Conceptos y procedimientos de detección y respuesta a incidentes de AWS

Guía del usuario de detección y respuesta a incidentes de AWS

Version May 15, 2025

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

Guía del usuario de detección y respuesta a incidentes de AWS: Conceptos y procedimientos de detección y respuesta a incidentes de AWS

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Incident Detection and Response? ... 1
Condiciones de uso ... 2
Arquitectura ... 3
Funciones y responsabilidades ... 4
Disponibilidad por región ... 6
Introducción ... 9
Cargas de trabajo ... 9
Alarmas ... 9
Incorporación ... 10
Incorporación de la carga de trabajo ... 10
Ingestión de alarmas ... 11
Cuestionarios de incorporación ... 11
Cuestionario de incorporación de la carga de trabajo: preguntas generales ... 12
Cuestionario de incorporación de la carga de trabajo: preguntas sobre arquitectura ... 12
Cuestionario de incorporación de la carga de trabajo: preguntas sobre los eventos AWS de servicio ... 15
Cuestionario de ingestión de alarmas ... 15
Matriz de alarmas ... 17
Descubrimiento de la carga ... 23
Suscriba una carga de trabajo ... 23
Defina y configure las alarmas ... 26
Cree CloudWatch alarmas ... 28
Cree CloudWatch alarmas con CloudFormation plantillas ... 31
Ejemplos de casos de uso de CloudWatch alarmas ... 34
Ingiera alarmas ... 37
Aprovisione el acceso ... 37
Intégrelo con CloudWatch ... 38
Ingiera alarmas desde APMs con la integración EventBridge ... 38
Ejemplo: integración de notificaciones de Datadog y Splunk ... 40
Ingiera alarmas sin necesidad de integración APMs EventBridge ... 50
Gestione las cargas de trabajo ... 51
Desarrolle manuales y planes de respuesta ... 51
Pruebe las cargas de trabajo integradas ... 58
CloudWatch alarmas ... 59

Alarmas APM de terceros ... 59
Salidas clave ... 59
Solicita cambios en una carga de trabajo ... 60
Suprima las alarmas ... 61
Suprima las alarmas en la fuente de alarma ... 62
Envíe una solicitud de cambio de carga de trabajo para suprimir las alarmas ... 68
Tutorial: Utilice una función matemática métrica para suprimir una alarma ... 68
Tutorial: Elimine una función matemática métrica para desactivar una alarma ... 71
Elimine una carga de trabajo ... 71
Supervisión y observabilidad ... 73
Implementación de la observabilidad ... 74
Administración de incidentes ... 75
Proporcione acceso a los equipos de aplicaciones ... 78
Gestión de incidentes para eventos de servicio ... 78
Solicite una respuesta a un incidente ... 79
Solicita a través del AWS Support Center Console ... 79
Solicita a través de la AWS Support API ... 81
Solicita a través del AWS Support App in Slack ... 81
Gestione los casos de asistencia en materia de detección y respuesta a incidentes con AWS Support App in Slack ... 82
Notificaciones de incidentes iniciadas por alarmas en Slack ... 83
Crea una solicitud de respuesta a un incidente en Slack ... 84
Informes ... 85
Seguridad y resiliencia ... 86
Acceso a sus cuentas ... 87
Sus datos de alarma ... 87
Historial de documentos ... 88
... xciv

¿Qué es AWS Incident Detection and Response?

AWS Incident Detection and Response ofrece a los clientes de AWS Enterprise Support elegibles una participación proactiva en caso de incidentes para reducir la posibilidad de fallas y acelerar la recuperación de las cargas de trabajo críticas tras una interrupción. Incident Detection and Response facilita su colaboración AWS para desarrollar manuales y planes de respuesta personalizados para cada carga de trabajo incorporada.

La detección y respuesta a incidentes ofrecen las siguientes funciones clave:

- Mejora de la observabilidad: AWS los expertos ofrecen orientación para ayudarle a definir y correlacionar las métricas y las alarmas entre los niveles de aplicación e infraestructura de su carga de trabajo a fin de detectar las interrupciones de forma temprana.
- Tiempo de respuesta de 5 minutos: los ingenieros de gestión de incidentes (IMEs) supervisan las cargas de trabajo integradas las 24 horas del día, los 7 días de la semana, para detectar incidentes críticos. IMEs Responden a los 5 minutos de que se active una alarma o en respuesta a un caso de Support crítico para la empresa que usted plantee a Incident Detection and Response.
- Resolución más rápida: IMEs utilice manuales predefinidos y personalizados desarrollados para que sus cargas de trabajo respondan en 5 minutos, cree un caso de Support en su nombre y gestione los incidentes de su carga de trabajo. IMEs gestionan los incidentes desde un único hilo y mantienen el contacto con los AWS expertos adecuados hasta que se resuelva el incidente.
- Gestión de incidentes para AWS eventos: como entendemos el contexto de su carga de trabajo crítica (por ejemplo, cuentas, servicios e instancias), podemos detectar y notificarle de forma proactiva cualquier posible impacto en su carga de trabajo durante un AWS evento de servicio. Si así lo solicita, IMEs interactuamos con usted durante los eventos AWS de servicio y le proporcionaremos información actualizada sobre los eventos. Si bien Incident Detection and Response no puede priorizar su recuperación durante un evento de servicio, Incident Detection and Response proporciona orientación de Support para ayudarlo a implementar su plan de mitigación.
- Reducción de las posibilidades de fallo: tras la resolución, le IMEs proporcionan una revisión posterior al incidente (previa solicitud). Además, los AWS expertos colaboran con usted para aplicar las lecciones aprendidas a fin de mejorar el plan de respuesta a los incidentes y los manuales de referencia. También puede aprovechar el seguimiento continuo AWS Resilience Hub de la resiliencia de sus cargas de trabajo.

Temas

- Condiciones de uso para la detección y respuesta a incidentes
- Arquitectura de detección y respuesta a incidentes
- Funciones y responsabilidades en la detección y respuesta a incidentes
- Disponibilidad regional para la detección y respuesta a incidentes

Condiciones de uso para la detección y respuesta a incidentes

En la siguiente lista se describen los requisitos y limitaciones clave para usar AWS Incident Detection and Response. Es importante que comprenda esta información antes de utilizar el servicio, ya que abarca aspectos como los requisitos del plan de soporte, el proceso de incorporación y la duración mínima de la suscripción.

- AWS Incident Detection and Response está disponible para las cuentas de Enterprise Support directas y revendidas por socios.
- La detección y respuesta a incidentes de AWS no están disponibles para las cuentas de Partner Led Support.
- Debe mantener AWS Enterprise Support en todo momento durante la vigencia de su servicio de detección y respuesta a incidentes. Para obtener más información, consulte Enterprise Support. La finalización de Enterprise Support implica la retirada simultánea del servicio AWS Incident Detection and Response.
- Todas las cargas de trabajo de AWS Incident Detection and Response deben pasar por el proceso de incorporación de cargas de trabajo.
- La duración mínima para suscribir una cuenta a AWS Incident Detection and Response es de noventa (90) días. Todas las solicitudes de cancelación deben presentarse treinta (30) días antes de la fecha de entrada en vigor prevista para la cancelación.
- AWS maneja su información como se describe en el Aviso AWS de privacidad.

> **Note**
>
> Si tienes preguntas sobre la detección y respuesta a incidentes relacionados con la facturación, consulta Cómo obtener ayuda con la AWS facturación.

Arquitectura de detección y respuesta a incidentes

AWS Incident Detection and Response se integra con su entorno actual, como se muestra en el siguiente gráfico. La arquitectura incluye los siguientes servicios:

- Amazon EventBridge: Amazon EventBridge actúa como el único punto de integración entre sus cargas de trabajo y AWS Incident Detection and Response. Las alarmas se ingresan desde sus herramientas de monitoreo, como Amazon CloudWatch, a través de Amazon EventBridge mediante reglas predefinidas administradas por AWS. Para permitir que Incident Detection and Response cree y gestione la EventBridge regla, debe instalar un rol vinculado a un servicio. Para obtener más información sobre estos servicios, consulta Qué es Amazon EventBridge y EventBridge las reglas de Amazon, Qué es Amazon CloudWatch y Uso de funciones vinculadas a servicios. AWS Health
- AWS Health: AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus cuentas Servicios de AWS . La función Detección y Respuesta AWS Health a Incidentes Servicios de AWS se utiliza para realizar un seguimiento de los eventos relacionados con sus cargas de trabajo y para notificarle cuando recibe una alerta de su carga de trabajo. Para obtener más información AWS Health, consulte Qué es AWS Health.
- AWS Systems Manager: Systems Manager proporciona una interfaz de usuario unificada para la automatización y la administración de tareas en todos sus AWS recursos. AWS Incident Detection and Response aloja información sobre sus cargas de trabajo, incluidos diagramas de arquitectura de cargas de trabajo, detalles de alarmas y sus correspondientes manuales de gestión de incidentes en AWS Systems Manager los documentos (para obtener más información, consulte AWS Systems Manager Documentos). Para obtener más información AWS Systems Manager, consulte Qué es. AWS Systems Manager
- Sus manuales específicos: un manual de gestión de incidentes define las acciones que AWS Incident Detection and Response lleva a cabo durante la gestión de incidentes. Sus manuales específicos indican a AWS Incident Detection and Response con quién ponerse en contacto, cómo ponerse en contacto con ellos y qué información compartir.

Funciones y responsabilidades en la detección y respuesta a incidentes

En la tabla RACI de detección y respuesta a incidentes de AWS (responsable, responsable, consultado e informado) se describen las funciones y responsabilidades de las diversas actividades relacionadas con la detección y la respuesta a incidentes. Esta tabla ayuda a definir la participación del cliente y del equipo de detección y respuesta a incidentes de AWS en tareas como la recopilación de datos, la revisión de la preparación para las operaciones, la configuración de la cuenta, la gestión de incidentes y la revisión posterior a los incidentes.

Actividad	Cliente	Detección y respuesta a incidentes
Recopilación de datos		
Introducción a los clientes y las cargas de trabajo	Consultado	Responsable
Arquitectura	Responsable	Responsable
Operaciones	Responsable	Responsable
Determine CloudWatch las alarmas que se van a configurar	Responsable	Responsable
Defina un plan de respuesta a incidentes	Responsable	Responsable
Completar el cuestionario de incorporación	Responsable	Responsable

Actividad	Cliente	Detección y respuesta a incidentes
Revisión de la preparación de las operaciones		
Realice una revisión bien estructurada (WAR) de la carga de trabajo	Consultado	Responsable
Valide la respuesta al incidente	Consultado	Responsable
Valide la matriz de alarmas	Consultado	Responsable
Identifique AWS los servicios clave que utiliza la carga de trabajo	Responsable	Responsable
Configuración de la cuenta		
Cree un rol de IAM en la cuenta del cliente	Responsable	Informado
Instale la EventBridge regla administrada mediante el rol creado	Informado	Responsable
Pruebe CloudWatch las alarmas	Responsable	Responsable
Verifique que las alarmas de los clientes activen la detección y respuesta a los incidentes	Informado	Responsable
Actualiza las alarmas	Responsable	Consultado

Actividad	Cliente	Detección y respuesta a incidentes
Actualice los manuales	Consultado	Responsable
Administración de incidentes		
Notifique de forma proactiva los incidentes detectados mediante la detección y respuesta a incidentes	Informado	Responsable
Proporcione una respuesta a los incidentes	Informado	Responsable
Proporcione la resolución de incidentes o la restauración de la infraestructura	Responsable	Consultado
Revisión posterior al incidente		
Solicite una revisión posterior al incidente	Responsable	Informado
Proporcione una revisión posterior al incidente	Informado	Responsable

Disponibilidad regional para la detección y respuesta a incidentes

Actualmente, AWS Incident Detection and Response está disponible en inglés y japonés para las cuentas de Enterprise Support alojadas en cualquiera de los siguientes sitios Regiones de AWS:

Nombre	Región de AWS
us-east-1	EE.UU. Este (Virginia)

Nombre	Región de AWS
us-east-2	Este de EE. UU. (Ohio)
us-west-1	Oeste de EE. UU. (Norte de California)
us-west-2	Oeste de EE. UU. (Oregón)
ca-central-1	Canadá (centro)
ca-west-1	Oeste de Canadá (Calgary)
sa-east-1	América del Sur (São Paulo)
eu-central-1	Europa (Fráncfort)
eu-west-1	Europa (Irlanda)
eu-west-2	Europa (Londres)
eu-west-3	Europa (París)
eu-north-1	Europa (Estocolmo)
eu-central-2	Europa (Zúrich)
eu-south-1	Europa (Milán)
eu-south-2	Europa (España)
ap-south-1	Asia-Pacífico (Bombay)
ap-northeast-1	Asia-Pacífico (Tokio)
ap-northeast-2	Asia-Pacífico (Seúl)
ap-southeast-1	Asia-Pacífico (Singapur)
ap-southeast-2	Asia-Pacífico (Sídney)
ap-east-1	Asia-Pacífico (Hong Kong)

Nombre	Región de AWS
ap-northeast-3	Asia-Pacífico (Osaka)
ap-south-2	Asia-Pacífico (Hyderabad)
ap-southeast-3	Asia-Pacífico (Yakarta)
ap-southeast-4	Asia-Pacífico (Melbourne)
ap-southeast-5	Asia-Pacífico (Malasia)
af-south-1	África (Ciudad del Cabo)
il-central-1	Israel (Tel Aviv)
me-central-1	Medio Oriente (EAU)
me-south-1	Medio Oriente (Baréin)

Comience con la detección y respuesta a incidentes

Las cargas de trabajo y las alarmas son fundamentales para la detección y respuesta a incidentes de AWS. AWS trabaja en estrecha colaboración con usted para definir y supervisar las cargas de trabajo específicas que son fundamentales para su empresa. AWS le ayuda a configurar alarmas que notifiquen rápidamente a su equipo sobre problemas importantes de rendimiento o sobre el impacto en los clientes. Las alarmas correctamente configuradas son esenciales para una supervisión proactiva y una respuesta rápida a los incidentes en el marco de la detección y respuesta a incidentes.

Cargas de trabajo

Puede seleccionar cargas de trabajo específicas para la supervisión y la gestión de incidentes críticos mediante AWS Incident Detection and Response. Una carga de trabajo es un conjunto de recursos y código que funcionan en conjunto para ofrecer valor empresarial. Una carga de trabajo puede consistir en todos los recursos y el código que componen su portal de pagos bancarios o un sistema de gestión de las relaciones con los clientes (CRM). Puedes alojar una carga de trabajo en AWS una o varias AWS cuentas.

Por ejemplo, puede tener una aplicación monolítica alojada en una sola cuenta (por ejemplo, la aplicación Employee Performance en el siguiente diagrama). O bien, puede que tengas una aplicación (por ejemplo, Storefront Webapp en el diagrama) dividida en microservicios que se distribuyen en distintas cuentas. Una carga de trabajo puede compartir recursos, como una base de datos, con otras aplicaciones o cargas de trabajo, como se muestra en el diagrama.

Para empezar a incorporar cargas de trabajo, consulte el cuestionario sobre incorporación de cargas de trabajo e incorporación de cargas de trabajo.

Alarmas

Las alarmas son una parte clave de la detección y respuesta a incidentes, ya que proporcionan visibilidad del rendimiento de las aplicaciones y la infraestructura subyacente. AWS AWS trabaja con usted para definir las métricas y los umbrales de alarma adecuados que solo se activarán cuando se produzca un impacto crítico en las cargas de trabajo supervisadas. El objetivo es que las alarmas capten la atención de los responsables de la resolución que especifiquen, quienes, a su vez, podrán colaborar con el equipo de gestión de incidentes para mitigar rápidamente cualquier problema.

Las alarmas deben configurarse para que solo entren en el estado de alarma cuando se produzca una degradación significativa del rendimiento o de la experiencia del cliente que requiera atención inmediata. Algunos tipos clave de alarmas incluyen las que indican el impacto en el negocio, Amazon CloudWatch Canaries y las alarmas agregadas que monitorean las dependencias.

Para empezar con la ingesta de alarmas, consulte el cuestionario sobre la ingesta de alarmas y la ingesta de alarmas.

> **Note**
>
> Para realizar cambios en sus manuales de ejecución, en la información de la carga de trabajo o en las alarmas monitorizadas en AWS Incident Detection and Response, consulteSolicite cambios en una carga de trabajo integrada en Incident Detection and Response.

Introducción a la detección y respuesta a incidentes

AWS trabaja con usted para incorporar su carga de trabajo y sus alarmas a AWS Incident Detection and Response. Usted proporciona información clave AWS en elCuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response. Se recomienda que también registre sus cargas de trabajo. AppRegistry Para obtener más información, consulte la Guía del usuario de AppRegistry .

El siguiente diagrama muestra el flujo de incorporación de cargas de trabajo y administración de alarmas en la detección y respuesta a incidentes:

Incorporación de la carga de trabajo

Durante la incorporación de la carga de trabajo, AWS trabaja con usted para comprender su carga de trabajo y cómo ayudarlo durante los incidentes y los eventos de AWS servicio. Usted proporciona información clave sobre su carga de trabajo que le ayuda a mitigar el impacto.

Resultados clave:

- Información general sobre la carga de trabajo
- Detalles de la arquitectura, incluidos los diagramas
- Información del manual

- Incidentes iniciados por el cliente
- AWS Eventos de servicio

Ingesta de alarmas

AWS trabaja con usted para incorporar sus alarmas. AWS Incident Detection and Response puede captar alarmas de herramientas de monitoreo del rendimiento de aplicaciones (APM) de Amazon CloudWatch y de terceros a través de Amazon. EventBridge La incorporación de alarmas permite una detección proactiva de incidentes y una interacción automatizada. Para obtener más información, consulta las alarmas de ingesta APMs que tienen una integración directa con Amazon EventBridge.

Resultados clave:

- Matriz de alarmas

En la siguiente tabla se enumeran los pasos necesarios para incorporar una carga de trabajo a AWS Incident Detection and Response. En esta tabla se muestran ejemplos de las duraciones de cada tarea. Las fechas reales de cada tarea se definen en función de la disponibilidad y el cronograma del equipo.

Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response

En esta página se proporcionan los cuestionarios que debe completar al incorporar una carga de trabajo a AWS Incident Detection and Response y al configurar las alarmas para incorporarlas al servicio. El cuestionario de incorporación de la carga de trabajo incluye información general sobre la carga de trabajo, los detalles de su arquitectura y los contactos necesarios para responder a los incidentes. En el cuestionario de ingesta de alarmas, debe especificar las alarmas críticas que deberían activar la creación de incidentes en Incident Detection and Response para su carga de trabajo, así como información resumida sobre con quién debe ponerse en contacto y qué medidas se deben tomar. Completar correctamente estos cuestionarios es un paso clave a la hora de configurar los procesos de supervisión y respuesta a incidentes para sus cargas de trabajo. AWS

Descargue el cuestionario de incorporación de cargas de trabajo.

Descarga el cuestionario de ingesta de alarmas.

Cuestionario de incorporación de la carga de trabajo: preguntas generales

Preguntas generales

Pregunta	Respuesta de ejemplo
Nombre de la empresa	Amazon Inc.
Nombre de esta carga de trabajo (incluya cualquier abreviatura)	Amazon Retail Operations (ARO)
El usuario final principal y la función de esta carga de trabajo.	Esta carga de trabajo es una aplicación de comercio electrónico que permite a los usuarios finales comprar varios artículos. Esta carga de trabajo es el principal generador de ingresos para nuestro negocio.
Los requisitos normativos o de cumplimiento aplicables a esta carga de trabajo y cualquier acción que sea necesaria AWS después de un incidente.	La carga de trabajo se refiere a los registros de salud de los pacientes, que deben mantenerse seguros y confidenciales.

Cuestionario de incorporación de la carga de trabajo: preguntas sobre arquitectura

Preguntas sobre arquitectura

Pregunta	Respuesta de ejemplo
Una lista de etiquetas de AWS recursos que se utilizan para definir los recursos que forman parte de esta carga de trabajo. AWS utiliza estas etiquetas para identificar los recursos de esta carga de trabajo a fin de agilizar el soporte durante los incidentes.	Nombre de la aplicación: Optimax entorno: Producción

Pregunta	Respuesta de ejemplo
Note Las etiquetas distinguen entre mayúsculas y minúsculas. Si proporcio na varias etiquetas, todos los recursos utilizados por esta carga de trabajo deben tener las mismas etiquetas.	
Una lista de AWS los servicios utilizados por esta carga de trabajo y la AWS cuenta y las regiones en las que se encuentran. **Note** Crea una nueva fila para cada servicio.	Ruta 53: enruta el tráfico de Internet al ALB. Cuenta: 123456789101 Región: US-EAST-1, US-WEST-2
Una lista de los AWS servicios utilizados por esta carga de trabajo, junto con la AWS cuenta y las regiones en las que se encuentran. **Note** Crea una nueva fila para cada servicio.	ALB: enruta el tráfico entrante a un grupo objetivo de contenedores ECS. Cuenta: 123456789101 Región: N/A
Una lista de AWS los servicios utilizados por esta carga de trabajo, junto con la AWS cuenta y las regiones en las que se encuentran. **Note** Crea una nueva fila para cada servicio.	ECS: infraestructura de cómputo para la flota principal de lógica empresarial. Responsab le de gestionar las solicitudes de los usuarios entrantes y de realizar consultas a la capa de persistencia. Cuenta: 123456789101 Región: US-EAST-1

Pregunta	Respuesta de ejemplo
Una lista de AWS los servicios utilizados por esta carga de trabajo, junto con la AWS cuenta y las regiones en las que se encuentran. Note Crea una nueva fila para cada servicio.	RDS: el clúster Amazon Aurora almacena los datos de los usuarios a los que accede la capa de lógica empresarial de ECS. Cuenta: 123456789101 Región: US-EAST-1
Una lista de AWS los servicios utilizados por esta carga de trabajo, junto con la AWS cuenta y las regiones en las que se encuentran. Note Crea una nueva fila para cada servicio.	S3: Almacena los activos estáticos del sitio web. Cuenta: 123456789101 Región: N/A
Detalle los componentes ascendentes/descendentes que no estén integrados y que puedan afectar a esta carga de trabajo en caso de producirse una interrupción.	Microservicio de autenticación: evitará que los usuarios carguen sus historiales médicos, ya que no estarán autenticados.
¿Hay algún AWS componente interno o ajeno a esta carga de trabajo? Si es así, ¿qué son y qué funciones se desempeñan?	Todo el tráfico de entrada y salida de Internet AWS se enruta a través de nuestro servicio de proxy local.
Proporcione detalles de cualquier plan manual o automatizado de recuperación ante fallos o desastres a nivel regional o de zona de disponibilidad.	Modo de espera en caliente. Conmutación por error automática al US-WEST-2 durante una caída sostenida de la tasa de éxito.

Cuestionario de incorporación de la carga de trabajo: preguntas sobre eventos de servicio AWS

AWS Preguntas sobre eventos de servicio

Pregunta	Respuesta de ejemplo
Proporcione los detalles de contacto (equipo de gestión de name/email/phone) of your company's internal major incident/IT crisis).	Equipo de gestión de incidentes graves mim@example.com +61 2 3456 7890
Proporcione detalles de cualquier puente estático de gestión de incidentes/crisis establecido por su empresa. Si utiliza puentes no estáticos, especifique su aplicación preferida y AWS solicitará estos detalles durante un incidente. Note Si no se proporciona ninguno, nos pondremos en contacto con nosotros durante un incidente y te AWS proporcionaremos un puente de Chime al que puedas unirte.	Amazon Chime https://chime.aws/1234567890

Cuestionario de ingestión de alarmas

Preguntas del manual

Pregunta	Respuesta de ejemplo
AWS contratará a los contactos relacionados con la carga de trabajo a través del Soporte caso. ¿Quién es el contacto principal cuando	Equipo de aplicaciones app@example.com

Pregunta	Respuesta de ejemplo
se activa una alarma relacionada con esta carga de trabajo? Especifique la aplicación de conferencias que prefiera y AWS solicitará estos detalles durante un incidente. **Note** Si no se proporciona una aplicación de conferencias preferida, nos pondremos en contacto contigo durante un incidente y te AWS proporcionaremos un Chime Bridge al que puedas unirte.	+61 2 3456 7890
Si el contacto principal no está disponible durante un incidente, indique los contactos de emergencia y el calendario en el orden de comunicación preferido.	1. Transcurridos 10 minutos, si el contacto principal no responde, interactúa con: John Smith: supervisor de aplicaciones john.smith@example.com +61 2 3456 7890 2. Transcurridos 10 minutos, si John Smith no responde, póngase en contacto con: Jane Smith, gerente de operaciones jane.smith@example.com +61 2 3456 7890

Pregunta	Respuesta de ejemplo
AWS comunica las actualizaciones a través del servicio de asistencia a intervalos regulares durante todo el incidente. ¿Hay contactos adicionales que deban recibir estas actualizaciones?	john.smith@example.com, jane.smith@example.com

Matriz de alarmas

Proporcione la siguiente información para identificar el conjunto de alarmas que activarán AWS Incident Detection and Response para crear incidentes en nombre de su carga de trabajo. Una vez que los ingenieros de AWS Incident Detection and Response hayan revisado sus alarmas, se darán los pasos de incorporación adicionales.

Criterios de alarma crítica de AWS para la detección y respuesta a incidentes:

- Las alarmas de detección y respuesta a incidentes de AWS solo deberían pasar al estado de «alarma» si el impacto empresarial en la carga de trabajo monitoreada fuera significativo (pérdida de ingresos o deterioro de la experiencia del cliente) que requiera la atención inmediata del operador.
- Las alarmas de detección y respuesta a incidentes de AWS también deben involucrar a los responsables de la carga de trabajo al mismo tiempo o antes de la activación. AWS Los gestores de incidentes colaboran con los responsables de la resolución en el proceso de mitigación y no actúan como agentes de primera línea que, a su vez, se ponen en contacto con usted.
- Los umbrales de alarma de detección y respuesta a incidentes de AWS se deben establecer con un umbral y una duración adecuados, de modo que cada vez que se active una alarma se lleve a cabo una investigación. Si una alarma se mueve entre los estados «Alarma» y «OK», se está produciendo un impacto suficiente como para justificar la respuesta y la atención del operario.

Política de detección y respuesta a incidentes de AWS en caso de incumplimiento de los criterios:

Estos criterios solo se pueden evaluar a case-by-case medida que se producen los eventos. El equipo de gestión de incidentes trabaja con sus gestores técnicos de cuentas (TAMs) para ajustar las alarmas y, en raras ocasiones, inhabilitar la supervisión si se sospecha que las alarmas de

los clientes no cumplen con este criterio y recurre al equipo de gestión de incidentes de forma innecesaria y regular.

> **Important**
>
> Proporcione direcciones de correo electrónico de distribución en grupo cuando indique las direcciones de contacto, de modo que pueda controlar las incorporaciones y eliminaciones de destinatarios sin necesidad de actualizar el manual.
> Indique el número de teléfono de contacto del equipo de ingeniería de confiabilidad (SRE) de su sitio si desea que el equipo de detección y respuesta a incidentes de AWS lo llame después de enviar un correo electrónico de contacto inicial.

Tabla de matrices de alarmas

Nombre de la métrica/ ARN/Umbral	Descripción	Notas	Acciones solicitadas
Volumen de carga de trabajo/ *CW Alarm ARN* / CallCount < 100 000 para 5 puntos de datos en 5 minutos, trate los datos faltantes como si faltaran	Esta métrica representa la cantidad de solicitudes entrantes que llegan a la carga de trabajo, medida en el nivel de Application Load Balancer. Esta alarma es importante porque las caídas significa tivas en las solicitud es entrantes pueden indicar problemas con la conectividad de la red ascendent e o problemas con nuestra implement ación del DNS	La alarma ha entrado en el estado de «Alarma» 10 veces en la última semana. Esta alarma corre el riesgo de producir falsos positivos. Está prevista una revisión de los umbrales. ¿Problemas? No o sí (si no, déjelo en blanco): esta alarma se activa con frecuencia durante la ejecución de un trabajo por lotes en particular.	Comuníquese con el equipo de ingenierí a de confiabilidad del sitio enviando un correo electrónico a *SRE@xyz.com* Cree un caso de AWS Premium Support para nuestros servicios ELB y Route 53. Si es necesaria una acción INMEDIATA : compruebe si hay memoria o espacio EC2 libre en disco e informe al *XYZ* equipo por correo

Nombre de la métrica/ ARN/Umbral	Descripción	Notas	Acciones solicitadas
	que hacen que los usuarios no puedan acceder a la carga de trabajo.	Resolvedores: ingenieros de confiabilidad del sitio	electrónico para que reinicie la instancia o ejecute una limpieza de registros. (si no es necesaria una acción inmediata, déjelo en blanco)

Nombre de la métrica/ ARN/Umbral	Descripción	Notas	Acciones solicitadas
Latencia de solicitud de carga de trabajo/ *CW Alarm ARN* / p90 Latencia superior a 100 ms para 5 puntos de datos en 5 minutos; trate los datos faltantes como si faltaran	Esta métrica representa la latencia de p90 para que la carga de trabajo atienda las solicitudes HTTP. Esta alarma represent a la latencia (una medida importante de la experiencia del cliente para el sitio web).	La alarma ha entrado en el estado de «Alarma» 0 veces en la última semana. ¿Problemas? No o sí (si no, déjelo en blanco): esta alarma se activa con frecuencia durante la ejecución de un trabajo por lotes en particular. Resolvedores: ingenieros de confiabil idad del sitio	Comuníquese con el equipo de ingenierí a de confiabilidad del sitio enviando un correo electrónico a *SRE@xyz.com* Cree un caso de AWS Premium Support para nuestros servicios de ECW y RDS. Si es necesaria una acción INMEDIATA : compruebe si hay memoria o espacio EC2 libre en disco e informe al *XYZ* equipo por correo electrónico para que reinicie la instancia o ejecute una limpieza de registros. (si no es necesaria una acción inmediata, déjelo en blanco)

Nombre de la métrica/ARN/Umbral	Descripción	Notas	Acciones solicitadas
Disponibilidad de solicitudes de carga de trabajo/ *CW Alarm ARN* / Disponibilidad inferior al 95% para 5 puntos de datos en 5 minutos; trate los datos faltantes como si faltaran.	Esta métrica representa la disponibilidad de las solicitudes HTTP para ser atendidas por la carga de trabajo (número de 200 HTTP/número de solicitudes) por período. Esta alarma represent a la disponibilidad de la carga de trabajo.	La alarma ha entrado en el estado de «Alarma» 0 veces en la última semana. ¿Problemas? No o sí (si no, déjelo en blanco): esta alarma se activa con frecuencia durante la ejecución de un trabajo por lotes en particular. Resolvedores: ingenieros de confiabil idad del sitio	Comuníquese con el equipo de ingenierí a de confiabilidad del sitio enviando un correo electrónico a *SRE@xyz.com* Cree un caso de AWS Premium Support para nuestros servicios ELB y Route 53. Si es necesaria una acción INMEDIATA : compruebe si hay memoria o espacio EC2 libre en disco e informe al *XYZ* equipo por correo electrónico para que reinicie la instancia o ejecute una limpieza de registros. (si no es necesaria una acción inmediata, déjelo en blanco)
Ejemplo de alarma New Relic			

Nombre de la métrica/ARN/Umbral	Descripción	Notas	Acciones solicitadas
Prueba de integración de extremo a extremo/ *CW Alarm ARN* / Tasa de error del 3% para métricas de 1 minuto de duración superior a 3 minutos; trate los datos faltantes como si faltaran Identificador de carga de trabajo: flujo de trabajo de pruebas de extremo a extremo, región de AWS: US-EAST-1, ID de cuenta de AWS: 012345678910	Esta métrica comprueba si una solicitud puede atravesar cada capa de la carga de trabajo. Si esta prueba falla, se trata de una falla crítica en el procesamiento de las transacciones comerciales. Esta alarma representa la capacidad de procesar las transacciones comerciales para la carga de trabajo.	La alarma ha entrado en el estado de «Alarma» 0 veces en la última semana. ¿Problemas? No o sí (si no, déjelo en blanco): esta alarma se activa con frecuencia durante la ejecución de un trabajo por lotes en particular. Resolvedores: ingenieros de confiabilidad del sitio	Comuníquese con el equipo de ingeniería de confiabilidad del sitio enviando un correo electrónico a *SRE@xyz.com* Cree un caso de AWS Premium Support para nuestros servicios de ECS y DynamoDB. Si es necesaria una acción INMEDIATA: compruebe si hay memoria o espacio EC2 libre en disco e informe al *XYZ* equipo por correo electrónico para que reinicie la instancia o ejecute una limpieza de registros. (si no es necesaria una acción inmediata, déjelo en blanco)

Descubrimiento de la carga de trabajo en la detección y respuesta a incidentes

AWS trabaja con usted para comprender lo más posible el contexto de su carga de trabajo. AWS Incident Detection and Response utiliza esta información para crear manuales que le ayuden durante los incidentes y los eventos AWS de servicio. La información requerida se incluye en. Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response Se recomienda registrar las cargas de trabajo en AppRegistry. Para obtener más información, consulte la Guía del usuario de AppRegistry .

Resultados clave:

- Información sobre la carga de trabajo, como la descripción de la carga de trabajo, los diagramas de arquitectura y los detalles de contacto y escalación.
- Detalles sobre cómo la carga de trabajo emplea AWS los servicios en cada AWS región.
- Información específica sobre cómo lo AWS apoya durante un evento de servicio.
- Alarmas utilizadas por su equipo que detectan un impacto crítico en la carga de trabajo.

Suscriba una carga de trabajo a Incident Detection and Response

Para suscribir una carga de trabajo a AWS Incident Detection and Response, cree un nuevo caso de soporte para cada carga de trabajo. Al crear el caso de soporte, tenga en cuenta lo siguiente:

- Para incorporar una carga de trabajo que está en una sola AWS cuenta, crea el caso de soporte desde la cuenta de la carga de trabajo o desde tu cuenta de pagador.
- Para incorporar una carga de trabajo que abarca varias AWS cuentas, crea el caso de soporte desde tu cuenta de pagador. En el cuerpo del caso de soporte, indica todas las cuentas IDs que deseas incorporar.

> **Important**
>
> Si crea un caso de soporte para suscribir una carga de trabajo a Incident Detection and Response desde una cuenta incorrecta, es posible que se produzcan retrasos y solicitudes de información adicional antes de poder suscribir sus cargas de trabajo.

Para suscribir una carga de trabajo

1. Vaya al AWS Support Centro y, a continuación, seleccione Crear caso, como se muestra en el siguiente ejemplo. Solo puede suscribir cargas de trabajo de cuentas que estén inscritas en Enterprise Support.

2. Complete el formulario del caso de soporte:

   - Seleccione Soporte técnico.
   - En Servicio, elija Detección y respuesta a incidentes.
   - En Categoría, elija Incorporar una nueva carga de trabajo.
   - En Gravedad, selecciona Guía general.

3. Introduce un asunto para este cambio. Por ejemplo:

   [A bordo] Detección y respuesta a incidentes de AWS - *workload_name*

4. Introduzca una descripción para este cambio. Por ejemplo, escriba «Esta solicitud es para incorporar una carga de trabajo a AWS Incident Detection and Response». Asegúrese de incluir la siguiente información en su solicitud:

   - Nombre de la carga de trabajo: el nombre de su carga de trabajo.
   - ID de cuenta: ID1 ID2 ID3,, etc. Estas son las cuentas que desea incorporar a AWS Incident Detection and Response.
   - Idioma: inglés o japonés.
   - Fecha de inicio de la suscripción: la fecha en la que desea iniciar la suscripción de AWS Incident Detection and Response.

5. En la sección Contactos adicionales (opcional), introduzca cualquier correo electrónico con el IDs que desee recibir correspondencia sobre esta solicitud.

   A continuación se muestra un ejemplo de la sección Contactos adicionales (opcional):

> **Important**
>
> Si no se añade el correo electrónico IDs en la sección Contactos adicionales (opcional), se podría retrasar el proceso de incorporación de AWS Incident Detection and Response.

6. Elija Enviar.

   Tras enviar la solicitud, puede añadir correos electrónicos adicionales de su organización. Para añadir correos electrónicos, responda al caso y, a continuación, añada el correo electrónico IDs en la sección Contactos adicionales (opcional).

   El siguiente es un ejemplo de la sección Contactos adicionales (opcional):

Tras crear un caso de soporte para la solicitud de suscripción, tenga preparados los dos documentos siguientes para continuar con el proceso de incorporación de la carga de trabajo:

- AWS diagrama de arquitectura de carga de trabajo.
- Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response: Complete toda la información del cuestionario relacionada con la carga de trabajo que va a incorporar. Si tienes que incorporar varias cargas de trabajo, crea un nuevo cuestionario de incorporación para cada carga de trabajo. Si tiene dudas sobre cómo completar el cuestionario de incorporación, póngase en contacto con su administrador técnico de cuentas (TAM).

> **Note**
>
> NO adjunte estos dos documentos al caso mediante la opción Adjuntar archivos. El equipo de detección y respuesta a incidentes de AWS responderá al caso con un enlace de Amazon Simple Storage Service Uploader para que cargue los documentos.

Para obtener información sobre cómo crear un caso con AWS Incident Detection and Response para solicitar cambios en una carga de trabajo integrada existente, consulte. Solicite cambios en una carga de trabajo integrada en Incident Detection and Response Para obtener información

sobre cómo eliminar una carga de trabajo, consulte. Elimine una carga de trabajo de la detección y respuesta a incidentes

Defina y configure las alarmas en la sección Detección y respuesta a incidentes

AWS trabaja con usted para definir métricas y alarmas a fin de proporcionar visibilidad del rendimiento de sus aplicaciones y su AWS infraestructura subyacente. Solicitamos que las alarmas cumplan los siguientes criterios al definir y configurar los umbrales:

- Las alarmas solo entran en el estado de «alarma» cuando se produce un impacto crítico en la carga de trabajo monitoreada (pérdida de ingresos o deterioro de la experiencia del cliente, lo que reduce significativamente el rendimiento) y requiere la atención inmediata del operador.
- Las alarmas también deben activar las soluciones especificadas para la carga de trabajo al mismo tiempo o antes de contactar con el equipo de gestión de incidentes. Los ingenieros de gestión de incidentes deberían colaborar con las personas encargadas de resolver las incidencias en el proceso de mitigación, no actuar como personal de primera línea y luego ponerse en contacto con usted.
- Los umbrales de alarma se deben establecer con un umbral y una duración adecuados, de modo que cada vez que se active una alarma, se lleve a cabo una investigación. Si una alarma oscila entre los estados «Alarma» y «OK», se está produciendo un impacto suficiente como para justificar la respuesta y la atención del operador.

Tipos de alarmas:

- Alarmas que muestran el nivel de impacto en el negocio y transmiten información relevante para una detección sencilla de fallas.
- Amazon CloudWatch canarios. Para obtener más información, consulte Canaries and X-Ray tracing y X-Ray.
- Alarmas agregadas (monitoreo de dependencias)

La siguiente tabla proporciona ejemplos de alarmas, todas ellas con el sistema CloudWatch de monitoreo.

Nombre de la métrica o umbral de alarma	ARN de alarma o ID de recurso	Si se activa esta alarma	Si está contratado, solicite un caso de soporte premium para estos servicios
Errores de API/ Número de errores >= 10 para 10 puntos de datos	arn:aws:cloudwatch:us-west- 2:0000000 00000:Alarma: E2 Lambda-Errores MPmim	El equipo de administradores de bases de datos (DBA) ha sido eliminado	Lambda, API Gateway
ServiceUnavailable (Código de estado HTTP 503) Número de errores >=3 para 10 puntos de datos (clientes diferentes) en un período de 5 minutos	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:http errorcode503	Boleto reducido al equipo de servicio	Lambda, API Gateway
ThrottlingException (Código de estado HTTP 400) Número de errores >=3 para 10 puntos	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:http errorcode400	Boleto eliminado para el equipo de servicio	EC2, Amazon Aurora

Nombre de la métrica o umbral de alarma	ARN de alarma o ID de recurso	Si se activa esta alarma	Si está contratado, solicite un caso de soporte premium para estos servicios
de datos (clientes diferentes) en un período de 5 minutos			

Para obtener más información, consulta Monitorización y observabilidad de la detección y respuesta a incidentes de AWS.

Resultados clave:

- Definición y configuración de las alarmas en sus cargas de trabajo.
- Completar los detalles de la alarma en el cuestionario de incorporación.

Temas

- Cree CloudWatch alarmas que se adapten a las necesidades de su empresa en materia de detección y respuesta a incidentes
- Cree CloudWatch alarmas en Incident Detection and Response con plantillas CloudFormation
- Ejemplos de casos de uso de CloudWatch alarmas en Incident Detection and Response

Cree CloudWatch alarmas que se adapten a las necesidades de su empresa en materia de detección y respuesta a incidentes

Al crear CloudWatch las alarmas de Amazon, hay varios pasos que puede seguir para asegurarse de que las alarmas se adapten mejor a las necesidades de su empresa.

> **Note**
>
> Para ver ejemplos de CloudWatch alarmas recomendadas para Servicios de AWS incorporarse a la detección y respuesta a incidentes, consulte las prácticas recomendadas en materia de detección y respuesta a incidentes en AWS re:Post.

Revise las CloudWatch alarmas propuestas

Revise las alarmas propuestas para asegurarse de que solo pasen al estado de «alarma» cuando la carga de trabajo monitoreada se vea afectada de manera crítica (pérdida de ingresos o deterioro de la experiencia del cliente, lo que reduce significativamente el rendimiento). Por ejemplo, ¿considera que esta alarma es lo suficientemente importante como para reaccionar inmediatamente si pasa al estado de «alarma»?

A continuación, se sugieren métricas que podrían representar un impacto empresarial crítico, por ejemplo, afectar a la experiencia de los usuarios finales con una aplicación:

- CloudFront: Para obtener más información, consulte las métricas de visualización CloudFront y funciones perimetrales.
- Equilibradores de carga de aplicaciones: se recomienda crear las siguientes alarmas para los balanceadores de carga de aplicaciones, si es posible:
  - HTTPCode_ELB_5xx_Count
  - HTTPCode_TARGET_5xx_Count

  Las alarmas anteriores le permiten monitorear las respuestas de los objetivos que están detrás del Application Load Balancer o detrás de otros recursos. Esto facilita la identificación del origen de los errores 5XX. Para obtener más información, consulte CloudWatch las métricas de su Application Load Balancer.
- Amazon API Gateway: si utiliza la WebSocket API en Elastic Beanstalk, considere la posibilidad de utilizar las siguientes métricas:
  - Tasas de error de integración (filtradas a 5XX errores)
  - Latencia de integración
  - Errores de ejecución

  Para obtener más información, consulta Supervisar la ejecución de la WebSocket API con CloudWatch métricas.

- Amazon Route 53: monitorea la EndPointUnhealthyENICountmétrica. Esta métrica es el número de interfaces de red elásticas en estado de recuperación automática. Este estado indica los intentos del solucionador de recuperar una o más de las interfaces de red de Amazon Virtual Private Cloud asociadas al punto final (especificadas por EndpointId). En el proceso de recuperación, el punto final funciona con una capacidad limitada. El punto final no puede procesar las consultas de DNS hasta que se haya recuperado por completo. Para obtener más información, consulte Supervisión de los puntos finales de Route 53 Resolver con Amazon CloudWatch.

Valide las configuraciones de sus alarmas

Tras confirmar que las alarmas propuestas se ajustan a las necesidades de su empresa, valide la configuración y el historial de las alarmas:

- Valide el umbral para que la métrica entre en estado de «alarma» en función de la tendencia gráfica de la métrica.
- Valide el período utilizado para sondear los puntos de datos. Los puntos de datos de sondeo a los 60 segundos ayudan a detectar los incidentes de forma temprana.
- Valide la DatapointToAlarmconfiguración. En la mayoría de los casos, se recomienda establecer este valor en 3 de 3 o 5 de 5. En caso de incidente, la alarma se activa después de 3 minutos si se establece en [métricas de 60 segundos con 3 de 3 DatapointToAlarm] o 5 minutos cuando se establece en [métricas de 60 segundos con 5 de 5 DatapointToAlarm]. Utilice esta combinación para eliminar las alarmas ruidosas.

> **Note**
>
> Las recomendaciones anteriores pueden variar en función del uso que se haga del servicio. Cada AWS servicio funciona de forma diferente dentro de una carga de trabajo. Además, el mismo servicio puede funcionar de manera diferente cuando se usa en varios lugares. Debe asegurarse de entender cómo su carga de trabajo utiliza los recursos que alimentan la alarma, así como los efectos ascendentes y descendentes.

Valide la forma en que sus alarmas gestionan los datos faltantes

Algunas fuentes de métricas no envían datos a CloudWatch intervalos regulares. En el caso de estas métricas, se recomienda tratar los datos faltantes como datos que no se filtran. Para obtener más

información, consulte Configurar el modo en que CloudWatch las alarmas tratan los datos faltantes y Evitar transiciones prematuras al estado de alarma.

Por ejemplo, si una métrica monitorea una tasa de errores y no hay errores, la métrica no muestra puntos de datos (nulos). Si configura la alarma para tratar los datos faltantes como ausentes, un solo punto de datos que infringe la seguridad seguido de dos puntos de datos sin datos (nulos) hace que la métrica pase al estado de «Alarma» (para 3 de cada 3 puntos de datos). Esto se debe a que la configuración de datos faltantes evalúa el último punto de datos conocido en el período de evaluación.

En los casos en que las métricas supervisan una tasa de error, si no se produce una degradación del servicio, se puede suponer que la ausencia de datos es algo positivo. Se recomienda tratar los datos faltantes como datos que no se infringen, de modo que los datos faltantes se traten como «correctos» y la métrica no entre en estado de «alarma» en un solo punto de datos.

Revisa el historial de cada alarma

Si el historial de una alarma muestra que pasa con frecuencia al estado de «Alarma» y, después, se recupera rápidamente, es posible que la alarma se convierta en un problema para usted. Asegúrese de ajustar la alarma para evitar ruidos o falsas alarmas.

Valide las métricas de los recursos subyacentes

Asegúrese de que sus métricas tengan en cuenta los recursos subyacentes válidos y utilicen las estadísticas correctas. Si se configura una alarma para revisar los nombres de recursos no válidos, es posible que la alarma no pueda rastrear los datos subyacentes. Esto podría provocar que la alarma entre en el estado de «Alarma».

Cree alarmas compuestas

Si proporciona a las operaciones de detección y respuesta a incidentes un gran número de alarmas para incorporarlas, es posible que se le pida que cree alarmas compuestas. Las alarmas compuestas reducen la cantidad total de alarmas que deben incorporarse.

Cree CloudWatch alarmas en Incident Detection and Response con plantillas CloudFormation

Para acelerar la incorporación a AWS Incident Detection and Response y reducir el esfuerzo necesario para crear alarmas, le AWS proporciona AWS CloudFormation plantillas. Estas plantillas

incluyen una configuración de alarma optimizada para los servicios comúnmente integrados, como Application Load Balancer, Network Load Balancer y Amazon. CloudFront

Cree alarmas con plantillas CloudWatch CloudFormation

1. Descargue una plantilla mediante los enlaces proporcionados:

NameSpac	Métricas	ComparisonOperator (Umbral)	Periodo	DatapointsToAlarm	TreatMissingData	Estadística	Enlace a la plantilla
Aplicación: Elastic Load Balancer	(m1+m2)/(m1+m2+mm4) *100 m1= _TARGET_xx_COUNT m2= _TARGET_xx_COUNT m3= _TARGET_xx_count m4= _TARGET_xx_count HTTPCode HTTPCode HTTPCode HTTPCode	LessThanThreshold(95)	60	3 de 3	desaparecido	Sum	Plantilla
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3 de 3	¿No está infringiendo	Media	Plantilla

NameSpac	Métricas	ComparisonOperator (Umbral)	Periodo	DatapointsToAlarm	TreatMissingData	Estadística	Enlace a la plantilla
Aplicación: Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 de 3	¿No está infringiendo	Máximo	Plantilla
Elastic Load Balancer de red	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 de 3	¿No está infringiendo	Máximo	Plantilla

2. Revise el archivo JSON descargado para asegurarse de que cumple con los procesos de operación y seguridad de su organización.
3. Crea una CloudFormation pila:

> **Note**
>
> Los siguientes pasos utilizan el proceso de creación de CloudFormation pilas estándar. Para ver los pasos detallados, consulte Crear una pila en la CloudFormation consola de AWS.

   a. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
   b. Seleccione Creación de pila.
   c. Seleccione La plantilla está lista y, a continuación, cargue el archivo de plantilla desde su carpeta local.

      El siguiente es un ejemplo de la pantalla Crear pila.

   d. Elija Siguiente.
   e. Introduzca la siguiente información necesaria:
      - AlarmNameConfigy AlarmDescriptionConfig: Introduce un nombre y una descripción para la alarma.

- ThresholdConfig: Revise el valor límite para que cumpla con los requisitos de su solicitud.

- Distribución IDConfig: asegúrate de que el identificador de distribución apunte a los recursos correctos de la cuenta en la que vas a crear la AWS CloudFormation pila.

f. Elija Siguiente.

g. Revisa los valores predeterminados de los DatapointsToAlarmConfigcampos PeriodConfigEvalutionPeriodConfig, y. Se recomienda utilizar los valores predeterminados para estos campos. Si es necesario, puede realizar ajustes para cumplir con los requisitos de su aplicación.

h. Si lo desea, introduzca las etiquetas y la información de notificación de SNS según sea necesario. Se recomienda activar la protección de terminación para evitar la eliminación accidental de la alarma. Para activar la protección de terminación, selecciona el botón de opción Activado, como se muestra en el siguiente ejemplo:

i. Elija Siguiente.

j. Revisa la configuración de tu pila y, a continuación, selecciona Crear pila.

k. Tras crear la pila, verás la alarma en la lista de CloudWatch alarmas de Amazon, como se muestra en el siguiente ejemplo:

4. Una vez que haya creado todas las alarmas en la cuenta y AWS región correctas, notifíquelo a su administrador técnico de cuentas (TAM). El equipo de detección y respuesta a incidentes de AWS revisa el estado de las nuevas alarmas y continúa con la incorporación.

Ejemplos de casos de uso de CloudWatch alarmas en Incident Detection and Response

Los siguientes casos de uso proporcionan ejemplos de cómo puedes usar CloudWatch las alarmas de Amazon en Incident Detection and Response. Estos ejemplos muestran cómo se pueden configurar CloudWatch las alarmas para monitorear las métricas y los umbrales clave en varios AWS servicios, lo que le permite identificar y responder a posibles problemas que podrían afectar a la disponibilidad y el rendimiento de sus aplicaciones y cargas de trabajo.

Ejemplo de caso de uso A: Application Load Balancer

Puede crear la siguiente CloudWatch alarma que indique un posible impacto en la carga de trabajo. Para ello, debe crear una métrica matemática que emita una alarma cuando las conexiones correctas caigan por debajo de un determinado umbral. Para ver las CloudWatch métricas disponibles, consulte CloudWatch las métricas de su Application Load Balancer

Métrica: `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/Aplicación ELB

ComparisonOperator(Umbral): inferior a x (x = umbral del cliente).

Periodo: 60 segundos

DatapointsToAlarm: 3 de 3

Tratamiento de datos faltantes: trate los datos faltantes como una violación.

Estadística: Sum

El siguiente diagrama muestra el flujo del caso de uso A:

Ejemplo de caso de uso B: Amazon API Gateway

Puede crear la siguiente CloudWatch alarma que indique el posible impacto en la carga de trabajo. Para ello, debe crear una métrica compuesta que emita una alarma cuando hay una latencia alta o un número medio alto de errores 4XX en la API Gateway. Para ver las métricas disponibles, consulte Dimensiones y métricas de Amazon API Gateway

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

NameSpace: AWS/Puerta de enlace API

ComparisonOperator(Umbral): superior a (los umbrales de x o y del cliente)

Periodo: 60 segundos

DatapointsToAlarm: 1 de cada 1

Tratamiento de datos faltantes: trate los datos faltantes como si no se tratara de una violación.

Estadística:

El siguiente diagrama muestra el flujo del caso de uso B:

Ejemplo de caso de uso C: Amazon Route 53

Puede supervisar sus recursos mediante la creación de comprobaciones de estado de Route 53 que se utilizan CloudWatch para recopilar y procesar datos sin procesar para convertirlos en métricas legibles y prácticamente en tiempo real. Puede crear la siguiente CloudWatch alarma que indique el posible impacto en la carga de trabajo. Puede usar las CloudWatch métricas para crear una alarma que se active cuando supere el umbral establecido. Para ver las CloudWatch métricas disponibles, consulte las CloudWatch métricas de las comprobaciones de estado de Route 53

Métrica: `R53-HC-Success`

NameSpace: AWS/Ruta 53

Umbral HealthCheckStatus: HealthCheckStatus < x para 3 puntos de datos en 3 minutos (es x el umbral del cliente)

Periodo: 1 minuto

DatapointsToAlarm: 3 de 3

Tratamiento de datos faltantes: trate los datos faltantes como una violación.

Estadística: Minimum

El siguiente diagrama muestra el flujo del caso de uso C:

Ejemplo de caso de uso D: Supervise una carga de trabajo con una aplicación personalizada

Es fundamental que te tomes el tiempo necesario para definir un chequeo de estado adecuado en este escenario. Si solo compruebas que el puerto de una aplicación esté abierto, significa que no has comprobado que la aplicación esté funcionando. Además, realizar una llamada a la página de inicio

de una aplicación no es necesariamente la forma correcta de determinar si la aplicación funciona. Por ejemplo, si una aplicación depende tanto de una base de datos como de Amazon Simple Storage Service (Amazon S3), la comprobación de estado debe validar todos los elementos. Una forma de hacerlo es crear una página web de monitoreo, como /monitor. La página web de monitoreo realiza una llamada a la base de datos para asegurarse de que puede conectarse y obtener datos. Además, la página web de monitoreo hace una llamada a Amazon S3. A continuación, diriges la comprobación de estado del balanceador de cargas a la página /monitor.

El siguiente diagrama muestra el flujo del caso de uso D:

Incorpore alarmas en AWS Incident Detection and Response

AWS Incident Detection and Response admite la ingesta de alarmas a través de Amazon EventBridge. En esta sección se describe cómo integrar AWS Incident Detection and Response con diferentes herramientas de monitoreo del rendimiento de las aplicaciones (APM) CloudWatch, incluida Amazon, APMs con integración directa con Amazon EventBridge (por ejemplo, Datadog y New Relic) y APMs sin integración directa con Amazon. EventBridge Para obtener una lista completa de las integraciones APMs con Amazon directamente EventBridge, consulta EventBridgelas integraciones de Amazon.

Temas

- Proporcione acceso para la recepción de alertas a la detección y respuesta a incidentes
- Integre la detección y respuesta a incidentes con Amazon CloudWatch
- Ingiera alarmas desde las APMs que se integró directamente con Amazon EventBridge
- Ejemplo: integre las notificaciones de Datadog y Splunk
- Usa webhooks para ingerir alarmas APMs sin necesidad de una integración directa con Amazon EventBridge

Proporcione acceso para la recepción de alertas a la detección y respuesta a incidentes

Para permitir que AWS Incident Detection and Response ingiera las alarmas de su cuenta, instale el rol `AWSServiceRoleForHealth_EventProcessor` vinculado a servicios (SLR). AWS asume que la SLR crea una regla EventBridge gestionada por Amazon. La regla administrada envía

notificaciones desde sus cuentas a AWS Incident Detection and Response. Para obtener información sobre esta SLR, incluida la política AWS administrada asociada, consulte Uso de funciones vinculadas a servicios en la Guía del AWS Health usuario.

Puede instalar este rol vinculado a un servicio en su cuenta siguiendo las instrucciones de Crear un rol vinculado a un servicio en la Guía del usuario.AWS Identity and Access Management O bien, puede usar el siguiente comando de la interfaz de línea de comandos de AWS (AWS CLI):

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

Resultados clave

- La función vinculada al servicio se instaló correctamente en su cuenta.

Información relacionada

Para obtener más información, consulte los temas siguientes:

- Uso de funciones vinculadas a servicios para AWS Health
- Crear un rol vinculado a un servicio
- Política gestionada por AWS: AWSHealth_EventProcessorServiceRolePolicy

Integre la detección y respuesta a incidentes con Amazon CloudWatch

AWS Incident Detection and Response utiliza el rol vinculado al servicio (SLR) que activó durante el aprovisionamiento del acceso para crear una regla EventBridge administrada por Amazon en su cuenta denominada. AWS `AWSHealthEventProcessor-DO-NOT-DELETE` Incident Detection and Response usa esta regla para ingerir CloudWatch las alarmas de Amazon de tus cuentas. No es necesario tomar medidas adicionales para ingerir las alarmas desde. CloudWatch

Ingiera alarmas desde las APMs que se integró directamente con Amazon EventBridge

La siguiente ilustración muestra el proceso de envío de notificaciones a las herramientas de AWS Incident Detection and Response desde las herramientas de monitoreo del rendimiento de las aplicaciones (APM) que tienen una integración directa con Amazon EventBridge, como Datadog y

Splunk. Para obtener una lista completa de las APMs que tienen integración directa EventBridge, consulta EventBridge las integraciones de Amazon.

Siga los siguientes pasos para configurar la integración con AWS Incident Detection and Response. Antes de realizar estos pasos, compruebe que el rol AWS vinculado al servicio (SLR) `AWSServiceRoleForHealth_EventProcessor` esté instalado en sus cuentas.

Configure la integración con AWS Incident Detection and Response

Debe completar los siguientes pasos para cada AWS cuenta y AWS región. Las alertas deben provenir de la AWS cuenta y la AWS región en las que residen los recursos de la aplicación.

1. Configura cada una de tus fuentes de eventos APMs como EventBridge socio de Amazon (por ejemplo,`aws.partner/my_apm/integrationName`). Para obtener instrucciones sobre cómo configurar tu APM como fuente de eventos, consulta Recibir eventos de un socio de SaaS de Amazon. EventBridge Esto crea un bus de eventos asociado en tu cuenta.
2. Realice una de las siguientes acciones:
   - (Método recomendado) Crea un bus de EventBridge eventos personalizado. AWS Incident Detection and Response instala un bus de reglas administradas (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) a través de la `AWSServiceRoleForHealth_EventProcessor` SLR. La fuente de la regla es el bus de eventos personalizado. El destino de la regla es AWS Incident Detection and Response. La regla coincide con el patrón de ingesta de eventos de APM de terceros.
   - (Método alternativo) Utilice el bus de eventos predeterminado en lugar de un bus de eventos personalizado. El bus de eventos predeterminado requiere que la regla administrada envíe alertas de APM a AWS Incident Detection and Response.
3. Cree una AWS Lambdafunción (por ejemplo`My_APM-AWSIncidentDetectionResponse-LambdaFunction`) para transformar los eventos del bus de eventos de su socio. Los eventos transformados coinciden con la regla gestionada`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
   a. Los eventos transformados incluyen un identificador único de detección y respuesta a incidentes de AWS y establecen el origen y el tipo de detalle del evento en los valores requeridos. El patrón coincide con la regla administrada.
   b. Establezca el objetivo de la función Lambda en el bus de eventos personalizado creado en el paso 2 (método recomendado) o en el bus de eventos predeterminado.

4. Cree una EventBridge regla y defina los patrones de eventos que coincidan con la lista de eventos que quiere enviar a AWS Incident Detection and Response. El origen de la regla es el bus de eventos asociado que defina en el paso 1 (por ejemplo, aws). partner/my_apm/integrationName). El objetivo de la regla es la función Lambda que se define en el paso 3 (por ejemplo,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`). Para obtener instrucciones sobre cómo definir tu EventBridge regla, consulta las reglas de Amazon EventBridge .

Para ver ejemplos sobre cómo configurar la integración de un bus de eventos asociado para usarla con AWS Incident Detection and Response, consulteEjemplo: integre las notificaciones de Datadog y Splunk.

Ejemplo: integre las notificaciones de Datadog y Splunk

Este ejemplo proporciona pasos detallados para integrar las notificaciones de Datadog y Splunk en AWS Incident Detection and Response.

Temas

- Paso 1: Configura tu APM como fuente de eventos en Amazon EventBridge
- Paso 2: Crea un bus de eventos personalizado
- Paso 3: Crea una AWS Lambda función para la transformación
- Paso 4: Crea una EventBridge regla de Amazon personalizada

Paso 1: Configura tu APM como fuente de eventos en Amazon EventBridge

Configure cada una de las APMs suyas como fuente de eventos en Amazon EventBridge en su cuenta de AWS. Para obtener instrucciones sobre cómo configurar tu APM como fuente de eventos, consulta las instrucciones de configuración de la fuente de eventos para tu herramienta en Amazon EventBridge Partners.

Al configurar su APM como fuente de eventos, puede transferir las notificaciones de su APM a un bus de eventos de su cuenta de AWS. Tras la configuración, AWS Incident Detection and Response puede iniciar el proceso de administración de incidentes cuando el bus del evento recibe un evento. Este proceso añade Amazon EventBridge como destino en tu APM.

Paso 2: Crea un bus de eventos personalizado

Se recomienda utilizar un bus de eventos personalizado. AWS Incident Detection and Response utiliza el bus de eventos personalizado para incorporar eventos transformados. Una AWS Lambda función transforma el evento del bus de eventos asociado y lo envía al bus de eventos personalizado. AWS Incident Detection and Response instala una regla administrada para ingerir eventos del bus de eventos personalizado.

Puede usar el bus de eventos predeterminado en lugar de un bus de eventos personalizado. AWS Incident Detection and Response modifica la regla administrada para que se ingiera desde el bus de eventos predeterminado en lugar de hacerlo desde uno personalizado.

Cree un bus de eventos personalizado en su AWS cuenta:

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/
2. Elige Buses, Event Bus.
3. En Autobús de eventos personalizado, selecciona Crear.
4. Introduzca un nombre para el autobús de eventos en Nombre. El formato recomendado es APMName- AWSIncidentDetectionResponse-EventBus.

   Como ejemplo, utilice uno de los siguientes si utiliza Datadog o Splunk:

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

Paso 3: Crea una AWS Lambda función para la transformación

La función Lambda transforma los eventos entre el bus de eventos asociado en el paso 1 y el bus de eventos personalizado (o predeterminado) del paso 2. La transformación de la función Lambda coincide con la regla gestionada de detección y respuesta a incidentes de AWS.

Cree una AWS Lambda función en su cuenta AWS

1. Abre la página de funciones en la AWS Lambda consola.
2. Elija Crear función.
3. Seleccione la pestaña Autor desde cero.
4. En Nombre de función, introduzca un nombre con el formato`APMName-AWSIncidentDetectionResponse-LambdaFunction`.

Los siguientes son ejemplos de Datadog y Splunk:

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

5. Para Runtime, introduzca Python 3.10.
6. Deje los campos restantes con los valores predeterminados. Elija Crear función.
7. En la página de edición de código, sustituya el contenido predeterminado de la función Lambda por la función de los siguientes ejemplos de código.

   Anote los comentarios que comienzan por # en los siguientes ejemplos de código. Estos comentarios indican qué valores se deben cambiar.

   Plantilla de código de transformación de Datadog:

```
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'])
```

Plantilla de código de transformación de Splunk:

```
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. Elija Implementar.
9. Añada PutEventspermiso a la función de ejecución de Lambda para el bus de eventos al que va a enviar los datos transformados:
   a. Abra la página de funciones en la AWS Lambda consola.
   b. Seleccione la función y, a continuación, elija Permisos en la pestaña Configuración.
   c. En Función de ejecución, seleccione el nombre de la función para abrir la función de ejecución en la AWS Identity and Access Management consola.
   d. En Políticas de permisos, seleccione el nombre de la política existente para abrirla.
   e. En Permisos definidos en esta política, elija Editar.
   f. En la página del editor de políticas, selecciona Añadir nueva declaración:
   g. El editor de políticas agrega una nueva declaración en blanco similar a la siguiente
   h. Sustituya la nueva declaración generada automáticamente por la siguiente:

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

   i. El recurso es el ARN del bus de eventos personalizado que creó Paso 2: Crea un bus de eventos personalizado o el ARN del bus de eventos predeterminado si utiliza el bus de eventos predeterminado en el código Lambda.

10. Revise y confirme que se hayan agregado los permisos necesarios al rol.
11. Seleccione Establecer esta nueva versión como predeterminada y, a continuación, seleccione Guardar cambios.

¿Qué se necesita para transformar una carga útil?

Los siguientes pares clave y valor de JSON son necesarios en los eventos de bus de eventos ingeridos por AWS Incident Detection and Response.

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

Los siguientes ejemplos muestran un evento de un bus de eventos asociado antes y después de su transformación.

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

Tenga en cuenta que antes de que se transforme el evento, `detail-type` indica el APM del que proviene la alerta, la fuente es de un APM asociado y la `incident-detection-response-identifier` clave no está presente.

La función Lambda transforma el evento anterior y lo coloca en el bus de eventos predeterminado o personalizado de destino. La carga útil transformada ahora incluye los pares clave-valor necesarios.


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

Tenga en cuenta que ahora `detail-type` es`ams.monitoring/generic-apm`, la fuente es ahora y`GenericAPMEvent`, en detalle, hay un nuevo par clave:valor:. `incident-detection-response-identifier`

En el ejemplo anterior, el `incident-detection-response-identifier` valor se toma del nombre de la alerta que aparece debajo de la ruta. `$.detail.meta.monitor.name` Las rutas de los nombres de alerta de APM son diferentes de un APM a otro. La función Lambda debe modificarse para tomar el nombre de la alarma de la ruta JSON del evento asociado correcto y usarlo como valor. `incident-detection-response-identifier`

Cada nombre único que aparece en el `incident-detection-response-identifier` se proporciona al equipo de detección y respuesta a incidentes de AWS durante la incorporación. Los eventos que tienen un nombre desconocido `incident-detection-response-identifier` no se procesan.

Paso 4: Crea una EventBridge regla de Amazon personalizada

El bus de eventos asociado creado en el paso 1 requiere que usted cree una EventBridge regla. La regla envía los eventos deseados desde el bus de eventos asociado a la función Lambda creada en el paso 3.

Para obtener instrucciones sobre cómo definir tu EventBridge regla, consulta EventBridge las reglas de Amazon.

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/
2. Elige Rules y, a continuación, selecciona el bus de eventos asociado a tu APM. Los siguientes son ejemplos de autobuses de eventos asociados:
   - Datadog: AWS. partner/datadog.com/eventbus-nombre
   - Splunk: AWS. partner/signalfx.com/RandomString
3. Seleccione Crear regla para crear una nueva EventBridge regla.
4. Para el nombre de la regla, introduzca un nombre con el siguiente formato y`APMName-AWS Incident Detection and Response-EventBridgeRule`, a continuación, seleccione Siguiente. A continuación se muestran ejemplos de nombres:
   - Datadog: Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk: Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. En Origen del evento, seleccione eventos de AWS o eventos de EventBridge socios.
6. Deje el evento de muestra y el método de creación como valores predeterminados.
7. En Patrón de eventos, elija lo siguiente:
   a. Fuente del evento: EventBridge socios.
   b. Socio: seleccione su socio de APM.
   c. Tipo de evento: Todos los eventos.

   Los siguientes son ejemplos de patrones de eventos:

   Ejemplo de patrón de eventos de Datadog

   Ejemplo de patrón de eventos de Splunk

8. En Targets, elige lo siguiente:
   a. Tipos de objetivos: AWS servicio
   b. Seleccione un objetivo: elija la función Lambda.

c. Función: el nombre de la función Lambda que creó en el paso 2.

9. Seleccione Siguiente, Guardar regla.

Usa webhooks para ingerir alarmas APMs sin necesidad de una integración directa con Amazon EventBridge

AWS Incident Detection and Response admite el uso de webhooks para la ingesta de alarmas de terceros APMs que no tienen una integración directa con Amazon. EventBridge

Para ver una lista de integraciones directas APMs con Amazon EventBridge, consulta EventBridge Integraciones de Amazon.

Siga los siguientes pasos para configurar la integración con AWS Incident Detection and Response. Antes de realizar estos pasos, compruebe que la regla gestionada por AWS, AWSHealthEventProcessorEventSource-DO-NOT-DELETE, esté instalada en sus cuentas

Ingiera eventos mediante webhooks

1. Defina una Amazon API Gateway para aceptar la carga útil de su APM.
2. Defina una AWS Lambda función de autorización mediante un token de autenticación, como se muestra en la ilustración anterior.
3. Defina una segunda función Lambda para transformar y añadir el identificador de detección y respuesta a incidentes de AWS a su carga útil. También puede usar esta función para filtrar los eventos que desee enviar a AWS Incident Detection and Response.
4. Configura tu APM para enviar notificaciones a la URL generada desde la API Gateway.

Gestione las cargas de trabajo en la detección y respuesta a incidentes

Una parte clave de una gestión eficaz de incidentes es contar con los procesos y procedimientos adecuados para incorporar, probar y mantener las cargas de trabajo supervisadas. En esta sección se describen los pasos esenciales, como la elaboración de manuales y planes de respuesta exhaustivos para guiar a sus equipos ante los incidentes, probar y validar exhaustivamente las nuevas cargas de trabajo antes de incorporarlas, solicitar cambios para actualizar la supervisión de las cargas de trabajo y desvincular adecuadamente las cargas de trabajo cuando sea necesario.

Temas

- Desarrolle manuales y planes de respuesta para responder a un incidente en el marco de la detección y respuesta a incidentes
- Pruebe las cargas de trabajo integradas en Detección y respuesta a incidentes
- Solicite cambios en una carga de trabajo integrada en Incident Detection and Response
- Evite que las alarmas activen la detección y respuesta a incidentes
- Elimine una carga de trabajo de la detección y respuesta a incidentes

Desarrolle manuales y planes de respuesta para responder a un incidente en el marco de la detección y respuesta a incidentes

Incident Detection and Response utiliza la información recopilada de su cuestionario de incorporación para desarrollar manuales y planes de respuesta para la gestión de los incidentes que afecten a sus cargas de trabajo. Los manuales documentan las medidas que toman los administradores de incidentes al responder a un incidente. Se asigna un plan de respuesta a al menos una de sus cargas de trabajo. El equipo de gestión de incidentes crea estas plantillas a partir de la información proporcionada por usted durante el descubrimiento de la carga de trabajo. Los planes de respuesta son plantillas de documentos AWS Systems Manager (SSM) que se utilizan para desencadenar incidentes. Para obtener más información sobre los documentos SSM, consulte AWS Systems Manager Documentos. Para obtener más información sobre Incident Manager, consulte ¿Qué es? Administrador de incidentes de AWS Systems Manager

Resultados clave:

- Finalización de la definición de la carga de trabajo en AWS Incident Detection and Response.
- Finalización de las alarmas, los manuales de ejecución y la definición del plan de respuesta en AWS Incident Detection and Response.

También puede descargar un ejemplo del Runbook de detección y respuesta a incidentes de AWS: aws-idr-runbook-example.zip.

Ejemplo de manual:

```
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.
```

Pruebe las cargas de trabajo integradas en Detección y respuesta a incidentes

> **Note**
>
> El AWS Identity and Access Management usuario o rol que utilice para las pruebas de alarmas debe tener `cloudwatch:SetAlarmState` permiso.

El último paso del proceso de incorporación consiste en dedicar un día de juego a tu nueva carga de trabajo. Una vez completada la ingesta de alarmas, AWS Incident Detection and Response confirmará la fecha y la hora que elija para empezar el día de juego.

Su día de juego tiene dos objetivos principales:

- Validación funcional: confirma que AWS Incident Detection and Response puede recibir correctamente sus eventos de alarma. Además, la validación funcional confirma que los eventos de alarma activan los manuales de ejecución adecuados y cualquier otra acción deseada, como la creación automática de cajas si la seleccionó durante la ingesta de alarmas.
- Simulación: El día de juego es una simulación completa de lo que puede ocurrir durante un incidente real. AWS Incident Detection and Response sigue los pasos del manual prescrito para

proporcionarle información sobre cómo podría desarrollarse un incidente real. El día del partido es una oportunidad para hacer preguntas o perfeccionar las instrucciones a fin de mejorar la participación.

Durante la prueba de alarma, AWS Incident Detection and Response trabaja con usted para solucionar cualquier problema identificado.

CloudWatch alarmas

AWS Incident Detection and Response comprueba CloudWatch las alarmas de Amazon monitorizando el cambio de estado de la alarma. Para ello, cambie manualmente la alarma al estado de alarma mediante el AWS Command Line Interface. También puede acceder al AWS CLI desde AWS CloudShell. AWS Incident Detection and Response le proporciona una lista de AWS CLI comandos para que los utilice durante las pruebas.

Ejemplo de AWS CLI comando para configurar un estado de alarma:

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

Para obtener más información sobre cómo cambiar manualmente el estado de CloudWatch las alarmas, consulte SetAlarmState.

Para obtener más información sobre los permisos necesarios para las operaciones de la CloudWatch API, consulta la referencia de CloudWatch permisos de Amazon.

Alarmas APM de terceros

Las cargas de trabajo que utilizan una herramienta de monitoreo del rendimiento de las aplicaciones (APM) de terceros, como Datadog, Splunk, New Relic o Dynatrace, requieren instrucciones diferentes para simular una alarma. Al comienzo del día de juego, AWS Incident Detection and Response le solicita que cambie temporalmente los umbrales de alarma o los operadores de comparación para forzar la alarma al estado de ALARMA. Este estado activa una carga útil para AWS Incident Detection and Response.

Resultados clave

Resultados clave:

- La entrada de la alarma se ha realizado correctamente y la configuración de la alarma es correcta.
- AWS Incident Detection and Response crea y recibe correctamente las alarmas.
- Se crea un caso de soporte para su contratación y se notifica a los contactos prescritos.
- AWS Incident Detection and Response puede contactar con usted a través de los medios de conferencia prescritos.
- Se resuelven todas las alarmas y los casos de asistencia generados durante el día del partido.
- Se envía un correo electrónico de Go-Live confirmando que AWS Incident Detection and Response está supervisando su carga de trabajo.

Solicite cambios en una carga de trabajo integrada en Incident Detection and Response

Para solicitar cambios en una carga de trabajo incorporada, complete los siguientes pasos para crear un caso de soporte con AWS Incident Detection and Response.

1. Vaya al AWS Support Centro y, a continuación, seleccione Crear caso, como se muestra en el siguiente ejemplo:

2. Elija Técnico.
3. En Servicio, elija Detección y respuesta a incidentes.
4. En Categoría, elija Solicitud de cambio de carga de trabajo.
5. En Gravedad, selecciona Guía general.
6. Introduzca un asunto para este cambio. Por ejemplo:

   Detección y respuesta a incidentes de AWS - *workload_name*
7. Introduzca una descripción para este cambio. Por ejemplo, escriba «Esta solicitud se refiere a cambios en una carga de trabajo existente integrada en AWS Incident Detection and Response». Asegúrese de incluir la siguiente información en su solicitud:

   - Nombre de la carga de trabajo: el nombre de su carga de trabajo.
   - ID de cuenta: ID1 ID2 ID3,, etc.
   - Detalles del cambio: introduce los detalles del cambio solicitado.

8. En la sección Contactos adicionales (opcional), introduce cualquier correo electrónico con el IDs que desees recibir correspondencia sobre este cambio.

   El siguiente es un ejemplo de la sección Contactos adicionales: opcional.

   > **Important**
   >
   > Si no se añade el correo electrónico IDs en la sección Contactos adicionales (opcional), se podría retrasar el proceso de cambio.

9. Elija Enviar.

   Después de enviar la solicitud de cambio, puede añadir correos electrónicos adicionales de su organización. Para añadir correos electrónicos, selecciona los detalles de Responder en caso de que se trate, como se muestra en el siguiente ejemplo:

   A continuación, añade el correo electrónico IDs en la sección Contactos adicionales (opcional).

   El siguiente es un ejemplo de la página de respuesta que muestra dónde puede introducir correos electrónicos adicionales.

Evite que las alarmas activen la detección y respuesta a incidentes

Especifique cuáles de sus alarmas de carga de trabajo integradas se activan con la supervisión de AWS Incident Detection and Response suprimiéndolas temporalmente o de forma programada. Por ejemplo, puede suprimir temporalmente las alarmas de carga de trabajo durante el mantenimiento planificado para evitar que las alarmas activen la función de detección y respuesta a incidentes. O bien, puede suprimir las alarmas de forma programada si tiene actividad de reinicio diaria. Puede suprimir las alarmas en la fuente de la alarma, como Amazon CloudWatch, o puede enviar una solicitud de cambio de carga de trabajo.

Temas

- Suprima las alarmas en la fuente de alarma
- Envíe una solicitud de cambio de carga de trabajo para suprimir las alarmas

- Tutorial: Utilice una función matemática métrica para suprimir una alarma
- Tutorial: Elimine una función matemática métrica para desactivar una alarma

Suprima las alarmas en la fuente de alarma

Especifique qué alarmas se activan con la detección y respuesta a incidentes y cuándo lo hacen suprimiendo las alarmas en la fuente de alarma.

Temas

- Utilice una función matemática métrica para suprimir una alarma CloudWatch
- Elimine una función matemática métrica para desactivar una alarma CloudWatch
- Ejemplos de funciones matemáticas métricas y casos de uso asociados
- Suprima las alarmas de un APM de terceros

Utilice una función matemática métrica para suprimir una alarma CloudWatch

Para suprimir la supervisión de la detección de incidentes y la respuesta a CloudWatch las alarmas de Amazon, utiliza una función matemática métrica para evitar que CloudWatch las alarmas entren en el `ALARM` estado durante un período designado.

> **Note**
>
> Si desactivas las acciones de alarma en una CloudWatch alarma, no se suprime la supervisión de las alarmas mediante la detección y la respuesta a incidentes. Los cambios de estado de alarma se ingieren a través de Amazon EventBridge, no a través de acciones CloudWatch de alarma.

Para utilizar una función matemática métrica para suprimir una CloudWatch alarma, complete los siguientes pasos:

1. Inicie sesión en AWS Management Console y abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Seleccione Alarmas y, a continuación, localice la alarma a la que desee añadir la función matemática métrica.

3. En la sección de matemáticas métricas, selecciona Editar.
4. Elija Añadir matemática, comience con una expresión vacía.
5. Introduce tu expresión matemática y, a continuación, selecciona Aplicar.
6. Deseleccione la métrica existente que la alarma monitorizó.
7. Seleccione la expresión que acaba de crear y, a continuación, elija Seleccionar métrica.
8. Elija Saltar a la vista previa y crear.
9. Revisa los cambios para asegurarte de que la función matemática métrica se aplica según lo previsto y, a continuación, selecciona Actualizar alarma.

Para ver un ejemplo paso a paso de cómo suprimir una CloudWatch alarma con una función matemática métrica, consulteTutorial: Utilice una función matemática métrica para suprimir una alarma.

Para obtener más información sobre la sintaxis y las funciones disponibles, consulte Funciones y sintaxis de las matemáticas métricas en la Guía del CloudWatch usuario de Amazon.

Elimine una función matemática métrica para desactivar una alarma CloudWatch

Desactiva una CloudWatch alarma quitando la función matemática métrica. Para eliminar una función matemática métrica de una alarma, complete los siguientes pasos:

1. Inicie sesión en AWS Management Console y abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Seleccione Alarmas y, a continuación, localice la alarma o alarmas de las que desee eliminar la expresión matemática métrica.
3. En la sección de matemáticas métricas, elija Editar.
4. Para eliminar la métrica de la alarma, selecciona Editar en la métrica y, a continuación, pulsa el botón x situado junto a la expresión matemática métrica.
5. Seleccione la métrica original y, a continuación, elija Seleccionar métrica.
6. Elija Saltar a la vista previa y crear.
7. Revisa los cambios para asegurarte de que la función matemática métrica se aplica según lo previsto y, a continuación, selecciona Actualizar alarma.

Ejemplos de funciones matemáticas métricas y casos de uso asociados

La siguiente tabla contiene ejemplos de funciones matemáticas métricas, junto con los casos de uso asociados y una explicación de cada componente métrico.

Función matemática métrica	Caso de uso	Explicación
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	Desactive la alarma todos los martes entre la 1:00 y las 3:00 a.m. UTC sustituyendo los puntos de datos reales por 0 durante este período.	• DÍA (m1) == 2: Garantiza que sea martes (lunes = 1, domingo = 7). • HORA (m1) >= 1 && HORA (m1) > 3: Especific a el intervalo de tiempo comprendido entre la 1 a. m. y las 3 a. m. UTC. • IF (condition, value_if_ true, value_if_false): Si las condiciones son verdadera s, sustituya el valor métrico por 0. De lo contrario, devuelve el valor original (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	Suprima la alarma entre las 11:00 p. m. y las 4:00 a. m. UTC, todos los días sustituye ndo los puntos de datos reales por 0 durante este período.	• HORA (m1) >= 23: captura las horas que comienzan a las 23:00 UTC. • HORA (m1) < 4: captura las horas hasta las 04:00 UTC (pero sin incluirlas). • ||: El OR lógico garantiza que la condición se aplique en dos rangos: a altas horas de la noche y a primera hora de la mañana. • IF (condition, value_if_true, value_if_false): devuelve

Función matemática métrica	Caso de uso	Explicación
		0 durante el intervalo de tiempo especificado. Conserva el valor métrico original m1 fuera de ese rango.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	Desactive las alarmas todos los días entre las 11:00 y las 13:00, hora peninsular española, sustituyendo los puntos de datos reales por 0 durante este período.	• HORA (m1) >= 11 && HORA (m1) < 13: captura el intervalo de tiempo comprendido entre las 11:00 y las 13:00 UTC. • IF (condition, value_if_true, value_if_false): si la condición es verdadera (por ejemplo, la hora está entre las 11:00 y las 13:00 UTC), devuelve 0. Si la condición es falsa, conserva el valor métrico original (m1).

Función matemática métrica	Caso de uso	Explicación
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	Desactive la alarma todos los martes entre la 1:00 y las 3:00 a. m. UTC; para ello, sustituya los puntos de datos reales por 99 durante este período.	• DÍA (m1) == 2: Garantiza que sea martes (lunes = 1, domingo = 7). • HORA (m1) >= 1 && HORA (m1) < 3: Especific a el intervalo de tiempo comprendido entre la 1 a. m. y las 3 a. m. UTC. • IF (condition, value_if_ true, value_if_false): si las condiciones son verdadera s, sustituye el valor métrico por 99. De lo contrario, devuelve el valor original (m1).

Función matemática métrica	Caso de uso	Explicación
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	Suprima la alarma todos los días entre las 23:00 y las 16:00, hora peninsular española, sustituyendo los puntos de datos reales por 100 durante este período.	• HORA (m1) >= 23: captura las horas que comienzan a las 23:00 UTC. • HORA (m1) < 4: captura las horas hasta las 04:00 UTC (pero sin incluirlas). • ||: El OR lógico garantiza que la condición se aplique en dos rangos: a altas horas de la noche y a primera hora de la mañana. • IF (condition, value_if_true, value_if_false): devuelve 100 durante el intervalo de tiempo especificado. Conserva el valor métrico original m1 fuera de ese rango.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	Desactive las alarmas todos los días entre las 11:00 y las 13:00, hora peninsular española, sustituyendo los puntos de datos reales por 99 durante este período.	• HORA (m1) >= 11 && HORA (m1) < 13: captura el intervalo de tiempo comprendido entre las 11:00 y las 13:00 UTC. • IF (condition, value_if_ true, value_if_false): si la condición es verdadera (por ejemplo, la hora está entre las 11:00 y las 13:00 UTC), devuelve 99. Si la condición es falsa, conserve el valor métrico original (m1).

Suprima las alarmas de un APM de terceros

Consulte la documentación de su proveedor de APM externo para obtener instrucciones sobre cómo suprimir las alarmas. Algunos ejemplos de proveedores de APM externos son New Relic, Splunk, Dynatrace, Datadog y. SumoLogic

Envíe una solicitud de cambio de carga de trabajo para suprimir las alarmas

Si no puede suprimir las alarmas en su origen como se describe en la sección anterior, envíe una solicitud de cambio en la carga de trabajo para indicar a Detección y Respuesta a los incidentes que supriman manualmente la supervisión de algunas o todas las alarmas de la carga de trabajo.

Para obtener instrucciones detalladas sobre cómo crear una solicitud de cambio de carga de trabajo, consulte Solicitar cambios en una carga de trabajo integrada en Detección y respuesta a incidentes. Al presentar una solicitud de cambio de carga de trabajo para solicitar la supresión de las alarmas, asegúrese de proporcionar la siguiente información obligatoria

- Nombre de la carga de trabajo: el nombre de su carga de trabajo.
- ID de cuenta: ID1 ID2 ID3,, etc.
- Detalles del cambio: supresión de alarmas
- Hora de inicio de la supresión: fecha, hora y zona horaria.
- Hora de finalización de la supresión: fecha, hora y zona horaria.
- Alarmas que se deben suprimir: una lista de identificadores de CloudWatch alarmas ARNs o eventos de APM de terceros que se deben suprimir.

Tras crear la solicitud de cambio de carga de trabajo para la supresión de alarmas, recibirá las siguientes notificaciones de Detección y Respuesta a Incidentes:

- Reconocimiento de su solicitud de cambio de carga de trabajo.
- Notificación cuando se suprimen las alarmas.
- Notificación cuando se vuelven a activar las alarmas para su supervisión.

Tutorial: Utilice una función matemática métrica para suprimir una alarma

En el siguiente tutorial, se explica cómo suprimir una CloudWatch alarma mediante la matemática métrica.

Escenario de ejemplo

Hay una actividad planificada que tendrá lugar entre la 1:00 y las 3:00 a. m. UTC del próximo martes. Desea crear una función matemática CloudWatch métrica que sustituya los puntos de datos reales durante este tiempo por 0 (un punto de datos que esté por debajo del umbral establecido).

1. Evalúa los criterios que hacen que se active la alarma. La siguiente captura de pantalla proporciona un ejemplo de los criterios de alarma:

   La alarma que se muestra en la captura de pantalla anterior monitorea la `UnHealthyHostCount` métrica de un grupo objetivo de Application Load Balancer. Esta alarma entra en `ALARM` estado cuando la `UnHealthyHostCount` métrica es mayor o igual a 3 para 5 de los 5 puntos de datos. La alarma considera que los datos faltantes son incorrectos (sobrepasando el umbral configurado).

2. Cree la función matemática métrica.

   En este ejemplo, la actividad planificada tendrá lugar entre la 1:00 y las 3:00 a. m. UTC del próximo martes. Por lo tanto, cree una función matemática CloudWatch métrica que sustituya los puntos de datos reales durante este tiempo por 0 (un punto de datos que esté por debajo del umbral establecido).

   Tenga en cuenta que el punto de datos de reemplazo que debe configurar varía según la configuración de la alarma. Por ejemplo, si tiene una alarma que monitorea la tasa de éxito de HTTP, con un umbral inferior a 98, sustituya los puntos de datos reales durante la actividad planificada por un valor superior al umbral configurado, 100. El siguiente es un ejemplo de función matemática métrica para este escenario.

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

   La función matemática métrica anterior contiene los siguientes elementos:

   - DÍA (m1) == 2: Garantiza que sea martes (lunes = 1, domingo = 7).
   - HORA (m1) >= 1 && HORA (m1) < 3: Especifica el intervalo de tiempo comprendido entre la 1 a. m. y las 3 a. m. UTC.
   - IF (condition, value_if_true, value_if_false): si las condiciones son verdaderas, la función reemplaza el valor métrico por 0. De lo contrario, se devuelve el valor original (m1).

Para obtener información adicional sobre la sintaxis y las funciones disponibles, consulte Funciones y sintaxis de las matemáticas métricas en la Guía del CloudWatch usuario de Amazon.

3. Inicie sesión en AWS Management Console y abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
4. Seleccione Alarmas y, a continuación, localice la alarma a la que desee añadir la función matemática métrica.
5. En la sección de matemáticas métricas, selecciona Editar.
6. Elija Añadir matemática, comience con una expresión vacía.
7. Introduzca la expresión matemática y, a continuación, seleccione Aplicar.

   La métrica existente que supervisa la alarma se convierte automáticamente en m1 y la expresión matemática en e1, como se muestra en el siguiente ejemplo:

8. (Opcional) Edita la etiqueta de la expresión matemática métrica para que otros usuarios entiendan su función y el motivo por el que se creó, como se muestra en el siguiente ejemplo:

9. Deseleccione m1, seleccione e1 y, a continuación, elija Seleccionar métrica. Esto configura la alarma para que supervise directamente la expresión matemática en lugar de la métrica subyacente.
10. Elija Saltar a la vista previa y crear.
11. Compruebe que la alarma esté configurada según lo previsto y, a continuación, seleccione Actualizar alarma para guardar el cambio.

En el ejemplo anterior, sin la función matemática métrica aplicada, la `UnHealthyHostCount` métrica real se habría registrado durante la actividad planificada. Esto habría provocado que la CloudWatch alarma entrara en `ALARM` estado y activara la función de detección y respuesta a incidentes, como se muestra en el siguiente ejemplo:

Una vez implementada la función matemática métrica, los puntos de datos reales se sustituyen por 0 durante la actividad y la alarma permanece en ese `OK` estado, lo que impide la detección de incidentes y la respuesta.

Tutorial: Elimine una función matemática métrica para desactivar una alarma

Si suprimes una CloudWatch alarma para una actividad única, elimina la función matemática métrica de la alarma una vez finalizada la actividad para reanudar la supervisión regular de la alarma. Para desactivar la alarma de forma regular, por ejemplo, si tienes una rutina de aplicación de parches semanal programada que hace que, por ejemplo, se reinicie el mismo día y a la misma hora cada semana, deja activa la función matemática métrica.

En el siguiente tutorial, se explica cómo eliminar una función matemática métrica para desactivar una alarma CloudWatch

1. Inicie sesión en AWS Management Console y abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Seleccione Alarmas y, a continuación, localice la alarma a la que desee añadir la función matemática métrica.
3. En la sección de matemáticas métricas, selecciona Editar.
4. Para eliminar la supresión de la alarma, pulse el botón x situado junto a la expresión matemática métrica.
5. Seleccione la métrica para reanudar la supervisión de la métrica real y, a continuación, elija Seleccionar métrica.
6. Seleccione Saltar a la vista previa y crear.
7. Compruebe que la alarma esté configurada según lo previsto y, a continuación, seleccione Actualizar alarma para guardar el cambio.

Elimine una carga de trabajo de la detección y respuesta a incidentes

Para excluir una carga de trabajo de AWS Incident Detection and Response, cree un nuevo caso de soporte para cada carga de trabajo. Al crear el caso de soporte, tenga en cuenta lo siguiente:

- Para eliminar una carga de trabajo que está en una sola AWS cuenta, crea el caso de soporte desde la cuenta de la carga de trabajo o desde tu cuenta de pagador.
- Para eliminar una carga de trabajo que abarca varias AWS cuentas, crea el caso de soporte desde tu cuenta de pagador. En el cuerpo del caso de soporte, incluye todas las cuentas IDs que deseas eliminar.

> **Important**
>
> Si crea un caso de soporte para retirar una carga de trabajo de la cuenta incorrecta, es posible que se produzcan retrasos y se solicite información adicional antes de poder descargar las cargas de trabajo.

Solicitud para eliminar una carga de trabajo

1. Ve al AWS Support Centro y, a continuación, selecciona Crear caso.
2. Elige Técnico.
3. En Servicio, elija Detección y respuesta a incidentes.
4. En Categoría, elija Workload Offlboarding.
5. En Gravedad, selecciona Guía general.
6. Introduzca un asunto para este cambio. Por ejemplo:

   [Fuera de bordo] Detección y respuesta a incidentes de AWS - *workload_name*
7. Introduzca una descripción para este cambio. Por ejemplo, escriba «Esta solicitud es para eliminar una carga de trabajo existente incorporada en AWS Incident Detection and Response». Asegúrese de incluir la siguiente información en su solicitud:

   - Nombre de la carga de trabajo: el nombre de su carga de trabajo.
   - ID de cuenta: ID1 ID2 ID3,, etc.
   - Motivo de la desvinculación: indica el motivo de la desvinculación de la carga de trabajo.
8. En la sección Contactos adicionales (opcional), introduce cualquier correo electrónico con el IDs que desees recibir correspondencia sobre esta solicitud de exclusión.
9. Elija Enviar.

Monitorización y observabilidad de la detección y respuesta a incidentes de AWS

AWS Incident Detection and Response le ofrece orientación experta sobre cómo definir la observabilidad en todas sus cargas de trabajo, desde la capa de aplicación hasta la infraestructura subyacente. La supervisión le indica que algo va mal. La observabilidad utiliza la recopilación de datos para determinar qué es lo que está mal y por qué ha ocurrido.

El sistema de detección y respuesta a incidentes monitorea sus AWS cargas de trabajo en busca de fallos y degradación del rendimiento mediante el uso de AWS servicios nativos como Amazon y CloudWatch Amazon EventBridge para detectar eventos que puedan afectar a su carga de trabajo. La supervisión le proporciona notificaciones de fallos inminentes, continuos, inminentes o potenciales, o de una degradación del rendimiento. Cuando incorporas tu cuenta a Incident Detection and Response, seleccionas qué alarmas de tu cuenta deben ser monitoreadas por el sistema de monitoreo de detección y respuesta a incidentes y asocias esas alarmas a una aplicación y un manual que se utilizan para la gestión de incidentes.

Incident Detection and Response utiliza Amazon CloudWatch y otros Servicios de AWS para crear su solución de observabilidad. AWS Incident Detection and Response le ayuda con la observabilidad de dos maneras:

- Métricas de resultados empresariales: la observabilidad de la detección y respuesta a incidentes de AWS comienza con la definición de las métricas clave que supervisan los resultados de las cargas de trabajo o la experiencia del usuario final. AWS Los expertos trabajan con usted para comprender los objetivos de su carga de trabajo, los resultados o factores clave que pueden afectar a la experiencia del usuario y para definir las métricas y alertas que captan cualquier degradación de esas métricas clave. Por ejemplo, una métrica empresarial clave para una aplicación de llamadas móviles es la tasa de éxito de la configuración de llamadas (monitorea la tasa de éxito de los intentos de llamada de los usuarios), y una métrica clave para un sitio web es la velocidad de la página. La participación en los incidentes se activa en función de las métricas de resultados empresariales.
- Métricas a nivel de infraestructura: en esta etapa, identificamos la infraestructura subyacente Servicios de AWS y la infraestructura que respalda su aplicación y definimos las métricas y las alarmas para hacer un seguimiento del rendimiento de estos servicios de infraestructura. Estas pueden incluir métricas, como las de las `ApplicationLoadBalancerErrorCount` instancias de

Application Load Balancer. Esto comienza una vez que se ha incorporado la carga de trabajo y se ha configurado la supervisión.

Implementación de la observabilidad en la detección y respuesta a incidentes de AWS

Como la observabilidad es un proceso continuo que puede no completarse en un ejercicio o período de tiempo, AWS Incident Detection and Response implementa la observabilidad en dos fases:

- Fase de incorporación: la observabilidad durante la incorporación se centra en detectar si los resultados empresariales de la aplicación se ven perjudicados. Con este fin, la observabilidad durante la fase de incorporación se centra en definir las métricas clave de los resultados empresariales a nivel de la aplicación para notificar las interrupciones en las cargas AWS de trabajo. De esta forma, AWS podrá responder rápidamente a estas interrupciones y ayudarle a recuperarse.
- Fase posterior a la incorporación: AWS Incident Detection and Response ofrece una serie de servicios proactivos para la observabilidad, que incluyen la definición de métricas a nivel de infraestructura, el ajuste de las métricas y la configuración de rastreos y registros en función del nivel de madurez del cliente. La implementación de estos servicios puede durar varios meses e involucrar a varios equipos. AWS Incident Detection and Response proporciona orientación sobre la configuración de la observabilidad y los clientes deben implementar los cambios necesarios en su entorno de carga de trabajo. Para obtener ayuda con la implementación práctica de las funciones de observabilidad, envíe una solicitud a sus administradores de cuentas técnicas (). TAMs

Gestión de incidentes con detección y respuesta a incidentes

AWS Incident Detection and Response le ofrece monitoreo proactivo y administración de incidentes las 24 horas del día, los 7 días de la semana, a cargo de un equipo designado de administradores de incidentes. El siguiente diagrama describe el proceso estándar de gestión de incidentes cuando una alarma de aplicación desencadena un incidente, que incluye la generación de alarmas, la participación del administrador de AWS incidentes, la resolución de incidentes y la revisión posterior al incidente.

1. Generación de alarmas: las alarmas que se activan en sus cargas de trabajo se envían a través de Amazon EventBridge a AWS Incident Detection and Response. AWS Incident Detection and Response muestra automáticamente el manual asociado a la alarma y lo notifica a un administrador de incidentes. Si se produce un incidente crítico en su carga de trabajo que no es detectado por las alarmas supervisadas por AWS Incident Detection and Response, puede crear un caso de soporte para solicitar una respuesta a incidentes. Para obtener más información sobre cómo solicitar una respuesta a un incidente, consulteSolicita una respuesta a un incidente.
2. AWS Interacción del administrador de incidentes: el administrador de incidentes responde a la alarma y lo contacta en una conferencia telefónica o según se especifique en el manual. El administrador de incidentes verifica el estado de la alarma Servicios de AWS para determinar si la alarma está relacionada con problemas relacionados con Servicios de AWS la carga de trabajo e informa sobre el estado de los servicios subyacentes. Si es necesario, el administrador de incidentes crea un caso en su nombre y contrata a los AWS expertos adecuados para que lo apoyen.

   Dado que AWS Incident Detection and Response monitorea Servicios de AWS específicamente sus aplicaciones, AWS Incident Detection and Response puede determinar que el incidente está relacionado con un Servicio de AWS problema incluso antes de que se declare un Servicio de AWS evento. En este escenario, el administrador de incidentes le informa sobre el estado del incidente Servicio de AWS, activa el flujo de administración de incidentes de eventos de AWS servicio y se pone en contacto con el equipo de servicio para resolverlo. La información proporcionada le brinda la oportunidad de implementar sus planes de recuperación o soluciones alternativas con prontitud para mitigar el impacto del evento de AWS servicio. Para obtener más información, consulte Gestión de incidentes para eventos de servicio.

3. Resolución de incidentes: el administrador de incidentes coordina el incidente entre los AWS equipos necesarios y se asegura de que sigas colaborando con los AWS expertos adecuados hasta que el incidente se mitigue o resuelva.
4. Revisión posterior al incidente (si se solicita): tras un incidente, AWS Incident Detection and Response puede realizar una revisión posterior al incidente si así lo solicita y generar un informe posterior al incidente. El informe posterior al incidente incluye una descripción del problema, el impacto, los equipos que participaron y las soluciones alternativas o las medidas adoptadas para mitigar o resolver el incidente. El informe posterior al incidente puede contener información que se puede utilizar para reducir la probabilidad de que se repita el incidente o para mejorar la gestión de un incidente similar en el futuro. El informe posterior al incidente no es un análisis de la causa raíz (RCA). Puede solicitar un RCA además del informe posterior al incidente. En la siguiente sección se proporciona un ejemplo de un informe posterior a un incidente.

> **Important**
>
> La siguiente plantilla de informe es solo un ejemplo.

```
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 Soporte support case on
 behalf of the customer.
  At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and Soporte 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 Support and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

Temas

- Proporcione acceso a AWS Support Center Console los equipos de aplicaciones
- Gestión de incidentes para eventos de servicio
- Solicita una respuesta a un incidente
- Gestione los casos de soporte de detección y respuesta a incidentes con el AWS Support App in Slack

Proporcione acceso a AWS Support Center Console los equipos de aplicaciones

AWS Incident Detection and Response se comunica con usted a través de Soporte los casos durante el ciclo de vida de un incidente. Para mantener correspondencia con los administradores de incidentes, sus equipos deben tener acceso al Soporte Centro.

Para obtener más información sobre el aprovisionamiento del acceso, consulte Administrar el acceso al Soporte Centro en la Guía del Soporte usuario.

Gestión de incidentes para eventos de servicio

AWS Incident Detection and Response le notifica durante Servicio de AWS las interrupciones que tienen un gran impacto en los clientes, incluidos los problemas que afectan a varios clientes o los problemas Servicios de AWS que su carga de trabajo utiliza dentro de una zona afectada Región de AWS o de disponibilidad. Si lo solicitan, los administradores de incidentes de AWS Incident Detection and Response pueden unirse a su puente de conferencias telefónicas para hacer lo siguiente:

- Le guiará durante la implementación del plan de recuperación
- Transmita posibles soluciones
- Reúna su información sobre el incidente y el impacto
- Defienda y escale los problemas internos AWS en su nombre

Recibes notificaciones de interrupción del servicio a través de AWS Health. Si opera en un entorno que Región de AWS no se ve afectado por la interrupción del servicio o no utiliza los servicios deteriorados, seguirá recibiendo asistencia a través de las contrataciones estándar de detección y respuesta a incidentes de AWS. Para obtener más información AWS Health, consulte ¿Qué es? AWS Health .

Para obtener más información sobre cómo AWS Incident Detection and Response le ayuda durante las interrupciones del servicio, consulte el siguiente diagrama de flujo de trabajo de respuesta a incidentes. El diagrama describe las medidas adoptadas por AWS los equipos y describe cómo los equipos de respuesta a incidentes colaboran con usted para identificar, mitigar y resolver la interrupción del servicio.

Solicita una respuesta a un incidente

Si se produce un incidente crítico en su carga de trabajo que no es detectado por las alarmas supervisadas por AWS Incident Detection and Response, puede crear un caso de soporte para solicitar una respuesta a incidentes. Puede solicitar una respuesta a incidentes para cualquier carga de trabajo que esté suscrita a AWS Incident Detection and Response, incluidas las cargas de trabajo en proceso de incorporación, mediante la AWS Support Center Console AWS Support API o. AWS Support App in Slack

El siguiente diagrama ilustra el end-to-end flujo de trabajo de un AWS cliente que solicita asistencia al equipo de detección y respuesta a incidentes, y detalla los pasos que van desde la solicitud inicial hasta la investigación, la mitigación y la resolución.

Para solicitar una respuesta ante un incidente que esté afectando activamente a tu carga de trabajo, crea un Soporte caso. Una vez planteado el caso de soporte, AWS Incident Detection and Response lo pone en contacto en una conferencia con los AWS expertos necesarios para acelerar la recuperación de su carga de trabajo.

Solicite una respuesta a un incidente mediante el AWS Support Center Console

1. Abra y AWS Support Center Console, a continuación, seleccione Crear caso.
2. Elija Técnico.
3. En Servicio, elija Detección y respuesta a incidentes.
4. En Categoría, elija Incidente activo.
5. En Gravedad, selecciona Sistema crítico para la empresa inactivo.
6. Introduzca un asunto para este incidente. Por ejemplo:

   Detección y respuesta a incidentes de AWS - Incidente activo - workload_name

7. Introduzca la descripción del problema de este incidente. Añada los siguientes detalles:
   - Información técnica:

     Nombre de carga de trabajo

     ARN (s) de AWS recursos afectados
   - Información empresarial:

     Descripción del impacto en el negocio

     [Opcional] Detalles de Customer Bridge
8. Para ayudarnos a contratar a AWS los expertos con mayor rapidez, proporcione los siguientes detalles:
   - Afectado Servicio de AWS
   - Servicios adicionales u otros afectados
   - Afectado Región de AWS
9. En la sección Contactos adicionales, introduce las direcciones de correo electrónico con las que deseas recibir correspondencia sobre este incidente.

   La siguiente ilustración muestra la pantalla de la consola con el campo Contactos adicionales resaltado.

10. Elija Enviar.

    Tras enviar una solicitud de respuesta a un incidente, puede añadir direcciones de correo electrónico adicionales de su organización. Para añadir direcciones adicionales, responda al caso y, a continuación, añada las direcciones de correo electrónico en la sección Contactos adicionales.

    La siguiente ilustración muestra la pantalla de detalles del caso con el botón Responder resaltado.

    La siguiente ilustración muestra el caso Responder con el campo Contactos adicionales y el botón Enviar resaltados.

11. AWS Incident Detection and Response reconoce su caso en cinco minutos y lo organiza en una conferencia con los AWS expertos correspondientes.

Solicite una respuesta a un incidente mediante la API AWS Support

Puede utilizar la AWS Support API para crear casos de soporte mediante programación. Para obtener más información, consulte Acerca de la AWS Support API en la Guía del AWS Support usuario.

Solicite una respuesta a un incidente mediante el AWS Support App in Slack

Para utilizar el AWS Support App in Slack para solicitar una respuesta a un incidente, complete los siguientes pasos:

1. Abre el canal de Slack AWS Support App in Slack en el que configuraste.
2. Escriba el siguiente comando:

```
/awssupport create
```

3. Introduzca un asunto para este incidente. Por ejemplo, introduzca AWS Incident Detection and Response - Active Incident - workload_name.
4. Introduzca la descripción del problema de este incidente. Añada los siguientes detalles:

   Información técnica:

   Servicio (s) afectado (s):

   Recurso (s) afectado (s):

   Región (s) afectada (s):

   Nombre de la carga de trabajo:

   Información empresarial:

   Descripción del impacto en el negocio:

   [Opcional] Detalles de Customer Bridge:
5. Elija Siguiente.

6. En Tipo de problema, selecciona Soporte técnico.
7. En Servicio, seleccione Detección y respuesta a incidentes.
8. En Categoría, elija Incidente activo.
9. En Gravedad, selecciona Sistema crítico para la empresa inactivo.
10. Si lo desea, introduzca hasta 10 contactos adicionales en el campo Contactos adicionales a notificar, separados por comas. Estos contactos adicionales reciben copias de la correspondencia por correo electrónico sobre este incidente.
11. Elija Revisar.
12. En el canal de Slack aparece un mensaje nuevo que solo tú puedes ver. Revisa los detalles del caso y, a continuación, selecciona Crear caso.
13. El identificador de tu caso se incluye en un mensaje nuevo de AWS Support App in Slack.
14. Incident Detection and Response reconoce su caso en un plazo de 5 minutos y lo pone en contacto con los AWS expertos correspondientes.
15. La correspondencia de Incident Detection and Response se actualiza en el hilo de casos.

Gestione los casos de soporte de detección y respuesta a incidentes con el AWS Support App in Slack

Con él AWS Support App in Slack, puede gestionar sus Soporte casos en Slack, recibir notificaciones sobre nuevos incidentes iniciados por alarmas en su carga de trabajo de detección y respuesta a incidentes de AWS y crear solicitudes de respuesta a incidentes.

Para configurarlo AWS Support App in Slack, siga las instrucciones que se proporcionan en la Guía del Soporte usuario.

> **Important**
>
> - Para recibir notificaciones en Slack de todos los incidentes iniciados por alarmas en su carga de trabajo, debe configurar las cuentas de todas las cargas de trabajo que estén

incorporadas a AWS Incident Detection and Response. AWS Support App in Slack Los casos de Support se crean en la cuenta en la que se originó la alarma de carga de trabajo.

- Se pueden abrir varios casos de asistencia de alta gravedad en tu nombre durante un incidente para involucrar a los encargados de Soporte resolverlos. Recibirás notificaciones en Slack sobre todos los casos de asistencia que se abran durante un incidente y que coincidan con tu configuración de notificaciones para el canal de Slack.
- Las notificaciones que recibas a través de AWS Incident Detection and Response durante un incidente AWS Support App in Slack no sustituyen a los contactos iniciales y de escalamiento de tu carga de trabajo, a los que se contacta por correo electrónico o llamada telefónica.

Temas

- Notificaciones de incidentes iniciadas por alarmas en Slack
- Crea una solicitud de respuesta a un incidente en Slack

Notificaciones de incidentes iniciadas por alarmas en Slack

Tras configurarlo AWS Support App in Slack en su canal de Slack, recibirá notificaciones sobre los incidentes iniciados por alarmas en su carga de trabajo supervisada por AWS Incident Detection and Response.

En el siguiente ejemplo, se muestra cómo aparecen en Slack las notificaciones de los incidentes iniciados por alarmas.

Ejemplo de notificación

Cuando AWS Incident Detection and Response reconoce el incidente provocado por una alarma, se genera en Slack una notificación similar a la siguiente:

Para ver la correspondencia completa agregada por AWS Incident Detection and Response, seleccione Ver detalles.

En el hilo del caso aparecen más actualizaciones de AWS Incident Detection and Response.

Seleccione Ver detalles para ver la correspondencia completa agregada por AWS Incident Detection and Response.

Crea una solicitud de respuesta a un incidente en Slack

Para obtener instrucciones sobre cómo crear una solicitud de respuesta a un incidente a través del AWS Support App in Slack, consulteSolicita una respuesta a un incidente.

Informes en la detección y respuesta a incidentes

AWS Incident Detection and Response proporciona datos operativos y de rendimiento para ayudarle a comprender cómo está configurado el servicio, el historial de sus incidentes y el rendimiento del servicio de detección y respuesta a incidentes. En esta página se describen los tipos de datos disponibles, incluidos los datos de configuración, los datos de incidentes y los datos de rendimiento.

Datos de configuración

- Todas las cuentas incorporadas
- Nombres de todas las aplicaciones
- Las alarmas, los manuales de ejecución y los perfiles de soporte asociados a cada aplicación

Datos de incidentes

- Las fechas, el número y la duración de los incidentes de cada aplicación
- Las fechas, el número y la duración de los incidentes asociados a una alarma específica
- Informe posterior al incidente

Datos de rendimiento

- Rendimiento del objetivo de nivel de servicio (SLO)

Póngase en contacto con su administrador técnico de cuentas para obtener los datos operativos y de rendimiento que pueda necesitar.

Seguridad y resiliencia de detección y respuesta a incidentes

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Soporte. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad Servicios de AWS que utilice.

Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos.

Para obtener información sobre la protección de datos en Europa, consulte la entrada del blog sobre el modelo de responsabilidad AWS compartida y el RGPD en el blog AWS de seguridad.

Para proteger los datos, le recomendamos que proteja las credenciales de las AWS cuentas y configure cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes maneras:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Use certificados Layer/Transport Layer Security (SSL/TLS (Secure Sockets) para comunicarse con AWS los recursos. Recomendamos TLS 1.2 o una versión posterior. Para obtener información, consulte ¿Qué es un certificado SSL/TLS? .
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener más información, consulte AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3. Para obtener información sobre Amazon Macie, consulte Amazon Macie.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto de conexión FIPS. Para obtener información sobre los puntos finales FIPS disponibles, consulte la Norma Federal de Procesamiento de Información (FIPS) 140-2.

Recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaja con Soporte o Servicios de AWS utilizando la consola, la API, la AWS CLI o AWS SDKs. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Acceso a sus cuentas con AWS Incident Detection and Response

AWS Identity and Access Management (IAM) es un servicio web que le ayuda a controlar de forma segura el acceso a AWS los recursos. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.

AWS Incident Detection and Response y sus datos de alarma

De forma predeterminada, Incident Detection and Response recibe el nombre del recurso de Amazon (ARN) y el estado de todas las CloudWatch alarmas de tu cuenta y, a continuación, inicia el proceso de detección y respuesta a incidentes cuando la alarma incorporada pasa al estado ALARM. Si desea personalizar la información que recibe la detección y respuesta a incidentes sobre las alarmas de su cuenta, póngase en contacto con su gestor técnico de cuentas.

Historial del documento

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de la guía IDR.

Cambio	Descripción	Fecha
Información actualizada sobre cómo la detección y respuesta a incidentes gestionan los eventos de servicio	Se actualizó la sección de gestión de incidente s para los eventos de servicio. Sección actualizada: Gestión de incidentes para eventos de servicio	15 de mayo de 2025
Nueva función: evita que las alarmas activen la detección y respuesta a incidentes	Se han añadido nuevas secciones a las cargas de trabajo gestionadas que proporcionan información sobre cómo suprimir las alarmas de forma temporal o programada Nueva sección: Evite que las alarmas activen la detección y respuesta a incidentes	9 de abril de 2025
Instrucciones actualizadas para solicitar una respuesta a un incidente mediante el AWS Support Center Console	Se agregaron detalles sobre la información que se debe introducir en el campo de descripción del problema. Sección actualizada: Solicita una respuesta a un incidente	6 de febrero de 2025
Adicional Regiones de AWS añadido	Se Regiones de AWS han agregado más a la sección de disponibilidad de detección y respuesta a incidentes. Sección actualizada: Disponibilidad regional para la detección y respuesta a incidentes	1 de noviembre de 2024
Actualizaciones para gestionar los casos de soporte de detección y respuesta a	Se trasladó la página a Gestión de incidentes, se revisó el texto y se sustituyeron las capturas de pantalla.	10 de octubre de 2024

Cambio	Descripción	Fecha
incidentes con la AWS Support App in Slack página	Sección actualizada: Gestione los casos de soporte de detección y respuesta a incidentes con el AWS Support App in Slack	
Se agregó una nueva página AWS Support App in Slack Gestión de incidentes actualizada con AWS Incident Detection and Response	Se agregó una nueva página para AWS Support App in Slack Se actualizó la gestión de incidentes con AWS Incident Detection and Response para añadir una nueva sección, «Solicitar una respuesta a un incidente mediante AWS Support App in Slack».	10 de septiembre de 2024
Suscripción a la cuenta actualizada	Se actualizó la sección de suscripción de la cuenta para incluir detalles sobre dónde abrir un caso de soporte cuando solicitas la suscripci ón de una cuenta. Sección actualizada: Suscriba una carga de trabajo a Incident Detection and Response	12 de junio de 2024
Ya está disponible el informe posterior al incidente para los eventos de servicio	Se actualizó la sección de gestión de incidente s para los eventos de servicio para incluir información sobre el informe posterior al incidente para los eventos de servicio. Sección actualizada: Gestión de incidentes para eventos de servicio	8 de mayo de 2024
Se agregó una nueva sección: Eliminar una carga de trabajo	Se agregó la sección Descargar una carga de trabajo en Primeros pasos para incluir informaci ón sobre la transferencia de cargas de trabajo Para obtener más información, consulte Elimine una carga de trabajo de la detección y respuesta a incidentes.	28 de marzo de 2024

Cambio	Descripción	Fecha
Suscripción a la cuenta actualizada	Se actualizó la sección de suscripción a la cuenta para incluir información sobre las cargas de trabajo que se descargan Para obtener más información, consulte Suscripción a una cuenta	28 de marzo de 2024
Pruebas actualizadas	Se actualizó la sección de pruebas para incluir información sobre las pruebas del día del partido como último paso del proceso de incorporación. Sección actualizada: Pruebe las cargas de trabajo integradas en Detección y respuesta a incidentes	29 de febrero de 2024
Actualización: ¿Qué es AWS Incident Detection and Response?	Se actualizó la sección Qué es la detección y respuesta a incidentes de AWS. Sección actualizada: ¿Qué es AWS Incident Detection and Response?	19 de febrero de 2024
Sección de cuestionarios actualizada	Se actualizó el cuestionario de incorpora ción de la carga de trabajo y se agregó el cuestionario de ingesta de alarmas. Se cambió el nombre de la sección de Cuestionario de incorporación de cargas de trabajo a cuestiona rios de incorporación de cargas de trabajo e ingestión de alarmas. Sección actualizada: Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response	2 de febrero de 2024

Cambio	Descripción	Fecha
Información actualizada sobre el evento de AWS servicio y la incorporación	Se actualizaron varias secciones con nueva información para la incorporación. Secciones actualizadas: • Gestión de incidentes para eventos de servicio • Descubrimiento de la carga de trabajo en la detección y respuesta a incidentes • Introducción a la detección y respuesta a incidentes • Suscriba una carga de trabajo a Incident Detection and Response Nuevas secciones • Proporcione acceso a AWS Support Center Console los equipos de aplicaciones	31 de enero de 2024
Se agregó una sección de información relacionada	Se agregó una sección de información relacionada en el aprovisionamiento de Access. Sección actualizada: Proporcione acceso para la recepción de alertas a la detección y respuesta a incidentes	17 de enero de 2024
Pasos de ejemplo actualiza dos	Se actualizó el procedimiento de los pasos 2, 3 y 4 del ejemplo: integración de notificaciones de Datadog y Splunk. Sección actualizada: Ejemplo: integre las notificaciones de Datadog y Splunk	21 de diciembre de 2023

Cambio	Descripción	Fecha
Texto y gráfico de introducción actualizados	Gráfico actualizado en las alarmas Ingest APMs que tienen integración directa con Amazon EventBridge. Sección actualizada: Desarrolle manuales y planes de respuesta para responder a un incidente en el marco de la detección y respuesta a incidentes	21 de diciembre de 2023
Plantilla de manual actualizada	Se actualizó la plantilla del manual en Desarrollo de manuales para la detección y respuesta a incidentes de AWS. Sección actualizada: Desarrolle manuales y planes de respuesta para responder a un incidente en el marco de la detección y respuesta a incidentes	4 de diciembre de 2023
Configuraciones de alarma actualizadas	Configuraciones de alarma actualizadas con información detallada sobre la configuración de CloudWatch alarmas. Nueva sección: Cree CloudWatch alarmas que se adapten a las necesidades de su empresa en materia de detección y respuesta a incidentes Nueva sección: Cree CloudWatch alarmas en Incident Detection and Response con plantillas CloudFormation Nueva sección: Ejemplos de casos de uso de CloudWatch alarmas en Incident Detection and Response	28 de septiembre de 2023

Cambio	Descripción	Fecha
Actualización: Cómo empezar	Introducción actualizada con información sobre las solicitudes de cambios en la carga de trabajo. Nueva sección: Solicite cambios en una carga de trabajo integrada en Incident Detection and Response Sección actualizada: Suscriba una carga de trabajo a Incident Detection and Response	05 de septiembre de 2023
Nueva sección en Cómo empezar	Se agregaron alertas Incorpore alarmas en AWS Incident Detection and Response de ingesta a AWS Incident Detection and Response.	30 de junio de 2023
Documento original	AWS Incident Detection and Response publicó por primera vez	15 de marzo de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.