AWS 事件检测和响应的概念和程序

AWS 事件检测和响应用户指南

版本 May 15, 2025

AWS 事件检测和响应用户指南: AWS 事件检测和响应的概念和程序

Table of Contents

什么是 AWS 事件检测和响应？

AWS 事件检测和响应为符合条件的 E AWS nterprise Support 客户提供了主动的事件参与，以降低故障的可能性并加快关键工作负载从中断中恢复的速度。事件检测和响应有助于您与 AWS 之合作，开发针对每项已上岗工作负载量定制的运行手册和响应计划。

事件检测和响应提供以下主要功能：

- 提高可观察性： AWS 专家提供指导，帮助您在工作负载的应用程序和基础架构层之间定义和关联指标和警报，从而尽早发现中断。
- 5 分钟响应时间：事件管理工程师 (IMEs) 全天候监控您的载入工作负载，以检测严重事件。在警报触发后 5 分钟内 IMEs 做出响应，或者对您向事件检测和响应提出的业务关键型 Support 案例做出响应。
- 更快地解决问题： IMEs 使用为您的工作负载开发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，并管理工作负载中的事件。 IMEs 为事件提供单线程所有权，让你与合适的 AWS 专家保持接触，直到事件得到解决。
- 事件事件管理：由于我们了解您的关键工作负载（例如账户、服务和实例）的背景，因此我们可以检测 AWS 服务事件期间您的工作负载可能受到的影响，并主动通知您。 AWS 如有要求， IMEs 请在 AWS 服务活动期间与您接触，并提供活动的最新信息。虽然事件检测和响应无法在服务事件期间优先考虑您的恢复，但事件检测和响应确实提供了 Support 指导，以帮助您实施缓解计划。
- 降低失败的可能性：解决问题后，将根据要求 IMEs 为您提供事后审查。而且， AWS 专家与您合作，运用经验教训来改进事件响应计划和操作手册。您还可以利用 AWS Resilience Hub 对工作负载进行持续的弹性跟踪。

主题

事件检测和响应使用条款

以下列表概述了使用 AWS 事件检测和响应的主要要求和限制。在使用服务之前，请务必了解这些信息，因为它涵盖了支持计划要求、入职流程和最低订阅期限等方面。

- AWS 事件检测和响应适用于直接账户和合作伙伴转售的 Enterprise Support 账户。
- AWS 事件检测和响应不适用于合作伙伴主导的 Support 账户。
- 在事件检测和响应服务期限内，您必须始终维护 E AWS nterprise Support。有关信息，请参阅E nterprise Suppor t。终止 Enterprise Support 会导致同时从 AWS 事件检测和响应服务中删除。
- AWS 事件检测和响应上的所有工作负载都必须通过工作负载载载入流程。
- 订阅 AWS 事件检测和响应账户的最短期限为九十 (90) 天。所有取消申请必须在预定的取消生效日期前三十 (30) 天提交。
- AWS 按照《AWS 隐私声明》中所述处理您的信息。

> **Note**
>
> 有关事件检测和响应计费的问题，请参阅获取 AWS 账单帮助。

事件检测和响应架构

AWS 事件检测和响应可与您的现有环境集成，如下图所示。该架构包括以下服务：

- 亚马逊 EventBridge：亚马逊 EventBridge 是您的工作负载与 AWS 事件检测和响应之间的唯一集成点。警报是 EventBridge 使用由管理的预定义规则通过亚马逊 CloudWatch从您的监控工具（例如亚马逊）中提取的 AWS。要允许 “事件检测和响应” 构建和管理 EventBridge 规则，您需要安装服务相关角色。要了解有关这些服务的更多信息，请参阅什么是亚马逊 EventBridge和亚马逊 EventBridge 规则，什么是亚马逊 CloudWatch，以及使用服务相关角色的 AWS Health用途。
- AWS Health： AWS Health 提供对您的资源绩效以及 AWS 服务 和账户可用性的持续可见性。事件检测和响应 AWS Health AWS 服务 用于跟踪您的工作负载所使用的事件，并在收到来自您的工作负载的警报时通知您。要了解更多信息 AWS Health，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 资源的自动化和任务管理。AWS 事件检测和响应在 AWS Systems Manager 文档中托管了有关您的工作负载的信息，包括工作负载架构图、警报详情及其相应的事件管理操作手册（有关详细信息，请参阅AWS Systems Manager 文档）。要了解更多信息 AWS Systems Manager，请参阅什么是 AWS Systems Manager。
- 您的具体操作手册：事件管理操作手册定义了 AWS 事件检测和响应在事件管理期间执行的操作。您的具体运行手册会告知 AWS 事件检测和响应应联系谁、如何联系他们以及要共享哪些信息。

事件检测和响应中的角色和职责

AWS 事件检测和响应 RACI（负责任、负责、咨询和知情）表概述了与事件检测和响应相关的各种活动的角色和责任。此表有助于定义客户和 AWS 事件检测和响应团队参与数据收集、运营准备情况审查、账户配置、事件管理和事后审查等任务的情况。

活动	Customer	事件检测和响应
数据收集		
客户和工作负载简介	已咨询	负责任
架构	负责任	负责任
运营	负责任	负责任
确定要配置的 CloudWatch 警报	负责任	负责任
定义事件响应计划	负责任	负责任
填写入职问卷	负责任	负责任
运营准备情况审查		
对工作负载进行精心设计的审查 (WAR)	已咨询	负责任
验证事件响应	已咨询	负责任
验证警报矩阵	已咨询	负责任
确定工作负载正在使用的关键 AWS 服务	负责任	负责任
账户配置		
在客户账户中创建 IAM 角色	负责任	知情
使用已创建的角色安装托管 EventBridge 规则	知情	负责任
测试 CloudWatch 警报	负责任	负责任

活动	Customer	事件检测和响应
验证客户警报是否与事件检测和响应相关	知情	负责任
更新警报	负责任	已咨询
更新运行手册	已咨询	负责任
事件管理		
主动通知事件检测和响应检测到的事件	知情	负责任
提供事件响应	知情	负责任
提供事件解决方案/恢复基础架构	负责任	已咨询
事后审查		
请求事后审查	负责任	知情
提供事后审查	知情	负责任

事件检测和响应的区域可用性

AWS 事件检测和响应目前提供英语和日语版本，适用于托管在以下任一网站的 Enterprise Support 账户 AWS 区域：

名称	AWS 区域
us-east-1	美国东部（弗吉尼亚）
us-east-2	美国东部（俄亥俄州）
us-west-1	美国西部（加利福尼亚北部）
us-west-2	美国西部（俄勒冈州）
ca-central-1	加拿大（中部）

名称	AWS 区域
ca-west-1	加拿大西部（卡尔加里）
sa-east-1	南美洲（圣保罗）
eu-central-1	欧洲地区（法兰克福）
eu-west-1	欧洲地区（爱尔兰）
eu-west-2	欧洲地区（伦敦）
eu-west-3	欧洲地区（巴黎）
eu-north-1	欧洲地区（斯德哥尔摩）
eu-central-2	欧洲（苏黎世）
eu-south-1	欧洲地区（米兰）
eu-south-2	欧洲地区（西班牙）
ap-south-1	亚太地区（孟买）
ap-northeast-1	亚太地区（东京）
ap-northeast-2	亚太地区（首尔）
ap-southeast-1	亚太地区（新加坡）
ap-southeast-2	亚太地区（悉尼）
ap-east-1	亚太地区（香港）
ap-northeast-3	亚太地区（大阪）
ap-south-2	亚太地区（海得拉巴）
ap-southeast-3	亚太地区（雅加达）
ap-southeast-4	亚太地区（墨尔本）

名称	AWS 区域
ap-southeast-5	亚太地区（马来西亚）
af-south-1	非洲（开普敦）
il-central-1	以色列（特拉维夫）
me-central-1	中东（阿联酋）
me-south-1	中东（巴林）

开始学习事件检测和响应

工作负载和警报是 AWS 事件检测和响应的核心。 AWS 与您密切合作，定义和监控对您的业务至关重要的特定工作负载。 AWS 帮助您设置警报，快速将重大绩效问题或客户影响通知您的团队。正确配置的警报对于在事件检测和响应中进行主动监控和快速事件响应至关重要。

工作负载

您可以使用 AWS 事件检测和响应选择特定工作负载进行监控和关键事件管理。工作负载是资源和代码的集合，它们协同工作以提供业务价值。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。您可以在单个 AWS 账户或多个 AWS 账户中托管工作负载。

例如，您可能在单个账户中托管了一个整体应用程序（例如，下图中的员工绩效应用程序）。或者，您可能将一个应用程序（例如图中的 Storefront Webapp）分解为跨不同账户的微服务。工作负载可能与其他应用程序或工作负载共享资源（例如数据库），如图所示。

要开始使用工作负载入门，请参阅工作负载入和工作负载入入问卷。

警报

警报是事件检测和响应的关键部分，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 与您合作定义适当的指标和警报阈值，这些指标和警报阈值只有在您监控的工作负载受到严重影响时才会触发。目标是让警报与您指定的解决人员接触，然后他们可以与事件管理团队合作以快速缓解任何问题。应将警报配置为仅在性能或客户体验明显下降且需要立即注意时才进入警报状态。一些关键类型的警报包括指示业务影响的警报、Amazon CloudWatch Canaries 警报和监控依赖关系的聚合警报。

要开始使用警报摄取，请参阅警报摄取和警报摄取调查问卷。

> **Note**
>
> 要更改您的运行手册、工作负载信息或 AWS 事件检测和响应中监控的警报，请参阅在 “事件检测和响应” 中请求更改已载入的工作负载。

入门事件检测和响应

AWS 与您合作，将您的工作负载和警报加入到 AWS 事件检测和响应中。您需要 AWS 在中提供关键信息事件检测和响应中的工作负载入和警报摄取问卷。最佳做法是同时注册工作负载 AppRegistry。有关更多信息，请参阅 AppRegistry 《用户指南》。

下图显示了 “事件检测和响应” 中工作负载入和警报摄取的流程：

工作负载入门

在工作负载启动期间， AWS 与您合作，了解您的工作量，以及如何在事件和 AWS 服务事件期间为您提供支持。您提供有关工作负载的关键信息，以帮助缓解影响。

主要产出：

- 一般工作负载信息
- 架构细节，包括图表
- 运行手册信息
- 客户发起的事件
- AWS 服务活动

警报摄取

AWS 与您配合使用警报器。AWS 事件检测和响应可以通过 Amazon 接收来自亚马逊 CloudWatch 和第三方应用程序性能监控 (APM) 工具的警报。 EventBridge入职警报可实现主动事件检测和自动互动。有关更多信息，请参阅从中提取与 Amaz APMs on EventBridge 直接集成的警报。

主要产出：

- 警报矩阵

下表列出了将工作负载加载到 AWS 事件检测和响应所需的步骤。下表显示了每项任务的持续时间示例。每项任务的实际日期是根据团队的空闲时间和日程安排来定义的。

事件检测和响应中的工作负载入和警报摄取问卷

本页提供了在向 AWS 事件检测和响应中加入工作负载以及配置警报以接收到服务时需要填写的调查问卷。工作负载入职调查表涵盖有关您的工作负载、其架构详细信息以及事件响应联系人的一般信息。在警报摄取调查问卷中，您可以在 “事件检测和响应” 中为您的工作负载指定应触发事件创建的关键警报，以及有关应联系谁以及应采取哪些措施的运行手册信息。正确填写这些调查问卷是为您的 AWS 工作负载设置监控和事件响应流程的关键步骤。

下载工作负载入职调查表。

下载警报摄取问卷。

工作负载入职调查表-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（包括任何缩写）	亚马逊零售业务 (ARO)
主要最终用户和该工作负载的功能。	此工作负载是一个电子商务应用程序，允许最终用户购买各种物品。这种工作量是我们业务的主要收入来源。
此工作负载的适用合规和/或监管要求以及事件发生 AWS 后需要采取的任何行动。	工作量涉及患者健康记录，这些记录必须安全保密。

工作负载入职问卷-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 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加快支持速度。	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 服务列表以及它们所在的 AWS 账户和区域。 Note 为每项服务创建一个新行。	路线 53：将互联网流量路由到 ALB。 账户：123456789101 区域：US-EAST-1、US-WEST-2
此工作负载使用的 AWS 服务列表以及它们所在的 AWS 账户和区域。 Note 为每项服务创建一个新行。	ALB：将传入流量路由到目标组 ECS 容器。 账户：123456789101 地区：不适用
此工作负载使用的 AWS 服务列表以及它们所在的 AWS 账户和区域。 Note 为每项服务创建一个新行。	ECS：主业务逻辑队列的计算基础架构。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 服务列表以及它们所在的 AWS 账户和区域。 Note 为每项服务创建一个新行。	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 服务列表以及它们所在的 AWS 账户和区域。 Note 为每项服务创建一个新行。	S3：存储网站静态资产。 账户：123456789101 地区：不适用
详细说明任何未上线/下游组件，这些组件在出现中断时可能会影响此工作负载。	身份验证微服务：将阻止用户加载健康记录，因为他们将未经身份验证。
是否有适用于此工作负载的本地或非AWS 组件？ 如果是，它们是什么，执行了哪些功能？	所有基于互联网的流量进出 AWS 均通过我们的本地代理服务进行路由。
提供可用区和区域级别的任何手动或自动故障转移/灾难恢复计划的详细信息。	热待机。成功率持续下降期间自动故障转移到 US-WEST-2。

工作负载入职调查表- AWS 服务事件问题

AWS 服务活动问题

问题	响应示例
提供联系方式（name/email/phone) of your company's internal major incident/IT危机管理小组。	重大事件管理小组 mim@example.com +61 2 3456 7890
提供贵公司建立的任何静态事件/危机管理桥梁的详细信息。如果您使用非静态网桥，请指定您的首选应用程序，并 AWS 将在事件发生期间请求这些详细信息。	Amazon Chime https://chime.aws/1234567890

问题	响应示例
Note 如果没有提供，则 AWS 会在事件发生时伸出援手，并提供一座 Chime 桥供你加入。	

警报摄取问卷

运行手册问题

问题	响应示例
AWS 将通过 支持 案例与工作负荷联系人接触。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，并 AWS 将在事件发生期间请求这些详细信息。 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 桥接器供您加入。	应用小组 app@example.com +61 2 3456 7890
如果事件发生期间主要联系人不可用，请按首选的沟通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： 约翰·史密斯-应用主管 john.smith@example.com +61 2 3456 7890 2. 10 分钟后，如果约翰·史密斯没有回复，请联系：

问题	响应示例
	简·史密斯——运营经理 jane.smith@example.com +61 2 3456 7890
AWS 在整个事件中，定期通过支持案例传达最新信息。还有其他联系人应该收到这些更新吗？	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，这些警报将使用 AWS 事件检测和响应来代表您的工作负载创建事件。AWS 事件检测与响应部的工程师查看您的警报后，将提供额外的入门步骤。

AWS 事件检测和响应关键警报标准：

- AWS 事件检测和响应警报应仅在监控工作负载受到重大业务影响（收入损失/客户体验降低）且需要操作员立即注意时才会进入 “警报” 状态。
- AWS 事件检测和响应警报还必须同时或在参与之前与您的处理人员联系以处理工作负载。 AWS 事件经理在缓解过程中与您的解决者合作，而不是充当第一线响应者，然后再上报给您。
- AWS 事件检测和响应警报阈值必须设置为适当的阈值和持续时间，这样每当警报触发时，都必须进行调查。如果警报在 “警报” 和 “正常” 状态之间移动，则产生的冲击力足以引起操作员的响应和注意。

针对@@ 违反标准的 AWS 事件检测和响应政策：

这些标准只能在事件发生时进行评估。 case-by-case如果怀疑客户警报不符合此标准，并且不必要地定期与事件管理团队接触，则事件管理团队会与您的技术客户经理（TAMs）合作调整警报，并在极少数情况下禁用监控。

> **Important**
>
> 在提供联系人地址时提供群组通讯电子邮件地址，这样您就可以在不更新运行手册的情况下控制收件人的添加和删除。
> 如果您希望 AWS 事件检测和响应团队在发送初始参与电子邮件后给他们打电话，请提供您的站点可靠性工程 (SRE) 团队的联系电话。

警报矩阵表

指标名称/ARN/阈值	描述	备注	请求的操作
工作负载量/ *CW Alarm ARN* / CallCount 在 5 分钟内获得 5 个数据点 < 100000，将缺失的数据视为丢失	该指标表示进入工作负载的传入请求数，在 Application Load Balancer 级别进行衡量。 此警报很重要，因为传入请求的大量下降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。	警报在上周已进入 “警报” 状态 10 次。此警报存在误报的风险。已计划进行阈值审查。 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，此警报会频繁翻转。 解析人员：现场可靠性工程师	向以下地址发送电子邮件，与现场可靠性工程团队接触 *SRE@xyz.com* 为我们的 ELB 和 Route 53 服务创建 AWS Premimum Support 案例。 如果需要立即采取行动：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知*XYZ*团队重启实例，或者运行日志刷新。（如果不需要立即采取行动，请留空）
工作负载请求延迟/ *CW Alarm ARN* / p90 5 分钟内 5 个数据点的延迟 > 100 毫秒，将丢失的数据视为丢失	该指标表示工作负载要完成 HTTP 请求的 p90 延迟。 此警报代表延迟（衡量网站客户体验的重要指标）。	上周，警报已进入 “警报” 状态 0 次。 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，此警报会频繁翻转。 解析人员：现场可靠性工程师	向以下地址发送电子邮件，与现场可靠性工程团队接触 *SRE@xyz.com* 为我们的 ECW 和 RDS 服务创建 AWS Premimum Support 案例。 如果需要立即采取行动：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知*XYZ*团队重启实例，或者运行日志刷新。（如果不

指标名称/ARN/阈值	描述	备注	请求的操作
			需要立即采取行动，请留空）
工作负载请求可用性/ *CW Alarm ARN* / 5 分钟内 5 个数据点的可用性小于 95%，将缺失的数据视为丢失。	此指标表示工作负载可以满足 HTTP 请求的可用性。（每期 HTTP 200 的请求数/# 个请求）。 此警报表示工作负载的可用性。	上周，警报已进入 “警报” 状态 0 次。 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，此警报会频繁翻转。 解析人员：现场可靠性工程师	向以下地址发送电子邮件，与现场可靠性工程团队接触 *SRE@xyz.com* 为我们的 ELB 和 Route 53 服务创建 AWS Premimum Support 案例。 如果需要立即采取行动：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知*XYZ*团队重启实例，或者运行日志刷新。（如果不需要立即采取行动，请留空）
新的遗物警报示例			

指标名称/ARN/阈值	描述	备注	请求的操作
端到端集成测试/ *CW Alarm ARN* / 在 3 分钟持续时间内，1 分钟指标的失败率为 3%，将缺失的数据视为丢失 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	该指标用于测试请求是否可以遍历工作负载的每一层。如果此测试失败，则表示无法处理业务交易。 此警报表示能够处理工作负载的业务交易。	上周，警报已进入“警报”状态 0 次。 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，此警报会频繁翻转。 解析人员：现场可靠性工程师	向以下地址发送电子邮件，与现场可靠性工程团队接触 *SRE@xyz.com* 为我们的 ECS 和 DynamoDB 服务创建 AWS Premimum Support 案例。 如果需要立即采取行动：检查 EC2 可用内存/磁盘空间，并通过电子邮件通知*XYZ*团队重启实例，或者运行日志刷新。（如果不需要立即采取行动，请留空）

事件检测和响应中的工作负载发现

AWS 与您合作，尽可能多地了解有关您的工作负载的背景信息。AWS 事件检测和响应使用这些信息来创建运行手册，以便在事件和 AWS 服务事件期间为您提供支持。所需信息在中捕获事件检测和响应中的工作负载入和警报摄取问卷。这是注册工作负载的最佳实践 AppRegistry。有关更多信息，请参阅 AppRegistry 《用户指南》。

主要产出：

- 工作负载信息，例如工作负载的描述、架构图、联系方式和上报详情。
- 每个 AWS 区域的工作负载如何使用 AWS 服务的详细信息。
- 有关在服务活动期间如何为您提供 AWS 支持的具体信息。
- 您的团队使用的警报，用于检测工作负载的严重影响。

为工作负载订阅事件检测和响应

要将工作负载订阅 AWS 事件检测和响应，请为每个工作负载创建一个新的支持案例。创建支持案例时，请记住以下几点：

- 要加载单个 AWS 账户中的工作负载，请从工作负载账户或付款人账户创建支持案例。
- 要加入跨多个 AWS 账户的工作负载，请使用您的付款人账户创建支持案例。在支持案例的正文中，列出所有 IDs 要加入的账户。

> **Important**
>
> 如果您创建支持案例以使用错误的帐户将工作负载订阅到 “事件检测和响应”，则在订阅工作负载之前，您可能会遇到延迟和要求提供更多信息的请求。

订阅工作负载

1. 转到 “AWS 支持 中心”，然后选择 “创建案例”，如下例所示。您只能通过注册了 Enterprise Support 的账户订阅工作负载。

2. 填写支持案例表：

   - 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 “载入新工作负载”。
   - 对于 “严重性”，选择 “一般指导”。

3. 输入此更改的主题。例如：

   [板载] AWS 事件检测和响应-*workload_name*

4. 输入此更改的描述。例如，输入 “此请求是将工作负载加载到 AWS 事件检测和响应”。请务必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。这些是您想要加入 AWS 事件检测和响应的账户。
   - 语言：英语或日语。
   - 订阅开始日期：您想要开始 AWS 事件检测和响应订阅的日期。

5. 在 “其他联系人-可选” 部分中，输入您 IDs 希望收到的有关此请求的信件的任何电子邮件。

   以下是 “其他联系人-可选” 部分的示例：

> **Important**
>
> 未能 IDs 在 “其他联系人-可选” 部分中添加电子邮件可能会延迟 AWS 事件检测和响应的入职流程。

6. 选择提交。

   提交请求后，您可以添加来自您的组织的其他电子邮件。要添加电子邮件，请回复问题，然后在 “其他联系人-可选” 部分 IDs 中添加电子邮件。

   以下是 “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，以继续工作负载入流程：

- AWS 工作负载架构图。
- 事件检测和响应中的工作负载入和警报摄取问卷：填写调查问卷中与你入职工作量有关的所有信息。如果您有多个工作负载需要加载，请为每个工作负载创建一个新的入职调查表。如果您对填写入职问卷有疑问，请联系您的技术客户经理 (TAM)。

> **Note**
>
> 请勿使用 “附加文件” 选项将这两份文件附加到案例中。AWS 事件检测和响应团队将通过亚马逊简单存储服务上传器链接回复问题，供您上传文档。

有关如何使用 AWS 事件检测和响应创建案例以请求更改现有已载入工作负载的信息，请参阅。在 “事件检测和响应” 中请求更改已载入的工作负载有关如何移除工作负载的信息，请参阅将工作负载从事件检测和响应中移除。

在 “事件检测和响应” 中定义和配置警报

AWS 与您合作定义指标和警报，以提供对应用程序及其底层 AWS 基础设施性能的可见性。我们要求警报在定义和配置阈值时遵守以下标准：

- 只有当监控的工作负载受到严重影响（收入损失或客户体验下降，从而显著降低性能），需要操作员立即注意时，警报才会进入 “警报” 状态。
- 警报还必须在与事件管理团队联系的同时或之前，与您指定的工作负载处理人员接触。事件管理工程师应在缓解过程中与您指定的解决人员合作，而不是充当第一线响应者，然后上报给您。
- 必须将警报阈值设置为适当的阈值和持续时间，这样每当警报触发时，都必须进行调查。如果警报在 “警报” 和 “正常” 状态之间摆动，则产生的冲击力足以引起操作员的响应和注意。

警报的类型：

- 可描述业务影响程度的警报，并传递相关信息，便于简单的故障检测。
- 亚马逊 CloudWatch 加那利群岛。有关更多信息，请参阅加那利群岛和 X-Ray 追踪以及 X- R ay。
- 聚合警报（监控依赖关系）

下表提供了所有使用 CloudWatch 监控系统的警报示例。

指标名称/警报阈值	警报 ARN 或资源 ID	如果此警报触发	如果参与其中，请为这些服务提出 Premium Support 案例
API 错误/ 10 个数据点的错误数 >= 10	arn: aws: cloudwatch: us-west-2:000000000000:alarm: e2 Lambda-Errors MPmim	数据库管理员 (DBA) 团队的门票	Lambda，API Gateway
ServiceUnavailable（Http 状态码 503）	arn: aws: cloudwatch: us-west-2: xxxxx: alarm: httperrorcode503	削减服务团队的门票	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	如果参与其中，请为这些服务提出 Premium Support 案例
在 5 分钟的时间内，10 个数据点（不同的客户端）的错误数 >=3			
ThrottlingException（Http 状态码 400） 在 5 分钟的时间内，10 个数据点（不同的客户端）的错误数 >=3	arn: aws: cloudwatch: us-west-2: xxxxx: alarm: httperrorcode400	削减服务团队的门票	EC2，亚马逊 Aurora

有关更多详细信息，请参阅 AWS 事件检测和响应监控和可观察性。

主要产出：

- 工作负载警报的定义和配置。
- 填写入职问卷上的警报详情。

主题

- 在 “事件检测和响应” 中创建符合您业务需求的 CloudWatch 警报
- 使用 CloudFormation 模板在 “事件检测和响应” 中生成 CloudWatch 警报
- 事件检测和响应中 CloudWatch 警报的示例用例

在 “事件检测和响应” 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您的警报最适合您的业务需求。

> **Note**
>
> 有关加入事件检测和响应的 AWS 服务 推荐 CloudWatch 警报示例，请参阅上的 “事件检测和响应警报最佳实践” AWS re:Post。

查看您建议的 CloudWatch 警报

查看您建议的警报，确保只有在监控的工作负载受到严重影响（收入损失或客户体验降级，从而显著降低性能）时，它们才会进入 “警报” 状态。例如，您是否认为此警报足够重要，以至于在它进入 “警报” 状态时必须立即做出反应？

以下是可能代表关键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 Application Load Balancer 后面或其他资源后面的目标的响应。这样可以更轻松地识别 5XX 错误的来源。有关更多信息，请参阅 App lication Load Balancer 的 CloudWatch 指标。
- Amazon API Gateway：如果你在 Elastic Beanstalk 中使用 WebSocket API，那么可以考虑使用以下指标：
  - 集成错误率（筛选为 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 执行情况。
- 亚马逊 Route 53：监控EndPointUnhealthyENICount指标。该指标是处于自动恢复状态的弹性网络接口的数量。此状态表示解析器尝试恢复与终端节点（由指定 EndpointId）关联的一个或多个 Amazon Virtual Private Cloud 网络接口。在恢复过程中，端点在容量有限的情况下运行。在完全恢复之前，终端节点无法处理 DNS 查询。有关更多信息，请参阅使用 Amazon CloudWatch 监控 Route 53 Resolver 终端节点。

验证您的警报配置

确认建议的警报符合您的业务需求后，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 秒内对数据点进行轮询有助于及早发现事件。
- 验证DatapointToAlarm配置。在大多数情况下，最佳做法是将其设置为三分之三或五分之五。在事件中，如果设置为 [60 秒指标，3 分中的 3 个 DatapointToAlarm]，则警报在 3 分钟后触发；如果设置为 [60 秒指标，5 分中的 5 个 DatapointToAlarm]，则警报会在 5 分钟后触发。使用这种组合可以消除嘈杂的警报。

> **Note**
>
> 根据您使用服务的方式，上述建议可能会有所不同。每项 AWS 服务在工作负载中的运行方式都不同。而且，在多个地方使用相同的服务时，操作方式可能会有所不同。您必须确保了解您的工作负载是如何利用发出警报的资源的，以及上游和下游的影响。

验证您的警报如何处理丢失的数据

某些指标源不会定期向其 CloudWatch 发送数据。对于这些指标，最佳做法是将缺失的数据视为 NotBre aching。有关更多信息，请参阅配置 CloudWatch 警报如何处理丢失的数据和避免过早过渡到警报状态。

例如，如果某个指标监控错误率，并且没有错误，则该指标不报告任何数据（零）数据点。如果您将警报配置为将丢失的数据视为缺失，则单个数据点泄露后跟两个无数据（零）数据点会导致该指标进入 “警报” 状态（3 个数据点中的 3 个）。这是因为缺失的数据配置会评估评估周期内最后一个已知的数据点。

在指标监控错误率的情况下，在没有服务降级的情况下，你可以假设没有数据是一件好事。最佳做法是将丢失的数据视为 NotBre aching，这样丢失的数据就会被视为 “正常”，并且指标不会在单个数据点上进入 “警报” 状态。

查看每个警报的历史记录

如果警报的历史记录显示它经常进入 “警报” 状态然后快速恢复，那么警报可能会成为你的问题。确保调整警报以防止出现噪音或误报。

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基础数据。这可能会导致警报进入 “警报” 状态。

创建复合警报

如果您为事件检测和响应操作提供了大量警报以供入职，则可能会要求您创建复合警报。复合警报减少了需要加载的警报总数。

使用 CloudFormation 模板在 “事件检测和响应” 中生成 CloudWatch 警报

为了加快 AWS 事件检测和响应的入门速度，并减少构建警报所需的工作量， AWS 我们为您提供了 AWS CloudFormation 模板。这些模板包括针对常用载服务（例如应用程序负载均衡器、网络负载均衡器和亚马逊）的优化警报设置。 CloudFront

使用 CloudFormation 模板生成 CloudWatch 警报

1. 使用提供的链接下载模板：

NameSpac	Metrics	Compariso nOperator （阈值）	周期	Datapoint sToAlarm	TreatMiss ingData	Statistic	模板链接
应用程序弹性负载均衡器	(m1+m2)/(m1+m2+m m4) *100 m1= _target_2 xx_Count m2= _target_3 xx_count m3= _target_4 xx_count m4= _target_5	LessThanT hreshold(95)	60	三分之三	缺失的	总和	模板

NameSpac	Metrics	Compariso nOperator （阈值）	周期	Datapoint sToAlarm	TreatMiss ingData	Statistic	模板链接
	xx_count HTTPCode HTTPCode HTTPCode HTTPCode						
Amazon CloudFron t	TotalErro rRate	GreaterTh anThresho ld(5)	60	三分之三	不违反	平均值	模板
应用程序弹性负载均衡器	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	三分之三	不违反	最大值	模板
Network Elastic Load	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	三分之三	不违反	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. 创建堆 CloudFormation 栈：

> **Note**
>
> 以下步骤使用标准 CloudFormation 堆栈创建流程。有关详细步骤，请参阅在 AWS CloudFormation 控制台上创建堆栈。

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

b. 选择创建堆栈。

c. 选择 “模板已准备就绪”，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：输入闹钟的名称和描述。
- ThresholdConfig：修改阈值以满足应用程序的要求。
- 分发 IDConfig：确保分配 ID 指向您创建 AWS CloudFormation 堆栈的账户中的正确资源。

f. 选择下一步。

g. 查看PeriodConfigEvalutionPeriodConfig、和DatapointsToAlarmConfig字段中的默认值。最佳做法是使用这些字段的默认值。如果需要，您可以进行调整以满足应用程序的要求。

h. （可选）根据需要输入标签和 SNS 通知信息。最佳做法是打开 “终止保护”，以防止警报被意外删除。要打开终止保护，请选择 “已激活” 单选按钮，如以下示例所示：

i. 选择下一步。

j. 查看您的堆栈设置，然后选择创建堆栈。

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

4. 在正确的账户和 AWS 地区创建所有警报后，请通知您的技术客户经理 (TAM)。AWS 事件检测和响应团队会审核您的新警报的状态，然后继续上线。

事件检测和响应中 CloudWatch 警报的示例用例

以下用例提供了如何在事件检测和响应中使用 Amazon CloudWatch 警报的示例。这些示例演示了如何配置 CloudWatch 警报以监控各种 AWS 服务的关键指标和阈值，从而使您能够识别和应对可能影响应用程序和工作负载可用性和性能的潜在问题。

示例用例 A：Application Load Balancer

您可以创建以下 CloudWatch 警报，表示工作负载可能受到影响。为此，您需要创建一个公制数学，当成功连接降至特定阈值以下时，会发出警报。有关可用 CloudWatch 指标，请参阅 App lication Load Balancer 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

NameSpace: AWS/applicat ionelB

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

周期：60 秒

DatapointsToAlarm: 三分之三

缺失数据处理：将丢失的数据视为数据泄露。

统计数据：Sum

下图显示了用例 A 的流程：

示例用例 B：亚马逊 API Gateway

您可以创建以下 CloudWatch 警报，表示工作负载可能受到影响。为此，您需要创建一个复合指标，该指标在 API Gateway 中存在高延迟或平均数 4XX 错误时发出警报。有关可用指标，请参阅 Amazon API Gateway 的维度和指标

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

NameSpace: AWS/API 网关

ComparisonOperator（阈值）：大于（x 或 y 个客户的阈值）

周期：60 秒

DatapointsToAlarm: 1 分中的 1

缺失数据处理：将缺失的数据视为未泄露。

统计数据：

下图显示了用例 B 的流程：

示例用例 C：亚马逊 Route 53

您可以通过创建 Route 53 运行状况检查 CloudWatch 来监控您的资源，这些检查用于收集原始数据并将其处理为可读的近乎实时的指标。您可以创建以下 CloudWatch 警报，表示工作负载可能受到影响。您可以使用这些 CloudWatch 指标创建警报，当警报超过既定阈值时触发。有关可用 CloudWatch 指标，请参阅 Route 53 运行状况检查的CloudWatch 指标

指标：R53-HC-Success

NameSpace: AWS/Route 53

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

时长：1 分钟

DatapointsToAlarm: 三分之三

缺失数据处理：将丢失的数据视为数据泄露。

统计数据：Minimum

下图显示了用例 C 的流程：

示例用例 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已打开，则说明您尚未验证该应用程序是否正在运行。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数据库和亚马逊简单存储服务 (Amazon S3) Service，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 /mon itor。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，您将负载均衡器上的运行状况检查指向 /monitor 页面。

下图显示了用例 D 的流程：

将警报引入 AWS 事件检测和响应

AWS 事件检测和响应支持通过 Amazon 接收警报。 EventBridge本节介绍如何将 AWS 事件检测和响应与不同的应用程序性能监控 (APM) 工具（包括亚马逊）集成 CloudWatch， APMs 与亚马逊 EventBridge （例如 Datadog 和 New Relic）直接集成， APMs 无需与亚马逊直接集成。 EventBridge 有关直接集成到亚马逊 APMs 的完整列表 EventBridge，请参阅亚马逊 EventBridge集成。

主题

配置对事件检测和响应的警报获取访问权限

要允许 AWS 事件检测和响应从您的账户获取警报，请安装`AWSServiceRoleForHealth_EventProcessor`服务相关角色 (SLR)。 AWS 假设 SLR 创建了 Amazon EventBridge 托管的规则。托管规则会将通知从您的账户发送到 AWS 事件检测和响应。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，您可以使用以下 AWS 命令行界面 (AWS CLI) Line CLI 命令：

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

关键产出

- 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：

- 在 AWS Health 中使用服务相关角色
- 创建服务相关角色
- AWS 托管策略： AWSHealth_EventProcessorServiceRolePolicy

将事件检测和响应与 Amazon 集成 CloudWatch

AWS 事件检测和响应使用您在访问权限配置期间开启的服务相关角色 (SLR) 在名为的账户 AWS 中创建亚马逊 EventBridge托管规则。`AWSHealthEventProcessor-DO-NOT-DELETE`事件检测和响应使

用此规则从您的账户中提取Amazon CloudWatch 警报。无需执行其他步骤即可从中 CloudWatch获取警报。

从与 Amazon 直接集成的警报中 APMs 提取警报 EventBridge

下图显示了通过与亚马逊 EventBridge直接集成的应用程序性能监控 (APM) 工具（例如 Datadog 和 Splunk）向 AWS 事件检测和响应发送通知的过程。有关与之直接集成的完整列表 APMs EventBridge，请参阅 Amazon EventBridge 集成。

使用以下步骤设置与 AWS 事件检测和响应的集成。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 事件检测和响应的集成

您必须为每个 AWS 账户和 AWS 地区完成以下步骤。警报必须来自应用程序资源所在的 AWS 账户和 AWS 区域。

1. 将您的每个事件源设置 APMs 为 Amazon EventBridge 合作伙伴（例如`aws.partner/my_apm/integrationName`）。有关将 APM 设置为事件源的指南，请参阅通过 A mazon EventBridge 接收来自 SaaS 合作伙伴的事件。这将在您的账户中创建合作伙伴活动总线。
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 事件检测和响应通过 `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 事件检测和响应。该规则与获取第三方 APM 事件的模式相匹配。
   - （替代方法）使用默认事件总线而不是自定义事件总线。默认事件总线要求托管规则向 AWS 事件检测和响应发送 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相匹配`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`。
   a. 转换后的事件包括唯一的 AWS 事件检测和响应标识符，并将事件的来源和详细信息类型设置为所需的值。该模式与托管规则相匹配。
   b. 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（推荐方法）或您的默认事件总线。
4. 创建 EventBridge 规则并定义与您要推送到 AWS 事件检测和响应的事件列表相匹配的事件模式。规则的来源是您在步骤 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 事件检测和响应的示例，请参阅示例：整合来自 Datadog 和 Splunk 的通知。

示例：整合来自 Datadog 和 Splunk 的通知

此示例提供了将来自 Datadog 和 Splunk 的通知集成到 AWS 事件检测和响应的详细步骤。

主题

第 1 步：在 Amazon 中将您的 APM 设置为事件源 EventBridge

在您的 AWS 账户中 APMs ，将您的每一个都设置为 Amazon EventBridge 中的事件源。有关将 APM 设置为事件源的说明，请参阅 A mazon EventBridge 合作伙伴中针对您的工具的事件源设置说明。

通过将您的 APM 设置为事件源，您可以将来自 APM 的通知提取到您的 AWS 账户中的事件总线。设置完成后，AWS 事件检测和响应可在事件总线收到事件时启动事件管理流程。此过程会将亚马逊添加 EventBridge 为您的 APM 中的目的地。

步骤 2：创建自定义事件总线

使用自定义事件总线是最佳实践。AWS 事件检测和响应使用自定义事件总线来摄取转换后的事件。AWS Lambda 函数转换伙伴事件总线事件并将其发送到自定义事件总线。AWS 事件检测和响应会安装托管规则，用于从自定义事件总线提取事件。

您可以使用默认事件总线代替自定义事件总线。AWS 事件检测和响应修改托管规则，使其从默认事件总线而不是自定义事件总线中提取。

在您的 AWS 账户中创建自定义事件总线：

1. 打开 Amazon EventBridge 控制台，网址为 https://console.aws.amazon.com/events/

2. 选择 “巴士”、“活动总线”。
3. 在 “自定义事件总线” 下，选择 “创建”。
4. 在 “名称” 下为您的活动巴士提供一个名称。推荐的格式为 APMName-AWSIncidentDetectionResponse-EventBus。

   例如，如果您使用 Datadog 或 Splunk，请使用以下方法之一：

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

步骤 3：创建用于转换的 AWS Lambda 函数

Lambda 函数在步骤 1 中的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 函数转换与 AWS 事件检测和响应托管规则相匹配。

在您的 AWS 账户中创建 AWS Lambda 函数

1. 在 AWS Lambda 控制台上打开 “函数” 页面。
2. 选择创建函数。
3. 选择 “从头开始作者” 选项卡。
4. 在函数名称中，使用格式输入名称`APMName-AWSIncidentDetectionResponse-LambdaFunction`。

   以下是 Datadog 和 Splunk 的示例：

   - Datadog： Datadog-AWSIncidentDetectionResponse-LambdaFunction
   - Splunk： Splunk-AWSIncidentDetectionResponse-LambdaFunction
5. 对于运行时，输入 Python 3.10。
6. 将其余字段保留为默认值。选择创建函数。
7. 在代码编辑页面上，将默认 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. 为要将转换后的数据发送到的事件总线的 Lambda 执行角色添加PutEvents权限：
   a. 在 AWS Lambda 控制台上打开 “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，选择添加新声明：

g. 策略编辑器添加了一个新的空白语句，类似于以下内容

h. 将新的自动生成的语句替换为以下语句：

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

i. 资源是您在中创建的自定义事件总线的 ARN，步骤 2：创建自定义事件总线或者如果您在 Lambda 代码中使用默认事件总线，则为默认事件总线的 ARN。

10. 查看并确认所需的权限已添加到角色中。

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 事件检测和响应提取的事件总线事件中需要以下 JSON 密钥:值对。

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

以下示例显示了转换前后来自合作伙伴事件总线的事件。

```
{
    "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表示警报来自哪个 APM，来源来自合作伙伴 APM，incident-detection-response-identifier密钥不存在。

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。转换后的有效载荷现在包括所需的键: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，现在detail-type是 sourceams.monitoring/generic-apm，现在是 sourceGenericAPMEvent，详细信息下有新的 key: value pair:。incident-detection-response-identifier

在前面的示例中，该incident-detection-response-identifier值取自路径下的警报名称$.detail.meta.monitor.name。APM 警报名称路径从一个 APM 到另一个 APM 不同。必须修改 Lambda 函数，才能从正确的合作伙伴事件 JSON 路径中获取警报名称并将其用作值。incident-detection-response-identifier

上设置的每个唯一名称都会在`incident-detection-response-identifier`入职期间提供给 AWS 事件检测和响应团队。不处理名称未知的事件。`incident-detection-response-identifier`

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. 打开 Amazon EventBridge 控制台，网址为 https://console.aws.amazon.com/events/
2. 选择规则，然后选择与您的 APM 关联的合作伙伴事件总线。以下是合作伙伴活动总线的示例：
   - Datadog：aws。 partner/datadog.com/eventbus-名字
   - Splunk：aws。 partner/signalfx.com/RandomString
3. 选择 “创建规则” 以创建新 EventBridge 规则。
4. 在规则名称中，输入以下格式的名称`APMName-AWS Incident Detection and Response-EventBridgeRule`，然后选择下一步。以下是示例名称：
   - Datadog： Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk： Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. 对于事件来源，选择 AWS 事件或 EventBridge 合作伙伴活动。
6. 将示例事件和创建方法保留为默认值。
7. 对于事件模式，请选择以下选项：
   a. 事件来源： 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。

   以下是事件模式示例：

   Datadog 事件模式示例

   Splunk 事件模式示例

8. 对于“目标”，请选择以下选项：
    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 从中获取警报， APMs 无需直接与 Amazon 集成 EventBridge

AWS 事件检测和响应支持使用 webhook 从未与 Amazon 直接集 APMs 成的第三方获取警报。EventBridge

有关 APMs 与亚马逊直接集成的列表 EventBridge，请参阅亚马逊 EventBridge 集成。

使用以下步骤设置与 AWS 事件检测和响应的集成。在执行这些步骤之前，请验证您的账户中是否安装了 AWS 托管规则 AWSHealthEventProcessorEventSource-DO-NOT-DELETE

使用 webhook 采集事件

1. 定义 Amazon API Gateway 以接受来自您的 APM 的有效负载。
2. 使用身份验证令牌定义授权 AWS Lambda 函数，如上图所示。
3. 定义第二个 Lambda 函数来转换并将 AWS 事件检测和响应标识符附加到您的有效负载。您还可以使用此功能筛选要发送到 AWS 事件检测和响应的事件。
4. 设置您的 APM 以向从 API Gateway 生成的网址发送通知。

在 “事件检测和响应” 中管理工作负载

有效的事件管理的一个关键部分是制定正确的流程和程序，以载入、测试和维护受监控的工作负载。本节涵盖了基本步骤，包括制定全面的运行手册和响应计划以指导您的团队应对突发事件，在入职前对新工作负载进行全面测试和验证，请求更改以更新工作负载监控，以及在需要时适当移除工作负载。

主题

在 “事件检测和响应” 中制定应对事件的运行手册和响应计划

事件检测和响应使用从入职调查问卷中获取的信息来制定操作手册和响应计划，以管理影响工作负载的事件。运行手册记录了事件管理者在应对事件时采取的步骤。响应计划会映射到您的至少一个工作负载。事件管理团队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，请参阅事件管理器是什么 AWS Systems Manager Incident Manager？

主要产出：

- 完成您对 AWS 事件检测和响应的工作负载定义。
- 完成 AWS 事件检测和响应方面的警报、操作手册和响应计划定义。

您也可以下载 AWS 事件检测和响应运行手册示例：aws-idr-runbook-example. zip。

运行手册示例：

```
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.
```

在“事件检测和响应”中测试已加载的工作负载

> **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。

入职流程的最后一步是为你的新工作量执行一个游戏日。警报提取完成后，AWS 事件检测和响应会确认您选择的开始比赛日的日期和时间。

你的比赛日有两个主要目的：

- 功能验证：确认 AWS 事件检测和响应可以正确接收您的警报事件。而且，功能验证可确认您的警报事件是否触发了相应的 runbook 和任何其他所需的操作，例如，如果您在警报摄取期间选择了自动创建案例。
- 模拟：游戏日是对真实事件中可能发生的事情的端到端模拟。AWS 事件检测和响应遵循您规定的运行手册步骤，让您深入了解真实事件可能如何发展。比赛日是你提出问题或完善说明以提高参与度的机会。

在警报测试期间，AWS 事件检测和响应会与您合作，修复发现的任何问题。

CloudWatch 警报

AWS 事件检测和响应通过监控 CloudWatch 警报的状态变化来测试您的 Amazon 警报。为此，请使用手动将警报更改为“警报”状态 AWS Command Line Interface。您也可以访问 AWS CLI 表单 AWS CloudShell。AWS 事件检测和响应为您提供了一个 AWS CLI 命令列表，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
```

要了解有关手动更改 CloudWatch 警报状态的更多信息，请参阅SetAlarmState。

要详细了解 CloudWatch API 操作所需的权限，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令来模拟警报。在比赛日开始时，AWS 事件检测和响应请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 事件检测和响应的有效负载。

关键产出

主要产出：

- 已成功接收警报，并且您的警报配置正确。
- AWS 事件检测和响应成功创建并接收警报。
- 系统会为您的项目创建支持案例，并通知您指定的联系人。
- AWS 事件检测和响应可以通过您规定的会议方式与您接触。
- 游戏日生成的所有警报和支持案例均已解决。
- 系统会发送一封上线电子邮件，确认您的工作负载正由 AWS 事件检测和响应监控。

在“事件检测和响应”中请求更改已载入的工作负载

要请求更改已载入的工作负载，请完成以下步骤，使用 AWS 事件检测和响应创建支持案例。

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. 输入此更改的主题。例如：

   AWS 事件检测和响应-*workload_name*
7. 输入此更改的描述。例如，输入“此请求用于更改 AWS 事件检测和响应中已加载的现有工作负载”。请务必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。

- 变更详情：输入您申请的变更详情。

8. 在 “其他联系人-可选” 部分中，输入您 IDs 希望收到的有关此更改的信件的任何电子邮件。

   以下是 “其他联系人-可选” 部分的示例。

   > **Important**
   >
   > 未能 IDs 在 “其他联系人-可选” 部分中添加电子邮件可能会延迟更改过程。

9. 选择提交。

   提交变更请求后，您可以添加来自您的组织的其他电子邮件。要添加电子邮件，请选择 “在问题详情中回复”，如下例所示：

   然后， IDs 在 “其他联系人-可选” 部分中添加电子邮件。

   以下是 “回复” 页面的示例，显示了您可以在其中输入其他电子邮件。

抑制警报，使其无法使用事件检测和响应

通过暂时或按计划禁用已载入的工作负载警报，指定哪些警报与 AWS 事件检测和响应监控相关。例如，在计划内维护期间，您可以暂时取消工作负载警报，以防止警报进入事件检测和响应。或者，如果您每天都有重启活动，则可以按计划取消警报。您可以抑制警报源（例如 Amazon）的警报 CloudWatch，也可以提交工作负载更改请求。

主题

抑制警报源的警报

通过抑制警报源的警报，指定哪些警报与事件检测和响应交互以及何时与之交互。

主题

使用公制数学函数抑制 CloudWatch 警报

要禁止对 Amazon CloudWatch 警报进行事件检测和响应监控，请使用指标数学函数阻止 CloudWatch 警报在指定时段内进入ALARM状态。

> **Note**
>
> 在警报上禁用 CloudWatch 警报操作不会抑制事件检测和响应对警报的监控。警报状态更改是通过 Amazon EventBridge 而不是通过 CloudWatch 警报操作获取的。

要使用指标数学函数抑制 CloudWatch 警报，请完成以下步骤：

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择 Alarms，然后找到要向其添加指标数学函数的警报。
3. 在量度数学部分中，选择编辑。
4. 选择添加数学，从空表达式开始。
5. 输入您的数学表达式，然后选择 “应用”。
6. 取消选择警报监控的现有指标。
7. 选择您刚刚创建的表达式，然后选择选择指标。
8. 选择 “跳至预览并创建”。
9. 查看您的更改以确保您的指标数学函数按预期应用，然后选择更新警报。

有关使用公制数学函数抑制 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 用户指南中的公制数学语法和函数。

移除指标数学函数以取消抑制警报 CloudWatch

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

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择 Alarms，然后找到要从中删除指标数学表达式的一个或多个警报。
3. 在量度数学部分中，选择编辑。
4. 要从警报中删除该指标，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 “跳至预览并创建”。
7. 查看您的更改以确保您的指标数学函数按预期应用，然后选择更新警报。

指标数学函数和相关用例示例

下表包含公制数学函数示例，以及相关的用例和对每个指标组成部分的解释。

公制数学函数	应用场景	说明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	在此时段内，将实际数据点替换为 0，从而抑制每周二世界标准时间凌晨 1:00 至 3:00 之间的警报。	• 日 (m1) == 2：确保是星期二（星期一 = 1，星期日 = 7）。 • 小时 (m1) >= 1 && HOUR (m1) > 3：指定从世界标准时间上午 1 点到凌晨 3 点的时间范围。 • I@@ F（条件，valu e_if_true，value_if_false：如果条件为真，则将指标值替换为 0。否则，返回原始值 (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	在此时段内，将实际数据点替换为 0，从而抑制每天晚上	• 小时 (m1) >= 23：捕捉从世界标准时间 23:00 开始的时间。

公制数学函数	应用场景	说明
	11:00 至凌晨 4:00 之间的警报。	• 小时 (m1) < 4：捕获截至（但不包括）UTC 04:00 的时间。 • ||：Logical OR 可确保条件适用于两个范围——深夜和清晨。 • I@@ F（条件，value_if_true，value_if_false）：在指定时间范围内返回 0。保留该范围之外的原始指标值 m1。
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	在此时段内，将实际数据点替换为 0，从而抑制世界标准时间每天上午 11:00 至下午 1:00 之间的警报。	• 小时 (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（条件，value_if_true，value_if_false）：如果条件为真（例如，时间介于世界标准时间 11:00 到 13:00 之间），则返回 0，如果条件为假，则保留原始指标值 (m1)。

公制数学函数	应用场景	说明
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	在此时段内，将实际数据点替换为 99，从而抑制每周二世界标准时间凌晨 1:00 至凌晨 3:00 之间的警报。	• 日 (m1) == 2:: 确保是星期二（星期一 = 1，星期日 = 7）。 • 小时 (m1) >= 1 && HOUR (m1) < 3：指定从世界标准时间上午 1 点到凌晨 3 点的时间范围。 • I@@ F（条件，valu e_if_true，value_if _false）：如果条件为真，则将指标值替换为 99。否则，返回原始值 (m1)。
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	在此时段内，每天将真实数据点替换为 100，从而抑制世界标准时间下午 11:00 至凌晨 4:00 之间的警报。	• 小时 (m1) >= 23：捕捉从世界标准时间 23:00 开始的时间。 • 小时 (m1) < 4：捕获截至（但不包括）UTC 04:00 的时间。 • ||：Logical OR 可确保条件适用于两个范围——深夜和清晨。 • I@@ F（条件，valu e_if_true，value_if _false）：在指定时间范围内返回 100。保留该范围之外的原始指标值 m1。

公制数学函数	应用场景	说明
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	在此时间段内，将实际数据点替换为 99，从而抑制世界标准时间每天上午 11:00 至下午 1:00 之间的警报。	• 小时 (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（条件，value_if_true，value_if_false）：如果条件为真（例如，时间介于世界标准时间 11:00 到 13:00 之间），则返回 99。如果条件为假，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

提交工作负载变更请求以抑制警报

如果您无法按照上一节所述在源头抑制警报，请提交工作负载更改请求，指示事件检测和响应手动禁止对工作负载的部分或全部警报的监控。

有关如何创建工作负载变更请求的详细说明，请参阅事件检测和响应中的请求更改已载入的工作负载。在提出工作负载变更请求以请求取消警报时，请务必提供以下必填信息

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

创建警报抑制工作负载变更请求后，您将收到来自事件检测和响应的以下通知：

- 确认您的工作负载变更请求。
- 警报被抑制时发出通知。
- 重新启用警报以进行监控时发出通知。

教程：使用指标数学函数抑制警报

以下教程将向您介绍如何使用公制数学来抑制 CloudWatch 警报。

示例方案

计划在即将到来的星期二世界标准时间凌晨 1:00 到 3:00 之间进行活动。您想要创建一个 CloudWatch 公制数学函数，该函数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条件的示例：

   前面的屏幕截图中显示的警报监控 Appl UnHealthyHostCount ication Load Balancer 目标组的指标。当 5 个数据点中有 5 个的UnHealthyHostCount指标大于或等于 3 时，此警报进入ALARM状态。警报将丢失的数据视为不良数据（超过配置的阈值）。
2. 创建指标数学函数。

   在此示例中，计划的活动发生在即将到来的星期二世界标准时间凌晨 1:00 到 3:00 之间。因此，创建一个 CloudWatch 公制数学函数，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，您必须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真实数据点替换为高于配置阈值 100 的值。以下是该场景的指标数学函数示例。

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

   前面的公制数学函数包含以下元素：

   - 日 (m1) == 2：确保现在是星期二（星期一 = 1，星期日 = 7）。
   - 小时 (m1) >= 1 && HOUR (m1) < 3：指定从世界标准时间上午 1 点到凌晨 3 点的时间范围。
   - I@@ F（条件，value_if_true，value_if_false）：如果条件为真，则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 Management Console 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
4. 选择 Alarms，然后找到要向其添加指标数学函数的警报。
5. 在量度数学部分中，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，以帮助其他人了解其功能及其创建原因，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，而不是直接监控基础指标。
10. 选择 “跳至预览并创建”。
11. 验证警报是否按预期配置，然后选择更新警报以保存更改。

在前面的示例中，如果不应用度量数学函数，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`状态并启动 “事件检测和响应”，如以下示例所示：

使用指标数学函数后，在活动期间将实际数据点替换为 0，警报保持`OK`状态，从而抑制事件检测和响应参与。

教程：移除指标数学函数以取消抑制警报

如果您取消了针对一次性活动的 CloudWatch 警报，请在活动完成后从警报中移除指标数学函数，以恢复对警报的定期监控。例如，要定期抑制警报，如果您计划每周修补例程，导致实例每周在同一天和同一时间重启，则保留指标数学函数。

以下教程将向您介绍如何移除指标数学函数以取消隐藏警报 CloudWatch

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。

2. 选择 Alarms，然后找到要向其添加指标数学函数的警报。
3. 在量度数学部分中，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. 选择指标以恢复对真实指标的监控。然后选择选择指标。
6. 选择 “跳至预览并创建”。
7. 验证警报是否按预期配置，然后选择更新警报以保存更改。

将工作负载从事件检测和响应中移除

要将工作负载从 AWS 事件检测和响应中移除，请为每个工作负载创建一个新的支持案例。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，请从工作负载账户或付款人账户创建支持案例。
- 要移除跨越多个 AWS 账户的工作量，请使用您的付款人账户创建支持案例。在支持案例的正文中，列出所有 IDs 要退出的账户。

> **Important**
>
> 如果您创建支持案例是为了将工作负载从错误的帐户中移除，则在卸载工作负载之前，您可能会遇到延迟和要求提供更多信息的请求。

请求移除工作负载

1. 转到 “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 “工作负载离职”。
5. 对于 “严重性”，选择 “一般指导”。
6. 输入此更改的主题。例如：

   [Offboard] AWS 事件检测和响应-*workload_name*

7. 输入此更改的描述。例如，输入 “此请求用于卸载到 AWS 事件检测和响应中的现有工作负载”。请务必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。
   - 离职原因：提供卸载工作负载的理由。
8. 在 “其他联系人-可选” 部分中，输入您 IDs 希望收到的有关此离职申请的信件的任何电子邮件。
9. 选择提交。

AWS 事件检测和响应监控和可观察性

AWS 事件检测和响应为您提供专家指导，帮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察性。监控会告诉你出了点问题。Observability 使用数据收集来告诉你出了什么问题以及问题发生的原因。

事件检测和响应系统通过利用 Amazon 和 Amazon 等原生 AWS 服务来检测可能影响您的 AWS 工作负载的事件， EventBridge 从而监控您的工作负载是否存在故障 CloudWatch 和性能下降。监控为您提供即将发生的、正在进行的、即将出现的故障或潜在的故障或性能下降的通知。当您将账户注册到 “事件检测和响应” 时，您可以选择账户中的哪些警报应由事件检测和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。

事件检测和响应使用 Amazon CloudWatch 和其他 AWS 服务 来构建您的可观察性解决方案。AWS 事件检测和响应可通过两种方式帮助您实现可观察性：

- 业务结果指标：AWS 事件检测和响应的可观察性始于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 专家与您合作，了解您的工作负载目标、可能影响用户体验的关键产出或因素，并定义捕捉这些关键指标中任何下降情况的指标和警报。例如，移动呼叫应用程序的关键业务指标是呼叫设置成功率（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。事件参与是根据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 和基础架构，并定义指标和警报以跟踪这些基础设施服务的性能。这些指标可能包括诸如 Application L `ApplicationLoadBalancerErrorCount` oad Balancer 实例的指标。这将在加载工作负载并设置监控后开始。

在 AWS 事件检测和响应中实现可观察性

由于可观察性是一个持续的过程，可能无法在一次练习或时间范围内完成，因此 AWS 事件检测和响应分两个阶段实现可观察性：

- 入职阶段：入职期间的可观察性侧重于检测应用程序的业务结果何时受到损害。为此，入职阶段的可观察性侧重于定义应用程序层的关键业务结果指标，以通知您的 AWS 工作负载中断。这种方式 AWS 可以迅速应对这些中断，并为您提供恢复方面的帮助。
- 入职后阶段：AWS 事件检测和响应为可观察性提供了许多主动服务，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。这些服务的实施可能需要几个月，涉及多个团队。AWS 事件检测和响应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。如需亲自实现可观测性功能的帮助，请向您的技术客户经理提出请求 (TAMs)。

利用事件检测和响应进行事件管理

AWS 事件检测和响应为您提供全天候主动监控和事件管理，由指定的事件经理团队提供。下图概述了应用程序警报触发事件时的标准事件管理流程，包括警报生成、 AWS 事件经理参与、事件解决方案和事后审查。

1. 警报生成：在您的工作负载上触发的警报将通过 Amazon 推送 EventBridge 到 AWS 事件检测和响应。AWS 事件检测和响应会自动调出与您的警报相关的操作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 事件检测和响应监控的警报未检测到，则您可以创建支持案例来请求事件响应。有关请求事件响应的更多信息，请参阅请求事件响应。
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的其他规定与您接触。事件经理会验证的运行状况， AWS 服务 以确定警报是否与工作负载 AWS 服务 使用的问题有关，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，并聘请合适的 AWS 专家提供支持。

   由于 AWS 事件检测和响应 AWS 服务 专门针对您的应用程序进行监控，因此 AWS 事件检测和响应可能会在宣布事件之前就确定 AWS 服务 事件与 AWS 服务 问题有关。在这种情况下，事件经理会向您提供状态建议 AWS 服务，触发 AWS 服务事件管理流程，并跟进服务团队以解决问题。所提供的信息使您有机会尽早实施恢复计划或变通方案，以减轻 AWS 服务事件的影响。有关更多信息，请参阅 服务事件的事故管理。
3. 事件解决方案：事件经理协调所需 AWS 团队中的事件，并确保在事件得到缓解或解决之前，您与合适的 AWS 专家保持接触。
4. 事后审查（如果需要）：事件发生后，AWS 事件检测和响应可以根据您的要求进行事后审查，并生成事后报告。事故后报告包括对问题的描述、影响、参与的团队以及为缓解或解决事件而采取的变通办法或行动。事故后报告可能包含可用于降低事件再次发生的可能性或改善对未来发生类似事件的管理的信息。事故后报告不是根本原因分析 (RCA)。除事故后报告外，您还可以申请 RCA。以下部分提供了事件后报告的示例。

> **Important**
>
> 以下报告模板仅为示例。

```
Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
```

Customer: Example Customer
AWS Support 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 AWS Support Center Console 提供访问权限

AWS 事件检测和响应会在事件生命周期内通过 支持 案例与您沟通。要与事件经理通信，您的团队必须有权访问 支持 中心。

有关配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 Center 的访问权限”。

服务事件的事故管理

AWS 事件检测和响应会在对客户产生广泛影响的 AWS 服务 中断期间通知您，包括影响多个客户的问题或您的工作负载在受影响区域 AWS 区域 或可用区域内使用的问题。 AWS 服务 根据请求，AWS 事件检测和响应事件经理可以加入您的电话会议桥以执行以下操作：

- 指导您完成恢复计划的实施
- 中继潜在的解决方法
- 收集有关事件和影响的信息

- 代表你在内部倡导和 AWS 上报问题

您可以通过接收服务中断通知 AWS Health。如果您在 AWS 区域 不受服务中断影响的情况下运营或不使用受损服务，则您可以继续通过标准的 AWS 事件检测和响应项目获得支持。有关的更多信息 AWS Health，请参阅什么是 AWS Health？ 。

要详细了解 AWS 事件检测和响应在服务中断期间如何为您提供支持，请查看以下事件响应工作流程图。该图概述了 AWS 团队采取的步骤，并描述了事件响应团队如何与您合作以识别、缓解和解决服务中断。

请求事件响应

如果您的工作负载上发生了严重事件，但 AWS 事件检测和响应监控的警报未检测到，则可以创建支持案例来请求事件响应。您可以使用、 AWS 支持 API 或为订阅了 AWS 事件检测和响应的任何工作负载（包括入职过程中的工作负载）请求事件响应。 AWS Support Center Console AWS Support App in Slack

下图说明了 AWS 客户向事件检测和响应团队请求事件帮助 end-to-end的工作流程，详细说明了从最初请求到调查、缓解和解决的步骤。

要针对正在积极影响您的工作量的事件请求事件响应，请创建 支持 案例。在提出支持案例后，AWS 事件检测和响应会让您与加快工作负载恢复所需的 AWS 专家进行会谈。

使用请求事件响应 AWS Support Center Console

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. 在 “类别” 中，选择 “活动事件”。
5. 对于 “严重性”，选择 “关键业务系统关闭”。
6. 输入此事件的主题。例如：

   AWS 事件检测和响应-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
- 商业信息：

  描述对业务的影响

  [可选] 客户桥详情

8. 为了帮助我们更快地与 AWS 专家接触，请提供以下详细信息：
   - 受影响 AWS 服务
   - 其他服务/其他受影响服务
   - 受影响 AWS 区域
9. 在 “其他联系人” 部分，输入您想要接收有关此事件的信件的所有电子邮件地址。

   下图显示了控制台屏幕，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，您可以从您的组织添加其他电子邮件地址。要添加其他地址，请回复问题，然后在 “其他联系人” 部分添加电子邮件地址。

   下图显示了 “案例详情” 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 事件检测和响应会在五分钟内确认您的案例，并与相应的 AWS 专家进行会谈。

使用 AWS 支持 API 请求事件响应

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。

使用请求事件响应 AWS Support App in Slack

要使用请求事件响应，请完成以下步骤： AWS Support App in Slack

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

```
/awssupport create
```

3. 输入此事件的主题。例如，输入 AWS 事件检测和响应-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：

   受影响区域：

   工作负载名称：

   商业信息：

   对业务影响的描述：

   [可选] 客户桥详情：
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. 在 “类别” 中，选择 “活动事件”。
9. 对于 “严重性”，选择 “关键业务系统关闭”。

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。这些其他联系人会收到有关此事件的电子邮件通信副本。

11选择审核。

12Slack 频道中会出现一条只有你才能看到的新消息。查看案例详情，然后选择创建案例。

13您的问题编号是在来自的新消息中提供的 AWS Support App in Slack。

14事件检测和响应会在 5 分钟内确认您的案例，并在会议桥上与相应的 AWS 专家接触。

15来自 “事件检测和响应” 的信件已在案例话题中更新。

使用管理事件检测和响应支持案例 AWS Support App in Slack

借助 AWS Support App in Slack，您可以在 Slack 中管理您的 支持 案例，在 AWS 事件检测和响应工作负载中接收有关新警报启动的事件的通知，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 中接收有关您的工作负载的所有警报启动事件的通知，您必须 AWS Support App in Slack 为所有已加入 AWS 事件检测和响应的工作负载账户进行配置。Support 案例是在产生工作负载警报的账户中创建的。
> - 在事件发生期间，可以代表您提出多个高严重性的支持案例，以吸引 支持 解决者。在 Slack 中，您会收到事件期间打开的所有支持案例的通知，这些案例与您的 Slack 频道的通知配置相匹配。
> - 您通过收到的通知并 AWS Support App in Slack 不能取代 AWS 事件检测和响应在事件发生期间通过电子邮件或电话联系的工作负载初始联系和上报联系人。

主题

在 Slack 中发出警报的事件通知

在 Slack 频道 AWS Support App in Slack 中配置后，您会收到有关在 AWS 事件检测和响应监控的工作负载上发生警报事件的通知。

以下示例显示了警报启动事件的通知如何在 Slack 中显示。

通知示例

当 AWS 事件检测和响应确认您的警报启动的事件时，Slack 中会生成类似于以下内容的通知：

要查看 AWS 事件检测和响应添加的完整信件，请选择查看详情。

AWS 事件检测和响应的更多更新将出现在该案例的话题中。

选择 “查看详情”，查看 AWS 事件检测和响应添加的完整信件。

在 Slack 中创建事件响应请求

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

在 “事件检测和响应” 中进行报告

AWS 事件检测和响应提供操作和性能数据，帮助您了解服务的配置方式、事件历史以及事件检测和响应服务的性能。本页介绍可用的数据类型，包括配置数据、事件数据和性能数据。

配置数据

- 所有账户均已登录
- 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

- 每个应用程序发生事件的日期、数量和持续时间
- 与特定警报相关的事件的日期、数量和持续时间
- 事故后报告

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营和绩效数据。

事件检测和响应安全性与弹性

分AWS 担责任模型适用于中的数据保护 支持。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。此内容包括您 AWS 服务 使用的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 安全博客上的责任AWS 共担模型和 GDPR 博客文章。

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) 设置个人用户账户。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 Secure Soc Layer/Transport Layer Security (SSL/TLS kets () 证书与 AWS 资源通信。建议使用 TLS 1.2 或更高版本。有关信息，请参阅什么是 SSL/TLS 证书？ 。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关信息，请参阅AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。有关亚马逊 Macie 的信息，请参阅亚马逊 Mac ie。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 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，请参阅联邦信息处理标准 (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）。这包括您使用控制台、API、CLI 支持 或以其他 AWS 服务 方式使用控制台、AP AWS I 或时 AWS SDKs。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 事件检测和响应访问您的账户

AWS Identity and Access Management (IAM) 是一项 Web 服务，可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 事件检测和响应以及您的警报数据

默认情况下，事件检测和响应会收到您账户中每个 CloudWatch 警报的 Amazon 资源名称 (ARN) 和状态，然后在您的已加载警报变为 “警报” 状态时启动事件检测和响应流程。如果您想自定义事件检测和响应会从您的账户接收的有关警报的信息，请联系您的技术客户经理。

文档历史记录

下表描述了自上次发布 IDR 指南以来对文档所做的重要更改。

更改	描述	日期
有关事件检测和响应如何处理服务事件的更新信息	更新了服务事件的事件管理部分。 更新的章节：服务事件的事故管理	2025 年 5 月 15 日
新功能：禁止警报进入事件检测和响应	在托管工作负载中添加了新的章节，提供了有关如何临时或按计划抑制警报的信息 新版块：抑制警报，使其无法使用事件检测和响应	2025 年 4 月 9 日
更新了使用 “请求事件响应” 的说明 AWS Support Center Console	添加了有关在 “问题描述” 字段中输入哪些信息的详细信息。 更新的章节：请求事件响应	2025 年 2 月 6 日
AWS 区域 已添加其他内容	AWS 区域 已在 “事件检测和响应” 可用性部分中添加了其他内容。 更新的章节：事件检测和响应的区域可用性	2024 年 11 月 1 日
通过 AWS Support App in Slack页面更新了 “管理事件检测和响应” 支持案例	将页面移至 “事件管理” 下，修改了文本，并替换了屏幕截图。 更新的章节：使用管理事件检测和响应支持案例 AWS Support App in Slack	2024 年 10 月 10 日
添加了新页面 AWS Support App in Slack 通过 AWS 事件检测和响应更新了事件管理	为添加了新页面 AWS Support App in Slack 使用 AWS 事件检测和响应更新了事件管理，增加了新部分 “使用请求事件响应 AWS Support App in Slack”。	2024 年 9 月 10 日
更新了账户订阅	更新了 “账户订阅” 部分，以详细说明当你申请订阅账户时，应在哪里提出支持案例。	2024 年 6 月 12 日

更改	描述	日期
	更新的章节：为工作负载订阅事件检测和响应	
服务事件后报告现已推出	更新了服务事件的事件管理部分，以包含有关服务事件的事件后报告的信息。 更新的章节：服务事件的事故管理	2024 年 5 月 8 日
添加了新章节：移除工作负载	在 “入门” 中添加了 “卸载工作负载” 部分，以包含有关卸载工作负载的信息 有关更多信息，请参阅 将工作负载从事件检测和响应中移除。	2024 年 3 月 28 日
更新了账户订阅	更新了账户订阅部分，添加了有关离职工作负载的信息 有关更多信息，请参阅账号订阅	2024 年 3 月 28 日
更新了测试	更新了 “测试” 部分，添加了有关游戏日测试的信息，这是入职流程的最后一步。 更新的章节：在 “事件检测和响应” 中测试已加载的工作负载	2024 年 2 月 29 日
已更新什么是 AWS 事件检测和响应	更新了什么是 AWS 事件检测和响应部分。 更新的章节：什么是 AWS 事件检测和响应？	2024 年 2 月 19 日
更新了问卷调查部分	更新了工作负载入职调查问卷并添加了警报摄取调查表。将该部分从入职调查表重命名为工作负载入职调查和警报摄取调查表。 更新的章节：事件检测和响应中的工作负载入和警报摄取问卷	2024 年 2 月 2 日

更改	描述	日期
更新了 AWS 服务活动和入职信息	更新了几个章节，其中包含了有关入职的新信息。 更新的章节： • 服务事件的事故管理 • 事件检测和响应中的工作负载发现 • 入门事件检测和响应 • 为工作负载订阅事件检测和响应 新章节 • 为应用程序团队 AWS Support Center Console 提供访问权限	2024 年 1 月 31 日
添加了 “相关信息” 部分	在访问配置中添加了相关信息部分。 更新的章节：配置对事件检测和响应的警报获取访问权限	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 的过程。 更新的章节：示例：整合来自 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 Ingest 警报 APMs 中与亚马逊 EventBridge直接集成的图片。 更新的章节：在 “事件检测和响应” 中制定应对事件的运行手册和响应计划	2023 年 12 月 21 日
更新了运行手册模板	更新了 AWS 事件检测和响应运行手册开发中的运行手册模板。 更新的章节：在 “事件检测和响应” 中制定应对事件的运行手册和响应计划	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，其中包含有关 CloudWatch 警报配置的详细信息。 新版块：在 “事件检测和响应” 中创建符合您业务需求的 CloudWatch 警报 新版块：使用 CloudFormation 模板在 “事件检测和响应” 中生成 CloudWatch 警报 新版块：事件检测和响应中 CloudWatch 警报的示例用例	2023 年 9 月 28 日
更新了入门	更新了《入门》，其中包含有关工作负载变更请求的信息。 新版块：在 “事件检测和响应” 中请求更改已载入的工作负载 更新的章节：为工作负载订阅事件检测和响应	2023年9月5日
入门中的新章节	在 AWS 事件检测和响应中添加了将警报引入 AWS 事件检测和响应提取警报。	2023 年 6 月 30 日
原始文档	AWS 事件检测和响应首次发布	2023 年 3 月 15 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。