AWS Lambda 函数，如上图所示。
3. 定义第二个 Lambda 函数来转换并将 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。

4. 将您的 APM 设置为向 API Gateway 生成的 URL 发送通知。

AWS 事件检测及响应服务 CLI

AWS 事件检测及响应服务客户命令行界面（CLI）是一款命令行界面工具，可简化您加载到 AWS 事件检测及响应服务的方式。

AWS CloudShell 中的事件检测及响应服务 CLI 用于收集加载信息，通过资源组标记 API 收集 AWS 资源数据，并管理支持案例。CLI 可以创建新的 Amazon CloudWatch 警报或摄取现有警报，还可以通过 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。您可以在交互模式下运行此 CLI 以指导您完成加载步骤，也可以在离线模式下运行批量或 DevOps 使用案例。

有关如何使用 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 CLI。

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。这一部分介绍了这些基本步骤，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，在加入前对新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

事件检测及响应服务会依据您在加入问卷中提供的信息来创建运行手册和响应计划，以便有效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发现期间提供的信息创建这些模板。响应计划是用于触发事件的 AWS Systems Manager（SSM）文档模板。要了解有关 SSM 文档的更多信息，请参阅 AWS Systems Manager 文档。要了解有关事件管理器的更多信息，请参阅什么是 AWS Systems Manager Incident Manager？

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警报、运行手册和响应计划的定义。

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：

```
Runbook template for AWS Incident Detection and Response
# Description
This document is intended for [CustomerName] [WorkloadName].
```

```
[Insert short description of what the workload is intended for].

## Step: Priority
**Priority actions**
1. When a case is created with Incident Detection and Response, lock the case to
 yourself, verify the Customer Stakeholders in the Case from *Engagement Plans -
 Initial Engagement*.
2. Send the first correspondence on the support case to the customer as below. If
 there is no support case or if it is not possible to use the support case then backup
 communication details are listed in the steps that follow.

```
Hello,

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

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
```


Compliance and regulatory requirements for the workload
<<e.g. The workload deals with patient health records which must be kept secured and
 confidential. Information not to be shared with any third parties.>>

Actions required from Incident Detection and Response in complying
<<e.g Incident Management Engineers must not shared data with third parties.>>

Step: Information
Review of common information

* This section provides a space for defining common information which may be needed
 through the life of the incident.
* The target user of this information is the Incident Management Engineer and
 Operations Engineer.
* The following steps may reference this information to complete an action (for
 example, execute the "Initial Engagement" plan).

Engagement plans

Describe the engagement plans applicable to this runbook. This section contains
 only contact details. Engagement plans will be referenced in the step by step
 Communication Plans.
```

```
* **Initial engagement**

AWS Incident Detection and Response Team will add customer stakeholder addresses below
 to the Support Case. AWS Stakeholders are for additional stakeholders that may need to
 be made aware of any issues.
When updating customer stakeholders details in this plan also update the Backup Mailto
 links.
  * ***Customer Stakeholders***:  customeremail1; customeremail2; etc
  * ***AWS Stakeholders***: aws-idr-oncall@amazon.com; tam-team-email; etc.
  * ***One Time Only Contacts***: [These are email contacts that are included on only
 the first communication. Remove these contacts after the first communication has gone
 out. These could be customer paging email addresses such as pager-duty that must not
 be paged for every correspondence]
  * ***Backup Mailto Impact Template***: <*Insert Impact Template Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.
  * ***Backup Mailto No Impact Template***: <*Insert No Impact Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.


* **Engagement Escalation**

AWS Incident Detection and Response will reach out to the following contacts when the
 contacts from the **Initial engagement** plan do not respond to incidents.
For each Escalation Contact indicate if they must be added to the support case, phoned
 or both.
  * ***First Escalation Contact***: [escalationEmailAddress#1] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * ***Second Escalation Contact***: [escalationEmailAddress#2] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * Etc;
---
**Communication plans**

Describe how Incident Management Engineer communicates with designated stakeholders
 outside the incident call and communication channels.

* **Impact Communication plan**
This plan is initiated when Incident Detection and Response have determined from step
 **Triage** that an alert indicates potential impact to a customer.
```

```
Incident Detection and Response will request the customer to join the predetermined
 bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated
 in **Engagement plans - Incident call setup**.
All backup email templates for use when cases can't be used are in **Engagement plans -
 Initial engagement**.
  * 1 – Before sending the impact notification, verify then remove and/or add customer
 contacts from the Support Case CC based on the contacts listed in the **Initial
 engagement** Engagement plan.
  * 2 – Send the engagement notification to the customer based the following Template:

    (choose one and remove the rest)
    ***Impact Template - Chime Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
    Please join the Chime Bridge below so we can start the steps outlined in your
 Runbook:
        <insert Chime Meeting ID>
        <insert Link to Chime Bridge>
        International dial-in numbers: https://chime.aws/dialinnumbers/
    ```

    ***Impact Template - Customer Provided Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023 3:30 PM UTC>
    Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
    ```
    ***Impact Template - Customer Static Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
    Please join the Bridge below so we can start the steps outlined in your Runbook:
        Conference Number: <insert conference number>
        Conference URL : <insert bridgeURL>
```
```

```
    ```
  * 3 - Set the Case to Pending Customer Action
  * 4 - Follow **Engagement Escalation** plan as mentioned above.
  * 5 - If the customer does not respond within 30 minutes, disengage and continue to
 monitor until the alarm recovers.

* **No Impact Communication plan**
This plan is initiated when an alarm recovers before Incident Detection and Response
 have completed initial **Triage**.
  * 1 - Before sending the no impact notification, verify then remove and/or add
 customer contacts from the Support Case CC based on the contacts listed in the
 Engagement plans - Initial engagement Engagement plan.
  * 2 - Send a no engagement notification to the customer based on the below template:

  No Impact Template
  ```
  AWS Incident Detection and Response received an alarm that has recovered for your
 workload.
      Alarm Identifier -  <insert CloudWatch Alarm ARN or APM Response Identifier>
      Alarm State Change Reason -  <insert state change reason>
      Alarm Start Time -  <Example: 1 January 2023, 3:30 PM UTC>
      Alarm End Time -  <Example: 1 January 2023, 3:35 PM UTC>
  This may indicate a brief customer impact that is currently not ongoing.
  If there is an ongoing impact to your workload, please let us know and we will engage
 to assist.
  ```
  * 3 - Put the case in to Pending Customer Action.
  * 4 - If the customer does not respond within 30 minutes Resolve the case.

* **Updates**
If AWS Incident Detection and Response is expected to provide regular updates to
 customer stakeholders, list those stakeholders here. Updates must be sent via the same
 support case.
Remove this section if not needed.
  * Update Cadence: Every XX minutes
  * External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc
  * Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

---
Application architecture overview

This section provides an overview of the application/workload architecture for Incident
 Management Engineer and Operations Engineer awareness.
```
```

```
* **AWS Accounts and Regions with key services** - list of AWS accounts with regions
 supporting this application. Assists Engineers in assessing underlying infrastructure
 supporting the application.
    * 123456789012
      * US-EAST-1 - brief desc as appropriate
        * EC2 - brief desc as appropriate
        * DynamoDB - brief desc as appropriate
        * etc.
      * US-WEST-1 - brief desc as appropriate
      * etc.
    * another-account-etc.

* **Resource identification** - describe how engineers determine resource association
 with application
    * Resource groups: etc.
    * Tag key/value: AppId=123456

* **CloudWatch Dashboards** - list dashboards relevant to key metrics and services
  * 123456789012
    * us-east-1
      * some-dashboard-name
      * etc.
  * some-other-dashboard-name-in-current-acct

## Step: Triage
**Evaluate incident and impact**
This section provides instructions for triaging of the incident to determine correct
 impact, description, and overall correct runbook being executed.

* **Evaluation of initial incident information**
  * 1 - Review Incident Alarm, noting time of first detected impact as well as the
 alarm start time.
  * 2 - Identify which service(s) in the customer application is seeing impact.
  * 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions
 with key services**.
  * 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

---
* **Impact**
Impact is determined when either the customer's metrics do not recover, appear to be
 trending worse or if there is indication of AWS Service Impact.
  * 1 – Start **Communication plans - Impact Communication plan**
  * 2 - Start **Engagement plans - Engagement Escalation** if no response is received
 from the **Initial Engagement** contacts.
```

```
  * 3 - Start **Communication plans - Updates** if specified in **Communication plans**

* **No Impact**
No Impact is determined when the customer's alarm recovers before Triage is complete
 and there are no indications of AWS service impact or sustained impact on the
 customer's CloudWatch Dashboards.
  * 1 - Start **Communication plans - No Impact Communication plan**

## Step: Investigate
**Investigation**

  This section describes performing investigation of known and unknown symptoms.

**Known issue**
  * *List all known issues with the application and their standard actions here*

**Unknown issues**
  * Investigate with the customer and AWS Premium Support.
  * Escalate internally as required.

## Step: Mitigation
**Collaborate**
* Communicate any changes or important information from the **Investigate** step to the
 members of the incident call.

**Implement mitigation**
* ***List customer failover plans / Disaster Recovery plans / etc here for implementing
 mitigation.

## Step: Recovery
**Monitor customer impact**
* Review metrics to confirm recovery.
* Ensure recovery is across all Availability Zones / Regions / Services
* Get confirmation from the customer that impact is over and the application has
 recovered.

**Identify action items**
* Record key decisions and actions taken, including temporary mitigation that might
 have been implemented.
* Ensure outstanding action items have assigned owners.
* Close out any Communication plans that were opened during the incident with a final
 confirmation of recovery notification.
```

测试已加入事件检测及响应服务的工作负载

> **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。

加入流程的最后一步是为您的新工作负载执行游戏日演练。警报摄取完成后，AWS 事件检测及响应服务会确认您选择开始执行游戏日演练的日期和时间。

您的游戏日演练有两个主要目的：

- 功能验证：确认 AWS 事件检测及响应服务可以正常接收您的警报事件。而且，功能验证可确认您的警报事件是否可以触发相应的运行手册以及任何其它所需的操作，例如，会根据您的选择在警报摄取期间自动创建案例。
- 模拟：游戏日演练是对真实事件中可能发生的情况进行端到端模拟。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指示，进而改进参与。

在警报测试期间，AWS 事件检测及响应服务团队会与您协作，纠正发现的任何问题。

CloudWatch 警报

AWS 事件检测及响应服务通过监控警报的状态变化来测试您的 Amazon CloudWatch 警报。为此，请使用 AWS Command Line Interface手动将警报改为警报状态。您还可以从 AWS CloudShell 访问 AWS CLI。AWS 事件检测及响应服务为您提供了一系列 AWS CLI 命令供您在测试期间使用。

设置警报状态的 AWS CLI 命令示例：

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

要详细了解如何手动更改 CloudWatch 警报的状态，请参阅 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指示来模拟警报。游戏日演练开始时，AWS 事件检测及响应服务将要求您暂时更改警报阈值或比较运算符，以强制警报进入警报状态。此状态会触发 AWS 事件检测及响应服务的有效载荷。

主要输出

主要输出：

- 成功摄取警报并正确配置警报。
- AWS 事件检测及响应服务成功创建并摄取警报。
- 系统会为您的联系创建支持案例，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联系。
- 游戏日演练期间生成的所有警报和支持案例均得以解决。
- 系统会发送一封正式上线电子邮件，确认您的工作负载已受 AWS 事件检测及响应服务监控。

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

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

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。 • 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。

指标数学函数	使用案例	说明
		• 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。要了解有关使用事件检测及响应服务命令行界面（CLI）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 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。
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

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

1. 打开 AWS Support Center Console，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，选择活动事件。
5. 对于严重性，选择关键业务系统停机。
6. 输入此事件的主题。例如：

   AWS 事件检测及响应服务 - 活动事件 - workload_name
7. 输入此事件的问题描述。添加以下详细信息：
   - 技术信息：

     工作负载名称

     受影响的 AWS 资源 ARN
   - 业务信息：

     业务影响描述

     [可选] 客户桥详细信息
8. 为了方便我们更快地与 AWS 专家联系，请提供以下详细信息：
   - 受影响的 AWS 服务
   - 受影响的更多服务/其它服务
   - 受影响的 AWS 区域
9. 在其他联系人部分，输入您希望接收有关此事件的通信信息的所有电子邮件地址。

   下图是控制台屏幕，其中突出显示了其他联系人字段。

10选择提交。

   提交事件响应请求后，您可以添加组织中的其它电子邮件地址。要添加其它地址，请回复案例，然后在其他联系人部分添加电子邮件地址。

   下图显示了案例详细信息屏幕，其中突出显示了回复按钮。

下图显示了案例回复，其中突出显示了其他联系人字段和提交按钮。

11AWS 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 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，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 云的全球基础结构。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
“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
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：事件检测及响应服务客户命令行界面（CLI）	添加了事件检测及响应服务客户命令行界面（CLI）部分，并更新了入门一章，以包含有关事件检测及响应服务客户命令行界面（CLI）的信息。 有关更多信息，请参阅 AWS 事件检测及响应服务 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

更改	描述	日期
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。有关更多信息，请参阅 事件检测及响应服务中的工作负载加入和警报摄取问卷。	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

更改	描述	日期
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，请参阅账户订阅。	2024 年 3 月 28 日

更改	描述	日期
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。 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	2024 年 2 月 2 日
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： • 事件检测及响应服务中的工作负载发现 • 加入事件检测及响应服务 • 为工作负载订阅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：预置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

更改	描述	日期
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。 更新了以下部分：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：为工作负载订阅事件检测及响应服务	2023 年 9 月 5 日

更改	描述	日期
“入门”中新增一个部分	增加了将警报摄取到 AWS 事件检测及响应服务，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