Conceptos y procedimientos de detección y respuesta a incidentes de AWS

Guía del usuario de detección y respuesta a incidentes de AWS

Version May 26, 2026

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

Table of Contents

¿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 se ponen en contacto con usted de forma proactiva a los 5 minutos de producirse una alarma, debido a sus cargas de trabajo o en respuesta a un caso crítico que usted presente.
- Resolución más rápida: los IME utilizan manuales predefinidos y personalizados desarrollados para sus cargas de trabajo, crean un caso de Support en su nombre y gestionan los incidentes de su carga de trabajo. Los IME ofrecen la titularidad de los incidentes mediante un único subproceso y permiten mantener el contacto con los AWS expertos adecuados hasta que se resuelva el incidente.
- Menor probabilidad de fallo: una vez resueltos, los IME le 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. También puede aprovechar el seguimiento continuo AWS Resilience Hub de la resiliencia de sus cargas de trabajo.

Temas

Inscríbase en una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte Cómo empezar con un Cuenta de AWS en la Guía de AWS Account Management referencia.

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 Direct Support y Partner-resold Enterprise Support.
- 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 los detalles de la arquitectura de las cargas de trabajo, los detalles de las 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 debe ponerse en contacto, cómo ponerse en contacto con ellos y qué información debe 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
Revisión de la preparación de las operaciones		

Actividad	Cliente	Detección y respuesta a incidentes
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 las alarmas integradas (CloudWatch o APM)	Responsable	Informado
Compruebe que las alarmas de los clientes activen la detección y la respuesta a los incidentes	Informado	Responsable
Actualiza las alarmas	Responsable	Consultado
Actualice los manuales	Consultado	Responsable

Actividad	Cliente	Detección y respuesta a incidentes
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
Post-incident revisión		
Solicitar una revisión posterior al incidente	Responsable	Informado
Proporcione una revisión posterior al incidente	Informado	Responsable

Disponibilidad regional para la detección y respuesta a incidentes

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

Región de AWS	Name
Región Este de EE. UU. (Norte de Virginia)	us-east-1
Región del este de EE. UU. (Ohio)	us-east-2

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

Región de AWS	Name
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Hyderabad)	ap-south-2
Asia-Pacífico (Yakarta)	ap-southeast-3
Asia-Pacífico (Melbourne)	ap-southeast-4
Asia-Pacífico (Malasia)	ap-southeast-5
África (Ciudad del Cabo)	af-south-1
Israel (Tel Aviv)	il-central-1
Medio Oriente (EAU)	me-central-1
Medio Oriente (Baréin)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

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 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 los incidentes.

Acerca de las cargas de trabajo en materia de detección y respuesta a incidentes

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 una Cuenta de AWS o varias Cuentas de AWS.

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 siguiente diagrama.

Para empezar con la incorporación de cargas de trabajo, consulte. Incorpore las cargas de trabajo a la detección y respuesta a incidentes

Acerca de las alarmas en la detección y respuesta a incidentes

Las alarmas son una parte clave de la detección y respuesta a incidentes. Las alarmas proporcionan visibilidad del rendimiento de sus aplicaciones y de la AWS infraestructura subyacente. AWS trabaja con usted para definir las métricas y los umbrales de alarma adecuados que solo se activan cuando hay un impacto crítico en las cargas de trabajo monitoreadas. El objetivo es que las alarmas capten la atención de los responsables específicos de la resolución, quienes, a su vez, colaboren con el equipo de gestión de incidentes para mitigar los problemas rápidamente. Configure sus alarmas

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. Ingestión de alarmas

Incorpore las cargas de trabajo a la detección y respuesta a incidentes

AWS Incident Detection and Response permite la supervisión y la gestión de incidentes críticos para las cargas de trabajo seleccionadas. Una carga de trabajo es un conjunto de recursos que trabajan juntos para ofrecer valor empresarial, como un portal de pagos o un sistema de gestión de relaciones con los clientes (CRM). Puede alojar estas cargas de trabajo en una sola cuenta Cuenta de AWS o distribuidas en varias cuentas, según su arquitectura.

Contenido

Incorpore la detección y respuesta a incidentes con la CLI de IDR

La interfaz de línea de comandos del cliente (IDR CLI) de AWS Incident Detection and Response es una herramienta de interfaz de línea de comandos que agiliza la incorporación a AWS Incident Detection and Response.

La CLI de IDR se ejecuta AWS CloudShell para realizar las siguientes funciones:

- Recopile información de incorporación
- Recopile datos AWS de recursos a través de la API de etiquetado de Resource Groups
- Gestione los casos AWS Support
- Crea nuevas CloudWatch alarmas de Amazon o ingiere las que ya tienes
- Implemente y pruebe la infraestructura AWS CloudFormation para permitir que herramientas de terceros envíen alertas para detectar y responder a incidentes.

La CLI de IDR se puede ejecutar en modo interactivo para guiarlo a través de los pasos de incorporación, o en modo fuera de línea para casos de uso masivos o de DevOps uso.

Para obtener más información sobre cómo utilizar la CLI de IDR, incluidos la instalación, los requisitos previos y los ejemplos integrales, consulte CLI para AWS Incident Detection and Response.

Soporte de idiomas para la CLI de IDR

AWS Incident Detection and Response está disponible en inglés, japonés, mandarín y coreano. Si necesita asistencia en japonés, mandarín o coreano, póngase en contacto AWS a través del AWS Support caso creado por la CLI de IDR o póngase en contacto con su administrador técnico de cuentas (TAM).

Opciones alternativas para la incorporación de cargas de trabajo

Si no puede usar la CLI de IDR para la incorporación, consulte a su administrador técnico de cuentas (TAM) para conocer las opciones alternativas. Para obtener más información, consulte Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response (ruta de excepciones)

Ingestión de alarmas

La interfaz de línea de comandos del cliente (IDR CLI) de AWS Incident Detection and Response puede crear nuevas CloudWatch alarmas de Amazon o incorporar las existentes, y puede implementar y probar la infraestructura AWS CloudFormation para permitir que herramientas de terceros envíen alertas a AWS Incident Detection and Response.

AWS Incident Detection and Response puede captar alarmas de Amazon CloudWatch y de herramientas de monitoreo del rendimiento de aplicaciones (APM) de terceros a través de Amazon: EventBridge

- Ingerir alarmas CloudWatch
- Ingerir alarmas de monitoreo del rendimiento de aplicaciones de terceros

Pasos para la ingesta de alarmas

Se deben completar los siguientes pasos para la ingesta de alarmas:

- Definición de alarma
- Ingesta de alarmas mediante la CLI de IDR
- Revisión y comentarios sobre las alarmas
- Proporcione acceso para la recepción de alarmas a la detección y respuesta a incidentes
- Las alarmas se activan

Opciones alternativas para la ingesta de alarmas

Si no puede usar la CLI de IDR para la ingesta de alarmas, consulte a su administrador técnico de cuentas (TAM) para conocer las opciones alternativas. Para obtener más información, consulte Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response (ruta de excepciones)

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

> **Note**
>
> Si no creó el rol vinculado al servicio (SLR) durante la incorporación de la CLI de IDR, siga los pasos que se indican a continuación para aprovisionar el acceso manualmente.

Para permitir que AWS Incident Detection and Response ingiera las alarmas de su cuenta, cree la `AWSServiceRoleForHealth_EventProcessor` SLR. AWS utiliza la SLR para crear una EventBridge regla gestionada en su cuenta. La EventBridge regla administrada envía notificaciones desde su cuenta 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 usuario.

Puede crear este rol vinculado a un servicio en su cuenta siguiendo las instrucciones de la Guía del usuario sobre cómo crear un rol vinculado a un servicio.AWS Identity and Access Management O bien, puede usar el siguiente AWS Command Line Interface comando ():AWS CLI

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

Salidas clave

- Creación correcta del rol vinculado al servicio en su cuenta.

> **Note**
>
> El rol vinculado al servicio - AWSServiceRoleForHealth _ EventProcessor debe crearse en cada cuenta que vaya a utilizar para enviar alarmas a AWS Incident Detection and Response.

Información relacionada

Para obtener más información, consulte los temas siguientes:

- Uso de roles vinculados a servicios de
- Crear un rol vinculado a un servicio
- AWS política gestionada: AWS Health_EventProcessorServiceRolePolicy

Definición de alarma

Al incorporar sus alarmas a AWS Incident Detection and Response, es responsable de definir las métricas y las configuraciones de alarmas que proporcionan visibilidad del rendimiento de sus aplicaciones. Como parte de este proceso, también debe identificar a los equipos de su organización responsables de responder a estas alarmas.

Al preparar las alarmas, recomendamos las siguientes prácticas recomendadas:

- Las alarmas solo entran en el estado de «Alarma» cuando la carga de trabajo supervisada está teniendo un impacto crítico continuo que requiere la atención inmediata de su equipo y AWS. Las alarmas que se activan y no se recuperan automáticamente requieren que sus equipos se unan a un puente de incidentes con AWS Incident Detection and Response.
- Asegúrese de que la información de contacto que proporciona permita a AWS Incident Detection and Response involucrar de manera confiable con los equipos correspondientes de su organización en un puente de incidentes 24/7.

Resultados clave

- Una lista de alarmas y detalles de contacto, que usted proporciona a AWS Incident Detection and Response mediante la CLI de IDR.

Para obtener más información sobre cómo definir e ingerir CloudWatch las alarmas de Amazon, consulteIngerir alarmas CloudWatch.

Para obtener más información sobre la ingesta de alarmas de monitoreo del rendimiento de aplicaciones de terceros, consulte. Ingerir alarmas de monitoreo del rendimiento de aplicaciones de terceros

Ingerir alarmas CloudWatch

AWS Incident Detection and Response puede incorporar CloudWatch las alarmas de Amazon para proporcionar una supervisión proactiva de sus cargas de trabajo críticas. Al incorporar las CloudWatch alarmas de Amazon para monitorizarlas, AWS Incident Detection and Response puede:

- Detecta automáticamente cuándo las alarmas entran en el estado de «Alarma».
- Involucre a sus equipos para que respondan y resuelvan los incidentes de forma colaborativa.

Para garantizar que las alarmas que incorpore sean eficaces, AWS Incident Detection and Response recomienda las siguientes prácticas recomendadas:

- Configure las alarmas con expresiones matemáticas métricas para suprimirlas durante los períodos de mantenimiento regular o la ejecución de tareas por lotes y evitar que se activen falsas alarmas positivas.
- Configure el tratamiento de los datos faltantes en las alarmas en función de la frecuencia de entrega prevista de los puntos de datos. Por ejemplo, las métricas de monitoreo de alarmas que generan un flujo continuo de puntos de datos deberían tratar los datos faltantes como «incumplidores» (incorrectos), ya que la falta de puntos de datos podría indicar un problema con el recurso subyacente monitoreado. Por el contrario, las métricas de monitoreo de alarmas que reportan puntos de datos con poca frecuencia, por ejemplo, las métricas de monitoreo de alarmas que solo registran puntos de datos cuando se produce una falla o error, deberían tratar los datos faltantes como (buenas). NotBreaching
- Defina alarmas que pasen al estado de «alarma» cuando se produzca un impacto crítico y continuo en su carga de trabajo. Por ejemplo, configure las alarmas para que se activen una vez transcurrido el tiempo previsto necesario para sustituir automáticamente los recursos en mal estado, en lugar de detectarlos inicialmente.

- Identifique y cree alarmas para métricas personalizadas que representen directamente la experiencia del cliente para su carga de trabajo.

Para obtener una lista de CloudWatch las alarmas de Amazon recomendadas para las más comunes Servicios de AWS, consulta las prácticas recomendadas para la detección de incidentes y las alarmas de respuesta en AWS Re:post.

Ingerir alarmas de monitoreo del rendimiento de aplicaciones de terceros

AWS Incident Detection and Response admite la ingesta de alarmas desde herramientas de monitoreo del rendimiento de aplicaciones (APM) de terceros a través de Amazon. EventBridge Esta integración proporciona flexibilidad al incorporar alertas de APM, lo que permite enrutar los eventos de APM a través de varios canales a Servicios de AWS un bus de eventos de Amazon EventBridge en su cuenta.

Ejemplos de rutas de integración:

- Fuente (APM) → AWS Servicio (ejemplo: Amazon API Gateway o Amazon SNS) → Función de transformación de Lambda → Amazon EventBridge Event Bus personalizado → Detección y respuesta a incidentes de AWS
- Fuente (APM) → Amazon EventBridge Event Bus asociado → Función de transformación de Lambda → EventBridge Amazon Event Bus personalizado → Detección y respuesta a incidentes de AWS

AWS Incident Detection and Response instala una regla administrada en el bus de eventos personalizado para ingerir las alertas que le envía Transform Lambda Functions. Es importante tener en cuenta que, en el caso de Amazon EventBridge Integrations con SaaS, el bus de eventos asociado no es el bus de eventos que tiene instalada una regla administrada. Para obtener una lista completa de los APM con integraciones de socios en Amazon EventBridge, consulta Integraciones de Amazon EventBridge .

Ejemplo de integración mediante un bus de eventos asociado u otras AWS fuentes de bus de eventos

El siguiente diagrama muestra un ejemplo de integración con un bus de eventos asociado u otras fuentes de bus de AWS eventos.

Para obtener una lista completa de los APM con integraciones de socios en Amazon EventBridge, consulta Integraciones de Amazon EventBridge .

Ejemplo de integración con Amazon API Gateway

En el siguiente diagrama se muestra un ejemplo de integración mediante una API Gateway.

Ejemplo de integración con Amazon Simple Notification Service

En el siguiente diagrama se muestra un ejemplo de integración mediante Amazon SNS.

Para simplificar el proceso de integración, AWS Incident Detection and Response proporciona CloudFormation plantillas para los tipos de integración más utilizados. Estas plantillas automatizan la configuración de AWS los recursos y las funciones de IAM necesarias.

CloudFormation Las plantillas e instrucciones para crear manualmente varios tipos de integración se encuentran en la documentación de integración correspondiente que aparece a continuación:

- Ingiera alarmas de los APM con integración directa EventBridge
- Ingiera alarmas de los APM sin una integración directa con EventBridge
- Administre alarmas de APM con la integración directa de Amazon SNS

> **Note**
>
> Las CloudFormation plantillas requieren modificaciones. Estas modificaciones se explican en los temas anteriores. Para obtener más información sobre el formato de carga útil necesario para enviar alertas de APM a AWS Incident Detection and Response, consulte. Requisitos de carga útil para ingerir alertas de APM con EventBridge

Requisitos de carga útil para ingerir alertas de APM con EventBridge

¿De dónde proviene la detección y respuesta a incidentes las alertas de APM?

AWS Incident Detection and Response instala una regla administrada en el bus de eventos al que se envía la carga útil transformada final. Para ello, se recomienda crear un bus de eventos personalizado.

¿En qué formato deben estar las cargas útiles?

Se requieren los siguientes pares de clave y valor de JSON como mínimo 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.

Antes de la 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}
 <= 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 el evento se `detail-type` transforme e `source` indique los detalles del APM donde se originó la alerta. Deben modificarse antes de su ingestión. La `incident-detection-response-identifier` clave aún no está presente y también debe añadirse antes de la ingestión.

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

Tras la transformación:


```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "UnHealthyHostCount",
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 <= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
```

```
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

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`

El `incident-detection-response-identifier` valor se toma del nombre de la alerta en función de la carga que envíe el APM. Las rutas de los nombres de las alertas de APM son diferentes de un APM a otro. Se debe configurar una función Lambda para que tome el nombre de la alarma de la ruta correcta de la carga útil JSON de APM recibida por Lambda y lo use como valor. `incident-detection-response-identifier`

`incident-detection-response-identifier`los valores deben ser únicos para cada tipo de alarma que se envíe a AWS Incident Detection and Response. Cada nombre único que aparezca en el `incident-detection-response-identifier` debe proporcionarse al equipo de detección y respuesta a incidentes de AWS durante la incorporación. Los eventos que tienen un valor desconocido o que falta en la `incident-detection-response-identifier` clave no se procesan.

Ingiera alarmas de los APM con integración directa EventBridge

En el siguiente tema se muestra el proceso de envío de alarmas a AWS Incident Detection and Response desde las herramientas de monitoreo del rendimiento de las aplicaciones (APM) que tienen una integración directa con Amazon EventBridge. Para obtener una lista completa de los APM

que tienen una integración directa con Amazon EventBridge, consulta EventBridgeIntegraciones de Amazon.

Puedes implementar la CloudFormation plantilla proporcionada o configurar esta integración manualmente. Antes de configurar la integración, compruebe que el rol AWS vinculado al servicio (SLR) `AWSServiceRoleForHealth_EventProcessor` se haya creado en sus cuentas.

Opción 1: usar CloudFormation

Hay disponible una CloudFormation plantilla para simplificar el proceso de creación de la infraestructura de integración necesaria para transferir las alarmas a AWS Incident Detection and Response desde su integración de APM con Amazon EventBridge.

> **Note**
>
> - Se incurre en costos adicionales por los recursos implementados a través de esta CloudFormation plantilla (por ejemplo, Lambda y EventBridge). Para obtener más información sobre los precios de estos servicios, consulte AWS Precios.
> - Implemente esta CloudFormation plantilla en todas las AWS cuentas y regiones en las que AWS Incident Detection and Response necesite incorporar alarmas. Los incidentes y los casos de soporte se abren en la AWS cuenta desde la que se recibió la alerta de APM.
> - Este documento usa New Relic como ejemplo, sin embargo, la CloudFormation plantilla se puede usar para cualquier APM que tenga una integración de SaaS con Amazon. EventBridge
> - Tras probar la integración, elimina las declaraciones logger.info () del `TransformLambdaFunction` para evitar que la carga aparezca en Amazon Logs. CloudWatch

Requisitos previos para implementar esta plantilla: CloudFormation

- Se debe configurar una fuente de eventos para socios en Amazon EventBridge. Para obtener instrucciones sobre cómo configurar su APM como fuente de eventos, consulte Recibir eventos de un socio de SaaS de Amazon EventBridge en la Guía del usuario de EventBridge Amazon.
- La `TransformLambdaFunction` (función Lambda) de la plantilla debe modificarse `["detail"]["incident-detection-response-identifier"]` para establecerla en el valor deseado en función de la ruta JSON del nombre de la alerta en la carga útil de APM.

Pasos previos:

1. Abre la EventBridge consola. En el menú de integración, seleccione Fuentes de eventos asociadas.
   - Busca tu APM en el cuadro de EventBridge socios de Amazon.
   - Selecciona Configuración y, a continuación, sigue las instrucciones que se proporcionan.
     - Nota: el último paso consiste en seleccionar Asociar con Event Bus en la consola como fuente de eventos del partner. Al seleccionar esta opción, se crea automáticamente un bus de eventos asociado con el mismo nombre que la fuente de eventos del socio (los nombres deben coincidir).
   - Copie el nombre del bus de eventos asociado o de la fuente. El bus de eventos o la fuente se utilizan como parámetro, denominado`PartnerEventBusNameParameter`, al implementar la CloudFormation plantilla.
     - Ejemplo de New Relic: `aws.partner/newrelic.com/1234567/source_name`
   - Copie la primera parte del bus o fuente de eventos del partner para introducirla en ella `PartnerEventBusPrefixParameter` al implementar la CloudFormation plantilla.
     - Un ejemplo de New Relic es `aws.partner/newrelic.com`
2. Descarga y edita la CloudFormation plantilla.
   - Ubique el `TransformLambdaFunction` en la plantilla
   - `def lambda_handler(event, context)event["detail"]["incident-detection-response-identifier"]`Establezca en la ruta json donde el nombre de la alarma aparece en la carga útil JSON de la alarma APM. Cada APM tendrá una ruta diferente. A continuación se muestran algunos ejemplos, pero sus cargas útiles específicas pueden diferir.
     - Ejemplo de New Relic:. `event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`
     - Ejemplo de Datadog: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
     - Ejemplo de Splunk: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
   - Guarde la CloudFormation plantilla.

Implementación de la CloudFormation plantilla:

1. Abre la CloudFormation consola en tu cuenta y región de destino.
2. Elige Crear pila, con nuevos recursos (estándar)
   - Selecciona Elegir una plantilla existente, Cargar un archivo de plantilla, Elegir archivo y, a continuación, carga la CloudFormation plantilla que guardaste localmente.
3. Especifica los detalles de la pila:
   - Introduzca un nombre de pila (ejemplo:`NewRelicIntegrationForIDR`).
   - Especifique los valores de los parámetros obtenidos al completar el requisito previo.
     - APMNameParameter(Ejemplo:`NewRelic`)
     - PartnerEventBusNameParameter(Ejemplo:`aws.partner/newrelic.com/1234567/source_name`)
     - PartnerEventBusPrefixParameter(Ejemplo:`aws.partner/newrelic.com`)
   - Elija Siguiente.
4. Configure las opciones de pila:
   - Desplázate hasta el final de la página y marca la casilla CloudFormation para permitir la creación de recursos de IAM con nombres personalizados.
5. Revise y cree:
   - Compruebe que los valores de los parámetros estén configurados correctamente y seleccione Enviar.
6. La CloudFormation pila implementa los recursos necesarios para integrar sus eventos de APM en AWS Incident Detection and Response. Espere a que aparezca el estado de la pila. `CREATE_COMPLETE`
7. La CloudFormation pila crea los siguientes recursos, suponiendo que los valores del ejemplo se introdujeron en los parámetros de New Relic y se ejecutaron en la US-EAST-1 región.
   - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
   - EventBridgeRule: AWS. partner/newrelic. com/1234567/nombre_fuente | NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
   - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission - [caden_aleatoria]

Pruebas de integración

Tras implementar la pila, pruebe la integración enviando una carga útil de prueba desde su APM:

1. Navegue hasta la consola Lambda y seleccione la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` función. Elija la pestaña Supervisar.
2. Busque una invocación correcta en los gráficos métricos.
3. Selecciona Ver Amazon CloudWatch Logs para comprobar si las transmisiones de registros contienen tu carga útil de prueba o si hay algún error.

Compartir el ARN de su bus de eventos con AWS Incident Detection and Response

1. Abre la Amazon EventBridge Console. Selecciona los autobuses del evento.
2. Copie el ARN del bus de eventos personalizado creado como parte de la CloudFormation pila (ejemplo: *`arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`*.)
   - Añada este ARN al campo «ARN del bus de EventBridge eventos» de la sección «Alarmas Third-Party APM» de su. Cuestionario de ingestión de alarmas: descripción general
3. Durante el proceso de incorporación, AWS Incident Detection and Response crea una EventBridge regla administrada en este bus de eventos personalizado para incorporar las alarmas de APM.

Opción 2: integración manual

Complete los siguientes pasos para cada AWS cuenta y AWS región desde la que AWS Incident Detection and Response necesite ingerir las alarmas. AWS Incident Detection and Response recomienda configurar las alarmas en la misma AWS cuenta y región que los recursos de la aplicación para que sea más rápido identificar e investigar los recursos afectados. Los incidentes y los casos de soporte se abren en la AWS cuenta desde la que se recibió la alerta de APM.

1. Crea un bus de eventos para EventBridge socios configurando tu APM como fuente de eventos para EventBridge socios de Amazon (por ejemplo,`aws.partner/apm_name/integrationName`). Para obtener instrucciones sobre cómo configurar tu APM como fuente de eventos, consulta Recibir eventos de un socio de SaaS de Amazon. EventBridge
2. Lleve a cabo una de las siguientes operaciones:

- (Recomendado) Crea un bus de eventos EventBridge personalizado con el nombre. `$YourApmName-AWSIncidentDetectionResponse-EventBus`
- (Alternativa) Utilice el bus de EventBridge eventos predeterminado en lugar de un bus de eventos personalizado.

AWS Incident Detection and Response instalará una regla administrada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) en el bus de eventos personalizado o predeterminado a través de la `AWSServiceRoleForHealth_EventProcessor` SLR. El origen de la regla será el bus de eventos personalizado o predeterminado, el destino de la regla será AWS Incident Detection and Response y la regla coincidirá con el patrón de ingesta de eventos de APM de terceros.

3. Cree una función Lambda con el nombre de transformar `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` los eventos del bus de eventos de su socio. Los eventos transformados coincidirán con la regla `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` gestionada.
   - 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. Esto permite que la estructura de carga útil de JSON transformada coincida con el patrón de reglas administradas.
   - Defina el objetivo de la función Lambda en el bus de eventos personalizado (recomendado) creado en el paso 2 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 creó en el paso 1 (`aws.partner/apm_name/integrationName`). El objetivo de la regla es la función Lambda que creó en el paso 3 ()`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`. Para obtener instrucciones sobre cómo definir tu EventBridge regla, consulta EventBridge las reglas de Amazon.

Para ver un ejemplo paso a paso sobre cómo configurar manualmente las integraciones de los buses de eventos de los socios con AWS Incident Detection and Response, consulte Integrar notificaciones de Datadog y Splunk.

Ingiera alarmas de los APM sin una integración directa con EventBridge

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

Puede implementar una CloudFormation plantilla o configurar la integración manualmente. Antes de configurar la integración, compruebe que el rol AWS vinculado al servicio (SLR) `AWSServiceRoleForHealth_EventProcessor` se haya creado en sus cuentas.

Opción 1: usar CloudFormation Plantilla

Hay disponible una CloudFormation plantilla para simplificar el proceso de creación de la infraestructura de integración necesaria para incorporar alarmas a AWS Incident Detection and Response desde su APM que no tiene una integración directa con Amazon EventBridge.

Consideraciones antes de implementar esta plantilla CloudFormation

- Esta solución utiliza un autorizador Lambda de API Gateway para comparar un token secreto transferido en la carga útil desde su APM con un token ingresado. AWS Secrets Manager Si el token no coincide, se devolverá una política con una denegación explícita. Para obtener más información, consulte Autorizadores Lambda.
- Según el modelo de responsabilidad AWS compartida, es su responsabilidad asegurarse de utilizar un enfoque de autenticación que cumpla con los requisitos de seguridad de su organización. Recomendamos utilizar AWS Secrets Manager un servicio similar, en lugar de almacenar información confidencial, como claves de API o tokens de autorización, como variables codificadas de forma rígida. Para obtener más información, consulte Cree y administre secretos con AWS Secrets Manager.
- Para ver un ejemplo adicional de cómo implementar el código de autenticación de Hash-Based mensajes (HMAC), consulte receive-webhooks en la página de Github de aws-samples. Para obtener más información sobre la implementación de la autorización de token, consulte un ejemplo de la función Lambda del autorizador de TOKEN en la documentación de API Gateway.
- La solución usa RateLimitBurstLimit, y una cuota en API Gateway para controlar los volúmenes de solicitudes. Estas herramientas limitan el número de solicitudes que se pueden procesar en un tiempo determinado. Esto ayuda a evitar la sobrecarga del sistema y mantiene estable el servicio. Para obtener más información sobre la regulación, consulta la Guía para desarrolladores de API Gateway.

- Considere la posibilidad de utilizar el AWS Web Application Firewall (WAF) para proteger la API Gateway de las direcciones IP incorrectas conocidas. Esto reduce el riesgo de que los atacantes inunden la API con solicitudes falsas que podrían bloquear los eventos de registro reales.
- AWS Secrets Manager los valores de los tokens deben almacenarse en la herramienta de monitoreo del rendimiento de las aplicaciones (APM) como un encabezado HTTP. Asegúrese de rotar el token de forma regular como práctica recomendada de seguridad.
- Se incurrirá en costos adicionales por los recursos implementados a través de esta CloudFormation plantilla (por ejemplo, Lambda y EventBridge). Para obtener más información sobre los precios de estos servicios, consulte AWS Precios.
- Tras probar la integración, elimine las sentencias logger.info () de la (función `TransformLambdaFunction` Lambda) para evitar que las cargas útiles aparezcan en Amazon Logs. CloudWatch
- Implemente esta CloudFormation plantilla en todas las AWS cuentas y regiones desde las que AWS Incident Detection and Response necesite recibir alarmas.

Preparación de la CloudFormation plantilla:

Nota: Los pasos de integración utilizan Dynatrace como ejemplo; sin embargo, esta plantilla se puede utilizar para cualquier APM que pueda enviar cargas útiles a una API Gateway.

1. Descarga y abre la plantilla.CloudFormation
2. `APIGWUsagePlan`Ubícala en la plantilla. Revise los valores configurados para `RateLimitBurstLimit`, y `Quota Limit` que están establecidos en 20, 50 y 2000 de forma predeterminada. Ajuste los valores para que se ajusten a sus requisitos.
3. Ubique `AuthorizerLambdaFunction` en la plantilla. Esta función Lambda sirve como ejemplo de un mecanismo de autenticación. Extrae un valor simbólico de un encabezado llamado`authorizationToken`, que se transfiere desde su APM. Puede modificar este código para adaptarlo a las políticas de seguridad y los requisitos de APM de su organización.
4. Búscalo `TransformLambdaFunction` en la plantilla. Sustituya la ruta del diccionario por la ruta del nombre de la alarma que se envía en la carga JSON desde su APM. `raw_json["detail"]["ProblemTitle"]` Deja esto como está para Dynatrace.

Implementación de la plantilla CloudFormation :

1. Abre la CloudFormation consola en tu cuenta de destino y Región de AWS.

2. Elija Crear pila, Con nuevos recursos (estándar).
   - Seleccione Elegir una plantilla existente, Cargar un archivo de plantilla, Elegir archivo y, a continuación, cargue la CloudFormation plantilla que guardó localmente.
3. Especifica los detalles de la pila:
   - Introduzca un nombre de pila (por ejemplo, *`DynatraceIntegrationForIDR`*.)
   - APMNameParameter (ejemplo, *`Dynatrace`*.)
   - Elija Siguiente.
4. Configure las opciones de pila:
   - Desplázate hasta el final de la página y marca la casilla CloudFormation para permitir la creación de recursos de IAM con nombres personalizados.
5. Revise y cree:
   - Compruebe que los valores de los parámetros estén configurados correctamente y seleccione Enviar.
6. El CloudFormation conjunto implementa los recursos necesarios para integrar sus eventos de APM en AWS Incident Detection and Response. Espere a que el estado de la CloudFormation pila sea CREATE_COMPLETE.
7. La CloudFormation pila crea los siguientes recursos suponiendo que el valor de ejemplo `Dynatrace` se haya introducido en los parámetros y se haya ejecutado en la región. US-EAST-1
   - Nombre secreto: DynatraceMySecretTokenName (se creará un valor secreto aleatorio junto a la clave secreta APMSecureToken)
   - Recursos de API Gateway:
     - Nombre de la API: Dynatrace-AWSIncidentDetectionResponse-APIGW
     - Nombre artístico: Dynatrace-Stage-Prod
     - Autorizadores: Dynatrace-APIGW-Authorizer
     - Plan de uso: APIGW_ Throttling_Plan
   - Funciones Lambda:
     - Función de autorización: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - Función de transformación: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - EventBus Nombre personalizado: Dynatrace-AWSIncidentDetectionResponse-EventBus
   - Función de IAM:
     - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1

- AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1

8. Registre la URL del Webhook y el valor del token:
   - Abre la consola de API Gateway y elige el nombre de la API que creaste como parte de la CloudFormation pila.
   - Selecciona Stages en el menú de navegación de la izquierda, expande el nombre de la etapa con el signo + y, a continuación, selecciona POST. Registra la URL de invocación. Configura esta URL en tu APM como destino para enviar webhooks en caso de eventos de alarma.
   - Abre la AWS Secrets Manager consola y elige el nombre secreto creado como parte de la CloudFormation pila. (Ejemplo: DynatraceMySecretTokenName.)
     - En la pestaña Valor secreto, selecciona Recuperar valor secreto. Verás la clave secreta como APMSecureToken. Registra el valor secreto. No comparta este valor secreto con nadie.

Pruebas de integración

Tras implementar la pila, pruebe la integración enviando una carga útil de prueba desde su APM:

1. Navegue hasta la Consola Lambda y seleccione `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` la función. Elija la pestaña Supervisar.
2. Busque una invocación correcta en los gráficos métricos.
3. Selecciona Ver Amazon CloudWatch Logs para comprobar si las transmisiones de registros contienen tu carga útil de prueba o si hay algún error.

Compartir el ARN de su bus de eventos con AWS Incident Detection and Response

1. Abre la Amazon EventBridge Console. Selecciona los autobuses del evento.
2. Copie el ARN del bus de eventos personalizado creado como parte de la CloudFormation pila, por ejemplo:. `arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`
   - Añada este ARN al campo «ARN del bus de EventBridge eventos» de la sección «Alarmas Third-Party APM» de su. Cuestionario de ingestión de alarmas: descripción general
3. Durante el proceso de incorporación, AWS Incident Detection and Response creará una EventBridge regla administrada en este bus de eventos personalizado para ingerir las alarmas de APM.

Opción 2: integración manual

Siga los siguientes pasos para configurar la integración con AWS Incident Detection and Response.

1. Cree una Amazon API Gateway para aceptar la carga útil de su APM.
2. Defina una función Lambda para la autorización mediante un token de autenticación.
3. Lleve a cabo una de las siguientes operaciones:
   - (Recomendado) Cree un bus de eventos EventBridge personalizado con el nombre`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternativa) Utilice el bus de EventBridge eventos predeterminado en lugar de un bus de eventos personalizado.
4. Defina una función de transformación Lambda para 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.
   - La API Gateway debe invocar la función Transform Lambda, que transformará la carga útil pasada por la API Gateway.
   - La función Transformar Lambda debe escribir los eventos transformados en el bus de eventos definido en el punto 3 anterior.
5. Configura tu APM para enviar notificaciones a la URL generada desde la API Gateway.

Administre alarmas de APM con la integración directa de Amazon SNS

Si su APM admite el envío de alarmas a los temas de Amazon SNS, puede seguir esta guía para incorporar sus alarmas de APM a AWS Incident Detection and Response.

Puede implementar la CloudFormation plantilla proporcionada o configurar esta integración manualmente. Antes de configurar la integración, compruebe que el rol AWS vinculado al servicio (SLR) `AWSServiceRoleForHealth_EventProcessor` se haya creado en sus cuentas.

Opción 1: usar CloudFormation

Hay disponible una CloudFormation plantilla para simplificar el proceso de creación de la infraestructura de integración necesaria para incorporar alarmas a AWS Incident Detection and Response desde su APM con la integración de Amazon SNS.

> **Note**
>
> - Se incurrirá en costos adicionales por los recursos implementados a través de esta CloudFormation plantilla (por ejemplo, Lambda y EventBridge). Para obtener más información sobre los precios de estos servicios, consulte AWS Precios.
> - Esta CloudFormation plantilla debe implementarse en todas las AWS cuentas y regiones desde las que AWS Incident Detection and Response necesite ingerir las alarmas.
> - Los ejemplos que se proporcionan en este documento son para Grafana, sin embargo, esta plantilla se puede utilizar para cualquier APM que tenga una integración directa con Amazon Simple Notification Service.
> - Por motivos de seguridad, AWS recomienda eliminar `logger.info()` las declaraciones del `TransformLambdaFunction` para evitar que la carga se registre en Amazon CloudWatch Logs.

Requisitos previos para implementar esta CloudFormation plantilla:

- Debe crearse un tema estándar de Amazon Simple Notification Service para recibir los eventos de alarma de su APM. Cree un tema de SNS en la consola de Amazon Simple Notification Service.
- El `TransformLambdaFunction` contenido de la plantilla debe modificarse `["detail"]["incident-detection-response-identifier"]` para establecer el valor deseado en función del APM que se utilice.

Cumplimiento del requisito previo:

1. Abra la consola Amazon SNS y, a continuación, seleccione Temas. Copie el ARN del tema estándar de Amazon SNS creado para recibir eventos de alarma de su APM.
   - Ejemplo: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. Descargue y abra la plantilla CloudFormation
   - Ubique el `TransformLambdaFunction` en la plantilla
     - Seleccione `def lambda_handler(event, context)` la ruta json en la `event["detail"]["incident-detection-response-identifier"]` que aparece el nombre de la alarma en la carga útil JSON del registro SNS.

- Cualquier evento enviado a `TransformLambdaFunction` través de SNS tiene una estructura de carga principal como. `event["Records"][n]["Sns"]["Message"]` El origen real de la carga útil desde la fuente (APM) está incluido dentro de la estructura principal.
- Ejemplo de Grafana: `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

Implementación de la CloudFormation plantilla:

1. Dirígete a la CloudFormation consola de la cuenta y la región en las que necesitas configurar la integración.
2. Navega hasta CloudFormation.
   - Elige Crear pila, con nuevos recursos (estándar)
     - Selecciona Elegir una plantilla existente, Cargar un archivo de plantilla, Elegir archivo y, a continuación, carga la CloudFormation plantilla que guardaste localmente.
3. Especifica los detalles de la pila:
   - Introduzca un nombre de pila Ejemplo: `<your-apm-name>IntegrationForIDR`
   - Especifique los valores de los parámetros obtenidos al completar el requisito previo
     - APMNameParameterEjemplo: `Grafana`
     - Ejemplo de TriggerSNParameter: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
   - Elija Siguiente.
4. Configure las opciones de pila:
   - Desplázate hasta el final de la página y marca la casilla de verificación CloudFormation para permitir la creación de recursos de IAM con nombres personalizados.
5. Revise y cree:
   - Compruebe que los valores de los parámetros estén configurados correctamente y, a continuación, seleccione Enviar.
6. La CloudFormation pila desplegará los recursos necesarios para integrar sus eventos de APM en AWS Incident Detection and Response. Espere a que el estado de la CloudFormation pila sea CREATE_COMPLETE.
7. La CloudFormation pila crea los siguientes recursos suponiendo que los valores del ejemplo se ingresaron en los parámetros de Grafana y se ejecutaron en la EU-WEST-1 región.

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

Pruebas de integración

Una vez que la CloudFormation pila se haya desplegado correctamente, puede validar la integración enviando una carga útil de prueba desde su APM. Una vez que la carga útil de prueba se envíe desde tu APM:

1. Navegue hasta la consola Lambda y seleccione la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` función. A continuación, seleccione la pestaña Monitor.
2. Se debe observar una invocación exitosa en los gráficos métricos.
3. Selecciona Ver Amazon CloudWatch Logs. Puede comprobar los eventos de registro de los flujos de registro para confirmar que la carga útil de prueba enviada desde su APM está presente o si se ha encontrado algún error.

Compartir el ARN de su bus de eventos con AWS Incident Detection and Response

1. Navega hasta Amazon EventBridge Console. Selecciona los autobuses del evento.
2. Registre el ARN del bus de eventos personalizado implementado como parte de la CloudFormation pila, por ejemplo:. `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`
   - Proporcione el ARN de este bus de eventos personalizado a AWS Incident Detection and Response en el campo «ARN del bus de EventBridge eventos» de la sección «Alarmas Third-Party APM» del. Cuestionario de ingestión de alarmas: descripción general
3. Durante el proceso de incorporación, AWS Incident Detection and Response creará una EventBridge regla administrada en este bus de eventos personalizado para ingerir las alarmas de APM.

Opción 2: integración manual

1. Abra la consola de Amazon SNS y cree un tema de Amazon SNS estándar `[apm_name]-sns` denominado para recibir eventos de alarma de su APM. Asegúrese de seleccionar Estándar (no FIFO) como tipo de tema. Anote el ARN del tema de Amazon SNS creado.
2. Lleve a cabo una de las siguientes operaciones:
   - (Recomendado) Cree un bus de eventos EventBridge personalizado con el nombre. `[apm_name]-AWSIncidentDetectionResponse-EventBus`
   - (Alternativa) Utilice el bus de EventBridge eventos predeterminado en lugar de un bus de eventos personalizado.

   AWS Incident Detection and Response instalará una regla administrada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) en el bus de eventos personalizado o predeterminado a través de la `AWSServiceRoleForHealth_EventProcessor` SLR. El origen de la regla será el bus de eventos personalizado o predeterminado, el destino de la regla será AWS Incident Detection and Response y la regla coincidirá con el patrón de ingesta de eventos de APM de terceros.
3. Cree una función Lambda con el nombre de transformar sus `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` cargas útiles de SNS.
   - Los eventos transformados deben cumplir los requisitos de carga útil establecidos en Requisitos de carga útil para ingerir alertas de APM con EventBridge
   - Defina el objetivo de la función Lambda en el bus de eventos personalizado (recomendado) creado en el paso 2 o en el bus de eventos predeterminado.
4. Defina el tema SNS como activador de la función `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` Lambda.
   - En la página «Añadir activadores», busque «SNS».
   - Añada el ARN de su tema de SNS dedicado creado en el paso 1.
   - Selecciona «Añadir».
5. Siga la documentación de APM para configurar un destino de SNS para las cargas útiles de APM que AWS Incident Detection and Response debe ingerir.

AWS Incident Detection and Response instalará una regla administrada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) en el bus de eventos

personalizado o predeterminado a través de la `AWSServiceRoleForHealth_EventProcessor` SLR. El origen de la regla será el bus de eventos personalizado o predeterminado, el destino de la regla será AWS Incident Detection and Response y la regla coincidirá con el patrón de ingesta de eventos de APM de terceros.

Ajustes de optimización y monitoreo de alarmas

Para garantizar una precisión óptima en la detección de incidentes, nuestros ingenieros de gestión de incidentes evalúan continuamente el rendimiento de las alarmas en relación con sus cargas de trabajo críticas. Proporcionamos los cambios recomendados en la configuración de las alarmas, que usted debe realizar, y colaboramos de forma proactiva con usted y sus administradores técnicos de cuentas (TAM) para afinar estos ajustes.

Si los datos de supervisión indican que es posible que las alarmas no estén alineadas con las operaciones fundamentales de la empresa, por ejemplo, cuando las alertas se activan sin que ello repercuta en los clientes o cuando los estados de alarma fluctúan con frecuencia, recomendamos eliminar las alarmas no críticas e incorporarlas de forma que reflejen mejor el impacto crítico en la carga de trabajo. Esto ayuda a mantener la eficacia general de su cobertura de respuesta a incidentes.

Revisión y comentarios sobre las alarmas

AWS Incident Detection and Response lleva a cabo revisiones exhaustivas de sus alarmas antes de incorporarlas para su supervisión. Las alarmas se evalúan en función de criterios técnicos de aceptación, incluidos los parámetros de configuración, la calidad de los datos y la eficacia de las alertas.

Sobre la base de esta revisión, se proporcionan dos tipos de comentarios:

- Requisitos de configuración obligatorios: estos cambios deben implementarse para que se acepten las alarmas.
- Recomendaciones de mejora opcionales: estos cambios mejoran la eficacia de las alarmas, pero no son obligatorios para su aceptación.

Tras recibir estos comentarios, puede decidir continuar incorporando únicamente las alarmas aceptadas y las que necesiten mejoras opcionales, mientras trabaja en los cambios de configuración de las alarmas con requisitos de configuración obligatorios en paralelo.

Como alternativa, puede implementar todos los cambios antes de ponerlos en marcha. Este enfoque amplía el plazo de incorporación, en función del número de alarmas que requieren ajustes.

Las alarmas se activan

Una vez completada la ingesta de alarmas, AWS Incident Detection and Response permite monitorear su carga de trabajo. A partir de este momento, las alarmas incorporadas se supervisan activamente y AWS Incident Detection and Response lo pone en contacto según el manual de la carga de trabajo cuando las alarmas incorporadas pasan al estado de ALARMA.

Salidas clave

- AWS Incident Detection and Response confirma que su carga de trabajo está activa y monitorizada.

Pasos siguientes

- Para comprobar que las alarmas incorporadas activan AWS Incident Detection and Response según lo previsto, consulte. Pruebe las cargas de trabajo integradas en la detección y respuesta a incidentes
- Para realizar cambios en las alarmas incorporadas, el manual o la información sobre la carga de trabajo, consulte. Solicita cambios en una carga de trabajo integrada en la sección Detección y respuesta a incidentes

Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response (ruta de excepciones)

> **Note**
>
> Si no puede usar la CLI de IDR para incorporar su carga de trabajo, utilice los siguientes cuestionarios para la incorporación de cargas de trabajo y alarmas.

En este tema 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 desencadenan la creación de incidentes en Incident Detection and Response para su carga de trabajo, así como información resumida sobre con quién contactar y qué medidas 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 la carga de trabajo:

- Versión en inglés
- Versión en japonés

Descargue el cuestionario de ingestión de alarmas:

- Versión en inglés
- Versión en japonés

Cuestionario sobre la 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.

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. **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.	Nombre de la aplicación: Optimax entorno: Producción
Una lista de Servicio de AWS los elementos utilizados por esta carga de trabajo, los Cuenta de AWS elementos y Región de AWS los componentes en los que se encuentran.	Servicios de AWS: Route 53, ALB, ECS,... Cuentas: 123456789101, 123456789102,... US-EAST-1Regiones: US-WEST-2,,...

Cuestionario de ingestión de alarmas: descripción general

En el cuestionario de ingesta de alarmas, usted especifica las alarmas críticas para su carga de trabajo que desea activar con AWS Incident Detection and Response, así como los contactos que desea que un ingeniero de gestión de incidentes active cuando se activen estas alarmas.

El cuestionario de ingesta de alarmas se divide en las siguientes secciones:

- Sección de contactos: en primer lugar, especifique los contactos principales que se incluirán en el Soporte caso creado con AWS Incident Detection and Response cuando se active una alarma, así como la aplicación de conferencias que prefiera para los puentes de incidentes. Si no se proporciona ninguna preferencia de puente, AWS Incident Detection and Response creará un puente de incidentes durante los incidentes. A continuación, especifique los contactos de escalamiento y los intervalos de tiempo para contactarlos cuando no se pueda contactar con los contactos principales. Por último, enumere los contactos que deberían recibir actualizaciones periódicas sobre el estado del incidente a través del servicio de asistencia durante el incidente.
- Matriz de alarmas: enumere el conjunto de alarmas que activarán AWS Incident Detection and Response cuando se activen. Consulte los «Criterios de alarma críticos» definidos por AWS Incident Detection and Response al seleccionar las alarmas para la incorporación. Para obtener más información, consulte Definición de alarma.
  - Amazon CloudWatch Alarms (deja esta sección en blanco si no tienes CloudWatch alarmas Amazon)
  - Alarmas APM de terceros (deja esta sección en blanco si no tienes alarmas APM de terceros)
    - EventBridge EventBus ARN: es el ARN del ARN personalizado que ha creado en o EventBus . Ingiera alarmas de los APM con integración directa EventBridge Ingiera alarmas de los APM sin una integración directa con EventBridge
    - Identificadores de alarma: comparten el número de cuenta, la región y el nombre de la alarma APM.

Cuestionario sobre la ingesta de alarmas: preguntas del manual

Preguntas del manual

Pregunta	Respuesta de ejemplo
AWS involucra a los contactos relacionados con la carga de trabajo a lo largo del caso Soporte . ¿Quién es el contacto principal cuando se activa una alarma relacionada con esta carga de trabajo? Especifique su aplicación de conferencias preferida y AWS solicitará estos detalles durante un incidente.	Equipo de aplicaciones app@example.com +61 2 3456 7890

Pregunta	Respuesta de ejemplo
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.	
Si el contacto principal no está disponible durante un incidente, indique los contactos de escalamiento y el cronograma 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

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 detección y respuesta a incidentes de AWS:

- Las alarmas de detección y respuesta a incidentes de AWS solo deben pasar al estado de «alarma» si el negocio tiene un impacto significativo en la carga de trabajo monitoreada (pérdida de experiencia del revenue/degraded 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 caso por caso a medida que se producen los eventos. El equipo de gestión de incidentes trabaja con sus gestores técnicos de cuentas (TAM) 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 está interactuando con el equipo de gestión de incidentes de forma innecesaria y periódica.

> **Important**
>
> Proporcione direcciones de correo electrónico de distribución grupal al proporcionar las direcciones de contacto, de modo que pueda controlar las adiciones 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 matricial de CloudWatch alarmas para alarmas

CloudWatch ARN de alarma	Contacto principal para esta alarma.	Especifique la más relevante Servicio de AWS para que esta alarma se active con el ingeniero adecuado. Introduzc a N/A si no es necesario.

	(Si es diferente del contacto principal de la carga de trabajo)	
Ejemplo: `arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response`	Ejemplo: Sam Smith, administrador de aplicaciones sam.smith@example.com +61 2 3456 7890	Ejemplo: ECS

Tabla matricial de alarmas para alarmas APM de terceros

EventBridge Autobús de eventos (ARN)
 	
(Esto se creó como parte de la integración de APM de terceros para enrutar las alertas a AWS Incident Detection and Response).
		Ejemplo: (Habrá un autobús de eventos por cada Account/Region combinación)
		
		`arn:aws:events:us-east-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`
		
		`arn:aws:events:us-west-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`	

Identificador de alarma	¿Qué representa esta métrica? ¿Por qué es importante esta alarma?	Contacto principal para esta alarma. (Si es diferente del contacto principal de la carga de trabajo)	Especifique la más relevante Servicio de AWS para que esta alarma se active con el ingeniero adecuado. Introduzca N/A si no es necesario.
Ejemplo:	Ejemplo:	Ejemplo:	Ejemplo:

ALB_5xx_ Target_Response ID de cuenta: 123456789012 Región: us-east-1	Esta métrica representa las respuestas a las transacciones de los objetivos detrás del ALB. Si 5XX errores superan el umbral, se trata de un fallo grave en el procesamiento de las transacciones comerciales.	Sam Smith, administrador de aplicaciones sam.smith@example.com +61 2 3456 7890	ECS

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, 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 materia de detección y respuesta a incidentes

AWS Incident Detection and Response utiliza la información recopilada de la incorporación de la CLI de IDR para desarrollar manuales de gestión de los incidentes que afectan 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 la incorporación de la carga de trabajo.

Resultados clave:

- Finalización de la definición de la carga de trabajo en AWS Incident Detection and Response.
- Finalización de las alarmas y los manuales de detección y respuesta a incidentes de AWS.

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

Ejemplo de manual

Example Ejemplo de manual

Description (Descripción)

Este documento está destinado a [CustomerName] - [WorkloadName].

Paso: Prioridad

Acciones prioritarias

1. Envíe la primera correspondencia sobre el Soporte caso al cliente de la siguiente manera.

```
Hello,

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

Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
```

Paso: Información

Planes de participación

En esta sección se describen los planes de participación aplicables a este manual y solo se incluyen los datos de contacto. Se hará referencia a los planes de participación en los planes de comunicación paso a paso.

- Compromiso inicial

  El equipo de detección y respuesta a incidentes de AWS añade las direcciones de las partes interesadas de los clientes a continuación al Soporte caso. AWS las partes interesadas son para otras partes interesadas a las que podría ser necesario informar sobre cualquier problema.

  - Clientes interesados: correo electrónico del cliente 1; correo electrónico del cliente 2; móvil 1

- AWS Partes interesadas: aws-idr-oncall@amazon.com; correo electrónico del equipo; etc.
- Contactos únicos: [Son contactos de correo electrónico que solo se incluyen en la primera comunicación. Elimine estos contactos una vez finalizada la primera comunicación. Podrían ser direcciones de correo electrónico de los clientes que buscan llamadas, como locer-duty, que no deben estar localizadas para cada correspondencia. Añade instrucciones explícitas en la sección «Prioridad», «Planes de comunicación», sobre cómo utilizarlos solo si está disponible One Time Only Contacts.]

- Configuración de llamadas en caso de incidente

  Indique si el cliente necesita AWS Incident Detection and Response para crear un puente, si el cliente utiliza un puente estático o si proporcionará un puente cuando se abra un incidente.

  (Elija una opción según las preferencias del cliente)

  - La detección y respuesta a incidentes de AWS crean un Amazon Chime/Zoom Bridge
  - El cliente proporcionó un puente estático
    - Número de conferencia: **<** Insert Conference number **>**
  - El cliente proporciona los detalles del puente para cada incidente respondiendo a la comunicación enviada por el equipo de detección y respuesta a incidentes de AWS.
  - Otros: especifique los detalles.

- Aumento de la participación

  AWS Incident Detection and Response contactará con los siguientes contactos cuando los contactos del plan de participación inicial no respondan a los incidentes.

  Para cada contacto de escalación, indique si debe añadirse al Soporte caso, llamar por teléfono o ambos.

  - Asegúrese de haber llamado al contacto inicial, si corresponde, antes de escalar la escala.
  - Primer contacto de escalación: [escalada EmailAddress #1]/[PhoneNumber] - Espere XX minutos antes de escalar a este contacto.
    - [Añadir contacto al caso/teléfono] este contacto.
  - Segundo contacto de escalada: [escalada EmailAddress #2]/[PhoneNumber] - Espere XX minutos antes de pasar a este contacto.
    - [Añadir contacto al caso/teléfono] este contacto.
  - etc.

Planes de comunicación

En esta sección se describe cómo los ingenieros de gestión de incidentes se comunican con las partes interesadas designadas fuera de los canales de comunicación y llamadas ante incidentes.

- Plan de comunicación de impacto

  Este plan se inicia cuando AWS Incident Detection and Response determina, a partir del paso Triage, que una alerta indica un posible impacto en un cliente.

  AWS Incident Detection and Response solicitará al cliente que se una al puente predeterminado, tal como se indica en Planes de participación: configuración de llamadas ante incidentes.

  (Elija uno en función de si One Time Only Contacts está disponible o no).

  1. Asegúrese de que las partes interesadas de los clientes no cuenten con los planes de participación: la participación inicial se añade al CC del caso.

  OR

  1. Asegúrese de que los clientes interesados y las partes interesadas se comuniquen una sola vez en los planes de participación: la participación inicial se agrega al CC del caso.
  2. Envía la notificación de compromiso al cliente según la siguiente plantilla:

     (Elige una opción)

     Plantilla de impacto: Amazon 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 2025, 3:30 PM UTC>
Please join the Amazon Chime Bridge below so we can start the steps outlined in
 your Runbook:
    Amazon Chime Meeting ID: <insert_Meeting_ID_here>
    Link to Amazon Chime Bridge: <insert_Link_here>
    International dial-in numbers: https://chime.aws/dialinnumbers/
```

     Plantilla de impacto: puente proporcionado por el cliente

```
The following alarm has engaged AWS Incident Detection and Response:
```

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

Plantilla de impacto: 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 2025, 3:30 PM UTC>
Please join the Bridge below so we can start the steps outlined in your Runbook:
    Conference Number: <insert_conference_number>
    Conference URL: <insert_bridge_URL>
```

3. Defina el caso como Acción pendiente del cliente.
4. Elimine los contactos únicos de la caja después de enviar la comunicación de impacto anterior. (Si los contactos de un solo uso están disponibles).
5. Siga el plan de intensificación de la participación mencionado anteriormente.
6. Si el cliente no responde en 30 minutos, desconéctelo y continúe monitoreando hasta que se recupere la alarma.

- Plan de comunicación sin impacto

  Este plan se inicia cuando una alarma se recupera antes de que la detección y respuesta a incidentes hayan completado la clasificación inicial.

  1. Antes de enviar la notificación sin impacto, verifique y, a continuación, elimine los and/or contactos de Soporte Case CC y, a continuación, elimine los contactos que figuran en los planes de participación (plan de participación inicial).

     ["NO añadas contactos de una sola vez"]. (Aplicable si los contactos de un solo uso están disponibles).
  2. Envía una notificación de no participación al cliente según la siguiente plantilla:

     Plantilla sin impacto

     ```
     AWS Incident Detection and Response received an alarm that has recovered for your
      workload.
     ```

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

3. Coloca el caso en Pending Customer Action.
4. Si el cliente no responde en 30 minutos, resuelve el caso.

Descripción general de la arquitectura de aplicaciones

En esta sección se proporciona una descripción general de la application/workload arquitectura para que los ingenieros de gestión de incidentes y de operaciones los conozcan.

- AWS Cuentas y regiones con servicios clave: lista de AWS cuentas con regiones compatibles con esta aplicación. Ayuda a los ingenieros a evaluar la infraestructura subyacente que respalda la aplicación.
  - 123456789012
    - US-EAST-1 - una breve descripción, según proceda
      - Amazon EC2: breve descripción, según proceda
      - DynamoDB: breve descripción, según proceda
      - etc.
    - US-WEST-1 - una breve descripción, según proceda
      - etc.
  - otra cuenta
    - etc.

Pruebe las cargas de trabajo integradas en la detección y respuesta a incidentes

Una vez Ingestión de alarmas finalizado, AWS Incident Detection and Response permite monitorizar la carga de trabajo y envía una Go-Live confirmación. Su carga de trabajo se monitorea activamente a partir de este momento.

Las pruebas de alarmas validan que las alarmas integradas activen AWS Incident Detection and Response según lo esperado, activen los manuales de ejecución adecuados y cualquier otra acción deseada, como la creación automática de casos si la seleccionó durante la ingesta de alarmas.

Las pruebas son opcionales, pero se recomienda encarecidamente. Eres responsable de validar tus mecanismos de respuesta antes de que se produzca un incidente real.

Opciones de prueba

AWS Incident Detection and Response ofrece dos opciones de prueba.

Opción 1: programada GameDay (recomendada)

Una programación GameDay es una simulación integral en vivo de lo que podría 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. GameDay Es una oportunidad para que formule preguntas o perfeccione las instrucciones para mejorar la participación.

Para programar una GameDay, sigue estos pasos:

1. Notifique a AWS Incident Detection and Response con una fecha preferida y un intervalo de tiempo de 1 hora, incluida la zona horaria. Proporcione un plazo de entrega de al menos 48 horas.
2. Planifique los recursos para el GameDay, incluidos su SRE/Ops equipo y los contactos de escalación.

GameDay horario:

1. Usted y AWS Incident Detection and Response se unen a la convocatoria.
2. Usted desactiva las acciones de alarma, si procede.
3. Para configurar manualmente las alarmas en el estado de ALARMA, siga las instrucciones que se indican en¿Cómo probar sus alarmas?.
4. AWS Incident Detection and Response confirma la recepción de la notificación de alarma.
5. AWS Incident Detection and Response responde a la alarma y se une al puente indicado en su manual.
6. Usted y AWS Incident Detection and Response confirman el GameDay resultado.

Opción 2: pruebas de alarmas fuera de línea

Puede probar las alarmas de forma independiente en cualquier momento sin programar una llamada. Al activar una alarma, AWS Incident Detection and Response se activa según su manual, tal como lo haría durante un incidente real.

Para realizar una prueba de alarma sin conexión a Internet, complete los siguientes pasos:

1. Para evitar acciones no deseadas, desactiva cualquier acción de CloudWatch alarma de Amazon.
2. Activa tus alarmas siguiendo las instrucciones que se indican en¿Cómo probar sus alarmas?.
3. En 5 minutos, se crea un caso de soporte en su nombre y AWS Incident Detection and Response se pone en contacto con usted según lo especificado en su manual.
4. Notifique al administrador de incidentes que está realizando una prueba de alarma fuera de línea.
5. El administrador de incidentes confirma qué cambios de estado de alarma se recibieron y valida las disposiciones de respuesta.

Si no se crea un caso de soporte en 5 minutos, envíe una solicitud de incidente para activar manualmente AWS Incident Detection and Response para la solución de problemas.

¿Cómo probar sus alarmas?

CloudWatch Alarmas Amazon

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

Utilice AWS Command Line Interface o AWS CloudShellpara configurar manualmente la alarma en el estado de ALARMA. Estos comandos cambian el estado de la alarma sin afectar a la carga de trabajo.

Para evitar acciones no deseadas, por ejemplo, el reinicio de la instancia Amazon EC2, desactive CloudWatch cualquier acción de alarma antes de cambiar el estado de la alarma. Puede

volver a activar las acciones de CloudWatch alarma una vez finalizadas las pruebas. Para obtener más información sobre cómo habilitar o deshabilitar las acciones de alarma, consulta DisableAlarmActionsy consulta EnableAlarmActionsla Amazon CloudWatch API Reference.

Desactivar las acciones de alarma:

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

Establezca el estado de alarma en ALARMA:

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

Re-enable acciones de alarma después de la prueba:

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

El estado de alarma vuelve a funcionar automáticamente en unos segundos.

Alarmas compuestas

El `set-alarm-state` comando no garantiza que las alarmas compuestas vuelvan al estado correcto. Como práctica recomendada, compruebe el estado de las alarmas compuestas tras la comprobación. Para restablecer manualmente una alarma compuesta, utilice el siguiente comando:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleCompositeAlarm" --state-value OK --
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, consulta SetAlarmStatela referencia de la CloudWatch API de Amazon.

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

Third-party Alarmas APM

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.

1. Desactiva las acciones de alarma en tu APM para evitar acciones no deseadas.
2. Modifique el umbral de alarma o el operador de comparación para forzar la alarma a pasar al estado de ALARMA. Esto activa una carga útil para AWS Incident Detection and Response.
3. Una vez finalizadas las pruebas, revierta el umbral o el operador de comparación cambia para restablecer el estado correcto de la alarma.

Resultados clave

Tras realizar las pruebas satisfactoriamente:

- Se confirma la entrada de la alarma y la configuración de la alarma es correcta.
- AWS Incident Detection and Response recibe las alarmas.
- Se crea un caso de soporte y se notifica a los contactos prescritos.
- AWS Incident Detection and Response lo contacta con los medios de conferencia prescritos.
- Se resuelven todas las alarmas y los casos de soporte generados durante las pruebas.

Preguntas frecuentes

¿Las pruebas de alarma son obligatorias?

No. Las pruebas son opcionales, pero se recomienda encarecidamente validar sus acuerdos de respuesta integrales antes de que se produzca un incidente real.

¿Se verá afectada mi carga de trabajo?

No. Sin embargo, durante las pruebas se activan todas las acciones de alarma configuradas en las alarmas, a menos que las desactive. Desactive las acciones de alarma antes de realizar las pruebas para evitar impactos no deseados.

¿A quién se notifica durante las pruebas?

Durante una sesión programada GameDay, se contacta con todos los contactos y rutas de escalamiento de tu lista de seguimiento para su verificación. Durante las pruebas de alarma fuera de línea, solo se notifica al contacto inicial especificado durante la activación de la alarma.

¿Puedo responder por correo electrónico a las actualizaciones de los casos?

No. Las copias por correo electrónico de la Soporte correspondencia de los casos se envían desde una dirección en la que no hay respuesta. Para actualizar un caso, usa el. AWS Support Center Console

¿Cómo solicito una puesta en marcha GameDay posterior?

Responda a su caso de soporte de incorporación actual, si existe, o cree un. Solicita cambios en una carga de trabajo integrada en la sección Detección y respuesta a incidentes

Solicita cambios en una carga de trabajo integrada en la sección Detección y respuesta a incidentes

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 dirección de correo electrónico con la que desees recibir correspondencia sobre este cambio.

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

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

9. Seleccione Enviar.

   Después de enviar la solicitud de cambio, puedes añadir correos electrónicos adicionales de tu 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 los ID de correo electrónico en la sección Contactos adicionales (opcional).

   El siguiente es un ejemplo de la página de respuesta que muestra dónde puedes 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 Consola de administración de AWS 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. Selecciona Acciones y, a continuación, selecciona Editar para cambiar la alarma.

4. Seleccione Editar métrica para modificar la métrica de la alarma.
5. Elija Añadir matemática y empezar con una expresión vacía.
6. Introduce tu expresión matemática y, a continuación, selecciona Aplicar.
7. Deseleccione la métrica existente que la alarma monitorizó.
8. Seleccione la expresión que acaba de crear y, a continuación, elija Seleccionar métrica.
9. Elija Saltar a la vista previa y crear.
10. 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 Consola de administración de AWS 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 entre la 1:00 y las 3:00 a. m. UTC de todos los martes sustituyendo 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 las alarmas se vuelven a activar 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. En la siguiente captura de pantalla se muestra 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 Consola de administración de AWS 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 Consola de administración de AWS 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 todos los identificadores de cuenta 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 transferir las cargas de trabajo.

Solicitud para eliminar una carga de trabajo

1. Ve al AWS Support Centro y, a continuación, selecciona Crear caso.
2. Elija Técnico.
3. En Servicio, selecciona 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 los ID de correo electrónico con los que deseas recibir correspondencia sobre esta solicitud de exclusión.
9. Seleccione 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. Para obtener más información sobre el uso de la interfaz de línea de comandos del cliente de AWS Incident Detection and Response para ayudar a automatizar estos pasos, consulte CLI para AWS Incident Detection and Response.
- Post-onboarding fase: 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 técnicos de cuentas (TAM).

Gestión de incidentes con detección y respuesta a incidentes

AWS Incident Detection and Response le ofrece supervisión proactiva y gestión 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, consulteSolicite 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 si el incidente está relacionado con un Servicio de AWS problema 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 Servicio de AWS flujo de trabajo de gestión de incidentes 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 Servicio de AWS evento.

   A veces, las alarmas se activan y se recuperan rápidamente. En este escenario, el administrador de incidentes envía una correspondencia sobre el caso en la que se indica que la alarma se ha

recuperado, pero no se pone en contacto con usted. Sin embargo, si una alarma se activa más de una vez en 15 minutos, el administrador de incidentes se pone en contacto con usted según las instrucciones del manual, incluso si la alarma se recupera.

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 para equipos de aplicaciones
- Solicite 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 para 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.

Solicite 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 flujo de trabajo integral para 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 a 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

Para solicitar una respuesta a un incidente, complete los siguientes pasos:

1. Abre el AWS Support Center Consolepara crear un nuevo caso de soporte.
2. En Asunto, introduzca un breve resumen del incidente. Por ejemplo, `AWS Incident Detection and Response - Active Incident - workload_name`.
3. En Descripción, introduzca los detalles del incidente. Le recomendamos que incluya los siguientes detalles en su caso de soporte:
   - ARN del AWS recurso afectado, nombre de la carga de trabajo y su función
   - Descripción del impacto en el negocio
   - (Opcional) La URL del puente de conferencias que prefiera. Si no proporciona los detalles del puente, AWS Incident Detection and Response crea un puente de AWS conferencia y le envía una invitación con la URL del puente.
4. (Opcional) Adjunte archivos que puedan ayudar a describir el incidente, como capturas de pantalla o extractos de un registro.
5. Configure los siguientes campos de clasificación de casos:
   - Tipo de caso: técnico
   - Servicio: detección y respuesta a incidentes
   - Categoría: Incidente activo
   - Gravedad: Business-critical el sistema no funciona
6. Proporcione contexto adicional para ayudar a AWS Incident Detection and Response a interactuar con AWS los expertos con mayor rapidez Servicio de AWS, como los afectados Región de AWS, el impacto empresarial, la hora de inicio del impacto y los recursos afectados.
7. Seleccione Enviar.
8. AWS Incident Detection and Response reconoce su caso en cinco minutos y lo pone en contacto con los AWS expertos correspondientes en una conferencia.

Solicite una respuesta a un incidente utilizando el AWS Support API

Puede usar 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. Introduzca 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 Business-critical Sistema 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

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, consulteSolicite 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
Se aclaró el tema estándar de Amazon SNS para la integración de APM	Se aclaró que los clientes deben crear un tema estándar de Amazon Simple Notification Service (no FIFO) al integrar alarmas de APM de terceros con AWS Incident Detection and Response. Para obtener más información, consulte Administre alarmas de APM con la integración directa de Amazon SNS.	26 de mayo de 2026
GameDay ahora es opcional, se ha simplificado el cuestionario de incorporación y se ha actualizado el desarrollo del manual	Las pruebas de alarma actualizadas (GameDay) pasarán a ser opcionales después Go-Live, con dos opciones de prueba: pruebas de alarma programadas GameDay o fuera de línea. Simplificó la incorporación de la carga de trabajo y los cuestionarios de ingesta de alarmas. Se actualizó el desarrollo del manual para eliminar las referencias a los documentos. AWS Systems Manager Para obtener más información, consulte Pruebe las cargas de trabajo integradas en la detección y respuesta a incidentes, Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response (ruta de excepciones) y Desarrolle manuales y planes de respuesta para responder a un incidente en materia de detección y respuesta a incidentes.	26 de mayo de 2026

Cambio	Descripción	Fecha
Procedimiento actualizado para solicitar una respuesta a un incidente	Se actualizó el procedimiento de solicitud de respuesta a un incidente para que coincidiera con la AWS Support Center Console interfaz de usuario actual, se agregó una guía de URL puente y se eliminaron las capturas de pantalla obsoletas. Para obtener más información, consulte Solicite una respuesta a un incidente mediante el AWS Support Center Console.	12 de mayo de 2026
Se actualizó la incorporación para acercarse CLI-first	Se actualizó el capítulo de introducción para promover la interfaz de línea de comandos para clientes de detección y respuesta a incidentes de AWS como el principal método de incorporación y se eliminaron el cuestiona rio de incorporación de cargas de trabajo y el cuestionario de ingesta de alarmas como la ruta de incorporación predeterminada. Los cuestionarios permanecen disponibles solo como una opción excepcional para los clientes que no pueden usar la CLI de IDR. Para obtener más información, consulte Incorpore las cargas de trabajo a la detección y respuesta a incidentes y Ingestión de alarmas.	12 de mayo de 2026

Cambio	Descripción	Fecha
Se agregaron enlaces a cuestionarios japoneses	Se agregaron enlaces de Japanese-language descarga para el cuestionario de incorpora ción de cargas de trabajo y el cuestionario de ingesta de alarmas. Para obtener más información, consulte Cuestionarios de incorporación de cargas de trabajo e ingesta de alarmas en Incident Detection and Response (ruta de excepciones).	20 de abril de 2026
Referencias de arquitectura actualizadas	Se eliminaron las referencias a los diagramas de arquitectura y se sustituyeron por detalles de la arquitectura. Para obtener más información, consulte Arquitectura de detección y respuesta a incidentes y Acerca de las cargas de trabajo en materia de detección y respuesta a incidentes.	31 de marzo de 2026
Se actualizó la versión de las cargas de trabajo integradas en la detección y respuesta a incidentes	Se agregó información sobre cómo deshabili tar las acciones de CloudWatch alarma antes de cambiar el estado de la alarma durante las pruebas. Para obtener más información, consulte Pruebe las cargas de trabajo integradas en la detección y respuesta a incidentes.	2 de marzo de 2026
Gestión de incidentes actualizada con detección y respuesta a incidentes	Se agregó información sobre la repetición del comportamiento de las alarmas y la participa ción del administrador de incidentes. Para obtener más información, consulte Gestión de incidentes con detección y respuesta a incidentes.	2 de marzo de 2026

Cambio	Descripción	Fecha
Se actualizaron los pasos de la sección Uso de una función matemática métrica para suprimir una CloudWatch alarma	Se han actualizado los pasos de la sección Utilizar una función matemática métrica para suprimir una CloudWatch alarma. Para obtener más información, consulte Suprima las alarmas en la fuente de alarma.	3 de febrero de 2026
Se agregó el coreano como idioma compatible	Se agregó el coreano como idioma compatible. Para obtener más información, consulte Disponibilidad regional para la detección y respuesta a incidentes.	22 de enero de 2026
Se agregó el mandarín como idioma compatible	Se agregó el mandarín como idioma compatibl e. Para obtener más información, consulte Disponibilidad regional para la detección y respuesta a incidentes.	13 de enero de 2026
Se agregó una nueva sección: Interfaz de línea de comandos del cliente para detección y respuesta a incidentes de AWS	Se agregó la sección CLI de IDR y se actualizó el capítulo de introducción para incluir informaci ón sobre la interfaz de línea de comandos del cliente de AWS Incident Detection and Response. Para obtener más información, consulte CLI para AWS Incident Detection and Response.	8 de diciembre de 2025

Cambio	Descripción	Fecha
Se actualizaron varias secciones: cuestionarios sobre la incorporación de la carga de trabajo y la ingesta de alarmas en Detección y respuesta a incidentes y Introducción a la detección y respuesta a incidentes	El proceso de gestión de Servicio de AWS eventos ya no forma parte de AWS Incident Detection and Response. Las secciones de esta guía del usuario se actualizaron para eliminar las referencias a este proceso. Seguirá recibiendo notificaciones de eventos de servicio a través del AWS Service Health Dashboard . Los clientes de AWS Incident Detection and Response pueden utilizar una solicitud de respuesta a incidentes para recibir ayuda durante los eventos de servicio según sea necesario. Para obtener más información, consulte Solicite una respuesta a un incidente.	14 de octubre de 2025
Sección eliminada: Gestión de incidentes para eventos de servicio	El proceso de gestión de Servicio de AWS eventos ya no forma parte de AWS Incident Detection and Response. Esta sección de la guía del usuario se eliminó para reflejar este cambio. Seguirá recibiendo notificac iones de eventos de servicio a través del AWS Service Health Dashboard. Los clientes de AWS Incident Detection and Response pueden utilizar una solicitud de respuesta a incidentes para recibir ayuda durante los eventos de servicio según sea necesario. Para obtener más información, consulte Solicite una respuesta a un incidente.	14 de octubre de 2025
Sección actualizada: Disponibi lidad regional para la detección y respuesta a incidentes	La detección y respuesta a incidentes de AWS ya están disponibles en AWS GovCloud (US-East) y AWS GovCloud (US-West). Para obtener más información, consulte Disponibi lidad regional para la detección y respuesta a incidentes	5 de octubre de 2025

Cambio	Descripción	Fecha
Sección actualizada: Cuestionarios sobre la incorporación de la carga de trabajo y la ingesta de alarmas en materia de detección y respuesta a incidentes	Se ha actualizado un ejemplo de dirección de correo electrónico para la tabla de matrices de alarmas.	26 de agosto de 2025
Sección actualizada: Suscriba una carga de trabajo a AWS Incident Detection and Response	Se ha eliminado la referencia al campo de fecha de inicio de la suscripción en la sección Descripción de la ventana Crear caso. Sección actualizada: Suscriba una carga de trabajo a AWS Incident Detection and Response	4 de agosto 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: Solicite 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

Cambio	Descripción	Fecha
Actualizaciones para gestionar los casos de soporte de detección y respuesta a incidentes con la AWS Support App in Slack página	Se trasladó la página a Gestión de incidentes, se revisó el texto y se sustituyeron las capturas de pantalla. Sección actualizada: Gestione los casos de soporte de detección y respuesta a incidentes con el AWS Support App in Slack	10 de octubre de 2024
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 AWS Incident Detection and Response	12 de junio 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 están excluyendo Para obtener más información, consulte Suscribir una carga de trabajo a AWS Incident Detection and Response	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 la 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.	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: • Incorpore las cargas de trabajo a la detección y respuesta a incidentes • Suscriba una carga de trabajo a AWS Incident Detection and Response Nuevas secciones • Proporcione acceso a AWS Support Center Console para 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 alarmas a la detección y respuesta a incidentes	17 de enero de 2024
Pasos de ejemplo actualizados	Se actualizó el procedimiento de los pasos 2, 3 y 4 del ejemplo: integración de notificaciones de Datadog y Splunk. Sección actualizada: Ejemplo: integración de notificaciones de Datadog y Splunk	21 de diciembre de 2023

Cambio	Descripción	Fecha
Gráfico y texto de introducción actualizados	Gráfico actualizado en las alarmas de ingesta de los APM que tienen integración directa con Amazon. EventBridge Sección actualizada: Desarrolle manuales y planes de respuesta para responder a un incidente en materia de 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 materia de 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 la detección y respuesta a incidentes con CloudFormation plantillas Nueva sección: Ejemplos de casos de uso de CloudWatch alarmas en la detección y respuesta a incidentes	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: Solicita cambios en una carga de trabajo integrada en la sección Detección y respuesta a incidentes Sección actualizada: Suscriba una carga de trabajo a AWS Incident Detection and Response	5 de septiembre de 2023
Nueva sección en Cómo empezar	Se agregaron alertas 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.