Conceitos e procedimentos de detecção e resposta a incidentes da AWS

Guia do usuário do AWS Incident Detection and Response

Versão May 26, 2026

Guia do usuário do AWS Incident Detection and Response: Conceitos e procedimentos de detecção e resposta a incidentes da AWS

Table of Contents

O que é o AWS Incident Detection and Response?

O AWS Incident Detection and Response oferece aos clientes qualificados do AWS Enterprise Support um engajamento proativo de incidentes para reduzir o potencial de falhas e acelerar a recuperação de cargas de trabalho críticas em caso de interrupções. A Detecção e Resposta a Incidentes facilitam sua colaboração AWS para desenvolver runbooks e planos de resposta personalizados para cada carga de trabalho integrada.

A Detecção e Resposta a Incidentes oferece os seguintes recursos principais:

- Observabilidade aprimorada: AWS especialistas fornecem orientação para ajudá-lo a definir e correlacionar métricas e alarmes entre as camadas de aplicativos e infraestrutura de sua carga de trabalho para detectar interrupções precocemente.
- Tempo de resposta de 5 minutos: os engenheiros de gerenciamento de incidentes envolvem você de forma proativa em até 5 minutos após um alarme, a partir de suas cargas de trabalho ou em resposta a um caso crítico enviado por você.
- Resolução mais rápida: os IMEs usam runbooks predefinidos e personalizados desenvolvidos para suas cargas de trabalho, criam um caso de Support em seu nome e gerenciam incidentes em sua carga de trabalho. Os IMEs fornecem propriedade única para incidentes e mantêm você envolvido com os AWS especialistas certos até que o incidente seja resolvido.
- Potencial reduzido de falha: após a resolução, os IMEs fornecem uma análise pós-incidente (mediante solicitação). Além disso, AWS especialistas trabalham com você para aplicar as lições aprendidas para melhorar o plano de resposta a incidentes e os runbooks. Você também pode aproveitar AWS Resilience Hub o rastreamento contínuo da resiliência em suas cargas de trabalho.

Tópicos

Inscreva-se para um Conta da AWS

Para começar AWS, você precisa de um Conta da AWS. Para obter informações sobre como criar um Conta da AWS, consulte Introdução a um Conta da AWS no Guia de AWS Gerenciamento de contas referência.

Termos de uso para detecção e resposta a incidentes

A lista a seguir descreve os principais requisitos e limitações para o uso do AWS Incident Detection and Response. É importante que você entenda essas informações antes de usar o serviço, pois elas abrangem aspectos como requisitos do plano de suporte, processo de integração e duração mínima da assinatura.

- O AWS Incident Detection and Response está disponível para contas diretas e de suporte Partner-resold corporativo.
- O AWS Incident Detection and Response não está disponível para contas no Partner Led Support.
- Você deve manter o AWS Enterprise Support em todos os momentos durante a vigência do seu serviço de Detecção e Resposta a Incidentes. Para obter informações, consulte Enterprise Support. O encerramento do Enterprise Support resulta na remoção simultânea do serviço AWS Incident Detection and Response.
- Todas as cargas de trabalho no AWS Incident Detection and Response devem passar pelo processo de integração da carga de trabalho.
- A duração mínima para assinar uma conta no AWS Incident Detection and Response é de noventa (90) dias. Todas as solicitações de cancelamento devem ser enviadas trinta (30) dias antes da data efetiva pretendida para o cancelamento.
- AWS trata suas informações conforme descrito no Aviso AWS de Privacidade.

> **Note**
>
> Para perguntas relacionadas ao faturamento de detecção e resposta de incidentes, consulte Como obter ajuda com o AWS faturamento.

Arquitetura de detecção e resposta a incidentes

O AWS Incident Detection and Response se integra ao seu ambiente atual, conforme mostrado no gráfico a seguir. A arquitetura inclui os seguintes serviços:

- Amazon EventBridge: A Amazon EventBridge serve como o único ponto de integração entre suas cargas de trabalho e o AWS Incident Detection and Response. Os alarmes são ingeridos de suas ferramentas de monitoramento, como a Amazon, por meio da Amazon CloudWatch, EventBridge usando regras predefinidas gerenciadas por. AWS Para permitir que a Detecção e Resposta a Incidentes criem e gerenciem a EventBridge regra, você instala uma função vinculada ao serviço. Para saber mais sobre esses serviços, consulte O que é a Amazon EventBridge e EventBridge as regras da Amazon, O que é a Amazon CloudWatch e Como usar funções vinculadas a serviços. AWS Health
- AWS Health: AWS Health fornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de suas Serviços da AWS contas. A Detecção e Resposta AWS Health a Incidentes é Serviços da AWS usada para rastrear eventos usados por suas cargas de trabalho e para notificá-lo quando um alerta é recebido de sua carga de trabalho. Para saber mais AWS Health, consulte O que é AWS Health.
- AWS Systems Manager: O Systems Manager fornece uma interface de usuário unificada para automação e gerenciamento de tarefas em seus AWS recursos. O AWS Incident Detection and Response hospeda informações sobre suas cargas de trabalho, incluindo detalhes da arquitetura da carga de trabalho, detalhes do alarme e seus respectivos runbooks de gerenciamento de incidentes em AWS Systems Manager documentos (para obter detalhes, consulte AWS Systems Manager Documentos). Para saber mais AWS Systems Manager, consulte O que é AWS Systems Manager.
- Seus runbooks específicos: um caderno de gerenciamento de incidentes define as ações que o AWS Incident Detection and Response executa durante o gerenciamento de incidentes. Seus runbooks específicos informam ao AWS Incident Detection and Response quem contatar, como entrar em contato com eles e quais informações compartilhar.

Funções e responsabilidades na detecção e resposta a incidentes

A tabela RACI (Responsável, Responsável, Consultado e Informado) da AWS descreve as funções e responsabilidades de várias atividades relacionadas à detecção e resposta a incidentes. Essa

tabela ajuda a definir o envolvimento do cliente e da equipe de detecção e resposta a incidentes da AWS em tarefas como coleta de dados, análise da prontidão operacional, configuração da conta, gerenciamento de incidentes e revisão pós-incidente.

Atividades	Cliente	Detecção e resposta a incidentes
Coleta de dados		
Introdução ao cliente e à carga de trabalho	Consultado	Responsável
Arquitetura	Responsável	Responsável
Operações	Responsável	Responsável
Determine CloudWatch os alarmes a serem configurados	Responsável	Responsável
Defina o plano de resposta a incidentes	Responsável	Responsável
Análise da prontidão operacional		
Conduza uma análise bem arquitetada (WAR) da carga de trabalho	Consultado	Responsável
Valide a resposta a incidentes	Consultado	Responsável
Validar matriz de alarmes	Consultado	Responsável

Atividades	Cliente	Detecção e resposta a incidentes
Identifique AWS os principais serviços que estão sendo usados pela carga de trabalho	Responsável	Responsável
Configuração da conta		
Crie a função do IAM na conta do cliente	Responsável	Informado
Instalar a EventBridge regra gerenciada usando a função criada	Informado	Responsável
Teste os alarmes integrados (ou APM) CloudWatch	Responsável	Informado
Verifique se os alarmes do cliente envolvem a detecção e a resposta a incidentes	Informado	Responsável
Atualizar alarmes	Responsável	Consultado
Atualizar runbooks	Consultado	Responsável
Gerenciamento de incidentes		
Notifique proativamente os incidentes detectados pela Detecção e Resposta a Incidentes	Informado	Responsável
Forneça resposta a incidentes	Informado	Responsável

Atividades	Cliente	Detecção e resposta a incidentes
Forneça resolução de incidentes e restauração da infraestrutura	Responsável	Consultado
Post-incident resenha		
Solicitar análise pós-incidente	Responsável	Informado
Forneça uma análise pós-incidente	Informado	Responsável

Disponibilidade regional para detecção e resposta a incidentes

O AWS Incident Detection and Response está disponível em inglês, japonês, mandarim e coreano para contas do AWS Enterprise Support hospedadas em qualquer um dos seguintes: Regiões da AWS

Região da AWS	Nome
Região Leste dos EUA (Norte da Virgínia)	us-east-1
Região Leste dos EUA (Ohio)	us-east-2
Região Oeste dos EUA (N. da Califórnia)	us-west-1
Região Oeste dos EUA (Oregon)	us-west-2
Região Canadá (Central)	ca-central-1
Região Oeste do Canadá (Calgary)	ca-west-1

Região da AWS	Nome
Região América do Sul (São Paulo)	sa-east-1
Região Europa (Frankfurt)	eu-central-1
Região Europa (Irlanda)	eu-west-1
Região Europa (Londres)	eu-west-2
Região Europa (Paris)	eu-west-3
Região Europa (Estocolmo)	eu-north-1
Região Europa (Zurique)	eu-central-2
Região Europa (Milão)	eu-south-1
Região Europa (Espanha)	eu-south-2
Ásia-Pacífico (Mumbai)	ap-south-1
Ásia-Pacífico (Tóquio)	ap-northeast-1
Ásia-Pacífico (Seul)	ap-northeast-2
Ásia-Pacífico (Singapura)	ap-southeast-1
Ásia-Pacífico (Sydney)	ap-southeast-2
Ásia-Pacífico (Hong Kong)	ap-east-1
Ásia-Pacífico (Osaka)	ap-northeast-3
Ásia-Pacífico (Hyderabad)	ap-south-2
Ásia-Pacífico (Jacarta)	ap-southeast-3
Ásia-Pacífico (Melbourne)	ap-southeast-4
Ásia-Pacífico (Malásia)	ap-southeast-5

Região da AWS	Nome
África (Cidade do Cabo)	af-south-1
Israel (Tel Aviv)	il-central-1
Oriente Médio (Emirados Árabes Unidos)	me-central-1
Oriente Médio (Bahrein)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Comece a usar a Detecção e Resposta a Incidentes

Cargas de trabalho e alarmes são fundamentais para a detecção e resposta a incidentes da AWS. AWS trabalha junto com você para definir e monitorar cargas de trabalho específicas que são essenciais para seus negócios. AWS ajuda você a configurar alarmes que notificam sua equipe sobre problemas significativos de desempenho ou impacto no cliente. Alarmes configurados corretamente são essenciais para o monitoramento proativo e a resposta rápida a incidentes na Detecção e Resposta a Incidentes.

Sobre cargas de trabalho em Detecção e Resposta a Incidentes

Você pode selecionar cargas de trabalho específicas para monitoramento e gerenciamento de incidentes críticos usando o AWS Incident Detection and Response. Uma carga de trabalho é uma coleção de recursos e códigos que trabalham juntos para agregar valor comercial. Uma carga de trabalho pode ser todos os recursos e códigos que compõem seu portal de pagamento bancário ou um sistema de gerenciamento de relacionamento com o cliente (CRM). Você pode hospedar uma carga de trabalho em uma única Conta da AWS ou em várias Contas da AWS.

Por exemplo, você pode ter um aplicativo monolítico hospedado em uma única conta (por exemplo, o Employee Performance App no diagrama a seguir). Ou você pode ter um aplicativo (por exemplo, o Storefront Webapp no diagrama) dividido em microsserviços que se estendem por contas diferentes. Uma carga de trabalho pode compartilhar recursos, como um banco de dados, com outros aplicativos ou cargas de trabalho, conforme mostrado no diagrama a seguir.

Para começar com a integração da carga de trabalho, consulte. Integre cargas de trabalho para detecção e resposta a incidentes

Sobre alarmes em Detecção e Resposta a Incidentes

Os alarmes são uma parte fundamental da detecção e resposta a incidentes. Os alarmes fornecem visibilidade do desempenho de seus aplicativos e da AWS infraestrutura subjacente. AWS trabalha com você para definir métricas e limites de alarme apropriados que só são acionados quando há um impacto crítico nas cargas de trabalho monitoradas. O objetivo é que os alarmes envolvam seus solucionadores específicos, que então colaboram com a equipe de gerenciamento de incidentes para mitigar rapidamente os problemas. Configure seus alarmes para entrarem no estado de alarme somente quando houver uma degradação significativa no desempenho ou na experiência do cliente

que exija atenção imediata. Alguns tipos principais de alarmes incluem aqueles que indicam impacto nos negócios, Amazon CloudWatch Canaries e alarmes agregados que monitoram dependências.

Para começar com a ingestão de alarmes, consulteIngestão de alarmes.

Integre cargas de trabalho para detecção e resposta a incidentes

O AWS Incident Detection and Response permite o monitoramento e o gerenciamento de incidentes críticos para suas cargas de trabalho selecionadas. Uma carga de trabalho é um conjunto de recursos trabalhando juntos para gerar valor comercial, como um portal de pagamento ou um sistema de gerenciamento de relacionamento com o cliente (CRM). Você pode hospedar essas cargas de trabalho em uma única conta Conta da AWS ou distribuídas em várias contas, dependendo da sua arquitetura.

Sumário

Integrado à detecção e resposta a incidentes com a CLI do IDR

A AWS Incident Detection and Response Customer Command Line Interface (IDR CLI) é uma ferramenta de interface de linha de comando que simplifica a integração com o AWS Incident Detection and Response.

A CLI do IDR é executada AWS CloudShell para executar as seguintes funções:

- Colete informações de integração
- Colete dados AWS de recursos por meio da API Resource Groups Tagging
- Gerenciar AWS Support casos
- Crie novos CloudWatch alarmes da Amazon ou consuma os existentes
- Implante e teste a infraestrutura AWS CloudFormation para permitir que ferramentas de terceiros enviem alertas para a Detecção e Resposta a Incidentes.

A CLI do IDR pode ser executada em um modo interativo para guiá-lo pelas etapas de integração ou no modo off-line para casos de uso em massa ou em massa DevOps .

Para obter mais informações sobre como usar a CLI do IDR, incluindo instalação, pré-requisitos e exemplos completos, consulte CLI for AWS Incident Detection and Response.

Suporte de idioma para a CLI do IDR

O AWS Incident Detection and Response está disponível em inglês, japonês, mandarim e coreano. Se precisar de suporte em japonês, mandarim ou coreano, entre em contato AWS por meio do AWS Support caso criado pela CLI do IDR ou entre em contato com seu gerente técnico de contas (TAM).

Opções alternativas para integrar cargas de trabalho

Se você não puder usar a CLI do IDR para integração, consulte seu gerente técnico de contas (TAM) para obter opções alternativas. Para obter mais informações, consulte Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes (caminho de exceção).

Ingestão de alarmes

A interface de linha de comando do cliente (IDR CLI) do AWS Incident Detection and Response pode criar novos alarmes CloudWatch da Amazon ou ingerir os existentes e pode implantar e testar a infraestrutura AWS CloudFormation para permitir que ferramentas de terceiros enviem alertas para o AWS Incident Detection and Response.

O AWS Incident Detection and Response pode ingerir alarmes da Amazon CloudWatch e de ferramentas de monitoramento de desempenho de aplicativos (APM) de terceiros via Amazon: EventBridge

- Alarmes de ingestão CloudWatch
- Ingestão de alarmes de monitoramento de desempenho de aplicativos de terceiros

Etapas para a ingestão de alarmes

As etapas a seguir precisam ser concluídas para a ingestão do alarme:

- Definição de alarme
- Ingestão de alarmes usando a CLI do IDR
- Análise e feedback de alarmes

- Provisionar acesso para ingestão de alarmes à detecção e resposta a incidentes
- Os alarmes entram em operação

Opções alternativas para ingerir alarmes

Se você não puder usar a CLI do IDR para ingestão de alarmes, consulte seu gerente técnico de contas (TAM) para obter opções alternativas. Para obter mais informações, consulte Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes (caminho de exceção).

Provisionar acesso para ingestão de alarmes à detecção e resposta a incidentes

> **Note**
>
> Se você não criou a função vinculada ao serviço (SLR) durante a integração da CLI do IDR, siga as etapas abaixo para provisionar o acesso manualmente.

Para permitir que o AWS Incident Detection and Response consuma alarmes da sua conta, crie a `AWSServiceRoleForHealth_EventProcessor` SLR. AWS assume a SLR para criar uma EventBridge regra gerenciada em sua conta. A EventBridge regra gerenciada envia notificações da sua conta para o AWS Incident Detection and Response. Para obter informações sobre essa SLR, incluindo a política AWS gerenciada associada, consulte Usando funções vinculadas ao serviço no Guia do usuário.

Você pode criar essa função vinculada ao serviço em sua conta seguindo as instruções em Criar função vinculada ao serviço no Guia do usuário.AWS Identity and Access Management Ou você pode usar o seguinte comando AWS Command Line Interface (AWS CLI):

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

Principais saídas

- Criação bem-sucedida da função vinculada ao serviço em sua conta.

> **Note**
>
> A função vinculada ao serviço - AWSServiceRoleForHealth _ EventProcessor precisa ser criada em cada conta que você usará para enviar alarmes para o AWS Incident Detection and Response.

Informações relacionadas

Para saber mais, consulte os seguintes tópicos:

- Usar funções vinculadas ao serviço do
- Criação de uma função vinculada ao serviço
- AWS política gerenciada: AWS Health_EventProcessorServiceRolePolicy

Definição de alarme

Ao integrar seus alarmes ao AWS Incident Detection and Response, você é responsável por definir as métricas e as configurações de alarmes que fornecem visibilidade sobre o desempenho de seus aplicativos. Como parte desse processo, você também deve identificar as equipes da sua organização que são responsáveis por responder a esses alarmes.

Ao preparar alarmes, recomendamos as seguintes práticas recomendadas:

- Os alarmes só entram no estado “Alarme” quando há um impacto crítico contínuo em sua carga de trabalho monitorada que requer atenção imediata de sua equipe e. AWS Alarmes que são acionados e não se recuperam automaticamente exigem que suas equipes se unam a uma ponte de incidentes com o AWS Incident Detection and Response.
- Garanta que as informações de contato que você fornece permitam que o AWS Incident Detection and Response envolva de forma confiável as equipes apropriadas da sua organização em uma ponte 24/7 de incidentes.

Principais saídas

- Uma lista de alarmes e detalhes de contato, que você fornece ao AWS Incident Detection and Response usando a CLI do IDR.

Para obter mais informações sobre como definir e ingerir CloudWatch alarmes da Amazon, consulte. Alarmes de ingestão CloudWatch

Para obter mais informações sobre a ingestão de alarmes de monitoramento de desempenho de aplicativos de terceiros, consulte. Ingestão de alarmes de monitoramento de desempenho de aplicativos de terceiros

Alarmes de ingestão CloudWatch

O AWS Incident Detection and Response pode ingerir CloudWatch alarmes da Amazon para fornecer monitoramento proativo para suas cargas de trabalho críticas. Ao ingerir seus CloudWatch alarmes da Amazon para monitoramento, o AWS Incident Detection and Response pode:

- Detecte automaticamente quando seus alarmes entram no estado “Alarme”.
- Envolva suas equipes para responder e resolver incidentes de forma colaborativa.

Para garantir que os alarmes que você incorpora sejam eficazes, o AWS Incident Detection and Response recomenda as seguintes melhores práticas:

- Configure alarmes com expressões matemáticas métricas para suprimi-los durante períodos de manutenção regular ou execuções de trabalhos em lote para evitar alertas falsos positivos.
- Defina o tratamento de dados ausentes nos alarmes com base na frequência esperada de entrega do ponto de dados. Por exemplo, métricas de monitoramento de alarmes que geram um fluxo contínuo de pontos de dados devem tratar os dados perdidos como “violação” (ruim), pois pontos de dados ausentes podem indicar um problema com o recurso subjacente monitorado. Inversamente, métricas de monitoramento de alarmes que raramente relatam pontos de dados, por exemplo, métricas de monitoramento de alarmes que registram pontos de dados somente quando ocorre uma falha ou erro, devem tratar os dados ausentes como (bons). NotBreaching
- Defina alarmes que entram no estado “Alarme” quando há um impacto crítico e contínuo em sua carga de trabalho. Por exemplo, configure os alarmes para serem acionados após o tempo esperado necessário para substituir automaticamente os recursos não íntegros, em vez da detecção inicial de recursos não íntegros.
- Identifique e crie alarmes para métricas personalizadas que representem diretamente a experiência do cliente em sua carga de trabalho.

Para obter uma lista de CloudWatch alarmes comuns recomendados pela Amazon Serviços da AWS, consulte as melhores práticas de detecção e resposta a alarmes de incidentes no AWS re:POST.

Ingestão de alarmes de monitoramento de desempenho de aplicativos de terceiros

O AWS Incident Detection and Response suporta a ingestão de alarmes de ferramentas terceirizadas de monitoramento de desempenho de aplicativos (APM) por meio da Amazon. EventBridge Essa integração fornece flexibilidade ao ingerir alertas de APM, permitindo o roteamento de eventos de APM por meio de vários para Serviços da AWS um barramento de eventos da Amazon em sua EventBridge conta.

Exemplos de caminhos de integração:

- Fonte (APM) → AWS Serviço (exemplo: Amazon API Gateway ou Amazon SNS) → Função Transform Lambda → Amazon EventBridge Event Bus personalizado → AWS Incident Detection and Response
- Fonte (APM) → Parceiro Amazon EventBridge Event Bus → Transforme a função Lambda → EventBridge Amazon Event Bus personalizado → AWS Incident Detection and Response

O AWS Incident Detection and Response instala uma regra gerenciada no barramento de eventos personalizado para ingerir alertas enviados por Transform Lambda Functions. É importante observar que, para as EventBridge integrações SaaS da Amazon, o barramento de eventos do parceiro não é o barramento de eventos que tem uma regra gerenciada instalada. Para obter uma lista completa de APMs com integrações de parceiros na Amazon EventBridge, consulte Integrações com a Amazon EventBridge .

Exemplo de integração usando um barramento de eventos parceiro ou outras fontes de barramento de AWS eventos

O diagrama a seguir mostra um exemplo de integração usando um barramento de eventos parceiro ou outras fontes de barramento de AWS eventos.

Para obter uma lista completa de APMs com integrações de parceiros na Amazon EventBridge, consulte Integrações com a Amazon EventBridge .

Exemplo de integração usando o Amazon API Gateway

O diagrama a seguir mostra um exemplo de integração usando um API Gateway.

Exemplo de integração usando o Amazon Simple Notification Service

O diagrama a seguir mostra um exemplo de integração usando um Amazon SNS.

Para simplificar o processo de integração, o AWS Incident Detection and Response fornece CloudFormation modelos para os tipos de integração mais usados. Esses modelos automatizam a configuração dos AWS recursos e das funções necessárias do IAM.

CloudFormation Modelos e instruções para criar manualmente vários tipos de integração podem ser encontrados na documentação de integração correspondente abaixo:

- Ingira alarmes de APMs com integração direta EventBridge
- Ingira alarmes de APMs sem integração direta com EventBridge
- Alarmes de ingestão de APMs com integração direta com o Amazon SNS

> **Note**
>
> Os CloudFormation modelos exigem modificações. Essas modificações são explicadas nos tópicos anteriores. Para obter mais informações sobre o formato de carga útil necessário para enviar alertas de APM para o AWS Incident Detection and Response, consulte. Requisitos de carga útil para ingerir alertas de APM com EventBridge

Requisitos de carga útil para ingerir alertas de APM com EventBridge

De onde a Detecção e Resposta a Incidentes ingerem alertas de APM?

O AWS Incident Detection and Response instala uma regra gerenciada no barramento de eventos para o qual você envia sua carga final transformada. É uma prática recomendada criar um ônibus de eventos personalizado para essa finalidade.

Em qual formato as cargas devem estar?

Os seguintes pares mínimos de chave/valor JSON são necessários em eventos de barramento de eventos ingeridos pelo AWS Incident Detection and Response:

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

```
    }
}
```

Os exemplos a seguir mostram um evento de um ônibus de eventos parceiro antes e depois de ser transformado.

Antes da transformação:

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

Observe isso antes de o evento ser transformado `detail-type` e `source` indica os detalhes do APM de onde o alerta se originou. Eles devem ser modificados antes da ingestão. A `incident-detection-response-identifier` chave ainda não está presente e também deve ser adicionada antes da ingestão.

Uma função Lambda transforma o evento acima e o coloca no barramento de eventos padrão ou personalizado de destino. A carga transformada deve incluir os pares chave-valor necessários.

Após a transformação:

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

Observe que agora `detail-type` é`ams.monitoring/generic-apm`, a fonte é agora e`GenericAPMEvent`, em detalhes, há um novo par chave-valor:. `incident-detection-response-identifier`

O `incident-detection-response-identifier` valor é obtido do nome do alerta com base na carga que seu APM envia. Os caminhos do nome do alerta do APM são diferentes de um APM para outro. Uma função Lambda deve ser configurada para pegar o nome do alarme do caminho correto na carga JSON do APM recebida pelo Lambda e usá-lo para o valor. `incident-detection-response-identifier`

`incident-detection-response-identifier`os valores devem ser exclusivos por tipo de alarme enviado para o AWS Incident Detection and Response. Cada nome exclusivo definido no `incident-detection-response-identifier` deve ser fornecido à equipe de detecção e resposta a incidentes da AWS durante a integração. Eventos que têm um valor desconhecido ou ausente para a `incident-detection-response-identifier` chave não são processados.

Ingira alarmes de APMs com integração direta EventBridge

O tópico a seguir mostra o processo de envio de alarmes para o AWS Incident Detection and Response a partir de ferramentas de monitoramento de desempenho de aplicativos (APM) que têm integração direta com a Amazon. EventBridge Para obter uma lista completa de APMs que têm integração direta com a Amazon EventBridge, consulte EventBridgeIntegrações com a Amazon.

Você pode implantar o CloudFormation modelo fornecido ou configurar manualmente essa integração. Antes de configurar a integração, verifique se a função AWS vinculada ao serviço (SLR) `AWSServiceRoleForHealth_EventProcessor` foi criada em suas contas.

Opção 1: Usando CloudFormation

Um CloudFormation modelo está disponível para simplificar o processo de criação da infraestrutura de integração necessária para ingerir alarmes para o AWS Incident Detection and Response do seu APM com a integração da Amazon. EventBridge

> **Note**
>
> - Custos adicionais são incorridos com recursos implantados por meio desse CloudFormation modelo (por exemplo: Lambda e). EventBridge Para obter mais informações sobre os preços desses serviços, consulte AWS Preços.
> - Implante esse CloudFormation modelo em todas as AWS contas e regiões em que o AWS Incident Detection and Response precise ingerir alarmes. Incidentes e Support Cases são abertos na AWS conta de onde o alerta do APM foi recebido.
> - Este documento usa o New Relic como exemplo, no entanto, o CloudFormation modelo pode ser usado para qualquer APM que tenha integração SaaS com a Amazon. EventBridge
> - Depois de testar a integração, remova as instruções logger.info () do `TransformLambdaFunction` para evitar que a carga apareça no Amazon Logs. CloudWatch

Pré-requisitos para implantar esse modelo: CloudFormation

- Uma fonte de eventos de parceiros deve ser configurada na Amazon EventBridge. Para obter instruções sobre como configurar seu APM como fonte de eventos, consulte Recebimento de eventos de um parceiro de SaaS com a EventBridge Amazon no Guia do usuário da EventBridge Amazon.
- A `TransformLambdaFunction` (função Lambda) no modelo deve ser modificada `["detail"]["incident-detection-response-identifier"]` para definir o valor desejado com base no caminho JSON do nome do alerta na carga do APM.

Etapas de pré-requisito:

1. Abra o EventBridge console. No menu Integração, selecione Fontes de eventos do parceiro.
   - Pesquise seu APM na caixa de EventBridge parceiros da Amazon.
   - Escolha Configuração e siga as instruções fornecidas.
     - Observação: a última etapa é escolher Associar ao Event Bus no console para a origem do evento Partner. Selecionar essa opção cria automaticamente um Partner Event Bus com o mesmo nome da origem do evento Partner (os nomes devem coincidir).

- Copie o nome do Partner Event Bus ou da fonte. O barramento de eventos ou a fonte é usado como um parâmetro, chamado`PartnerEventBusNameParameter`, ao implantar o CloudFormation modelo.
  - Exemplo de New Relic: `aws.partner/newrelic.com/1234567/source_name`
- Copie a primeira parte do Partner Event Bus ou da fonte a ser inserida no `PartnerEventBusPrefixParameter` ao implantar o CloudFormation modelo.
  - Um exemplo para New Relic é `aws.partner/newrelic.com`

2. Baixe e edite o CloudFormation modelo.
   - Localize o `TransformLambdaFunction` no modelo
   - Em `def lambda_handler(event, context)` definido como `event["detail"]["incident-detection-response-identifier"]` o caminho json em que o nome do alarme aparece na carga JSON do alarme APM. Cada APM terá um caminho diferente. Alguns exemplos podem ser vistos abaixo, mas suas cargas específicas podem ser diferentes.
     - Exemplo de New Relic:`event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`.
     - Exemplo de Datadog: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
     - Exemplo do Splunk: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
   - Salve o CloudFormation modelo.

Implantando o CloudFormation modelo:

1. Abra o CloudFormation console na sua conta e região de destino.
2. Escolha Criar pilha, com novos recursos (padrão)
   - Selecione Escolher um modelo existente, Carregar um arquivo de modelo, Escolher arquivo e, em seguida, carregue o CloudFormation modelo que você salvou localmente.
3. Especifique os detalhes da pilha:
   - Insira o nome da pilha (Exemplo:`NewRelicIntegrationForIDR`).
   - Especifique os valores dos parâmetros obtidos durante o preenchimento do pré-requisito.
     - APMNameParameter(Exemplo:`NewRelic`)

    - PartnerEventBusNameParameter(Exemplo:`aws.partner/newrelic.com/1234567/source_name`)
    - PartnerEventBusPrefixParameter(Exemplo:`aws.partner/newrelic.com`)
  - Escolha Próximo.
4. Configure as opções de pilha:
  - Role até o final da página e marque a caixa para permitir CloudFormation a criação de recursos do IAM com nomes personalizados.
5. Revisar e criar:
  - Verifique se os valores dos parâmetros estão configurados corretamente e escolha Enviar.
6. A CloudFormation pilha implanta os recursos necessários para integrar seus eventos de APM ao AWS Incident Detection and Response. Aguarde até que o status da pilha seja exibido`CREATE_COMPLETE`.
7. A CloudFormation pilha cria os seguintes recursos, supondo que os valores de exemplo tenham sido inseridos nos parâmetros do New Relic e tenham sido executados na região. US-EAST-1
  - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
  - EventBridgeRule: leis. partner/newrelic. com/1234567/nome_do_fonte | NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
  - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
  - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
  - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission - [seqüência_aleatória]

Teste de integração

Depois de implantar a pilha, teste a integração enviando uma carga de teste do seu APM:

1. Navegue até o console Lambda e selecione a `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` função. Escolha a guia Monitor (Monitorar).
2. Procure uma invocação bem-sucedida nos gráficos métricos.
3. Escolha Exibir Amazon CloudWatch Logs para verificar a carga útil do teste ou verificar se há erros nos fluxos de log.

Compartilhando seu ARN do Event Bus com o AWS Incident Detection and Response

1. Abra o Amazon EventBridge Console. Selecione Ônibus de eventos.
2. Copie o ARN do barramento de eventos personalizados criado como parte da CloudFormation pilha (exemplo:.) `arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`
   - Adicione esse ARN ao campo “ARN do EventBridge Event Bus” na seção “Alarmes do Third-Party APM” do seu. Questionário de ingestão de alarmes - Visão geral
3. Durante o processo de integração, o AWS Incident Detection and Response cria uma EventBridge regra gerenciada nesse barramento de eventos personalizado para ingerir seus alarmes de APM.

Opção 2: integração manual

Conclua as etapas a seguir para cada AWS conta e AWS região da qual o AWS Incident Detection and Response precisa ingerir alarmes. O AWS Incident Detection and Response recomenda configurar alarmes na mesma AWS conta e região dos recursos do seu aplicativo para agilizar a identificação e a investigação dos recursos afetados. Incidentes e Support Cases são abertos na AWS conta de onde o alerta do APM foi recebido.

1. Crie um ônibus de eventos EventBridge parceiro configurando seu APM como uma fonte de eventos EventBridge parceiros da Amazon (por exemplo,`aws.partner/apm_name/integrationName`). Para obter diretrizes sobre como configurar seu APM como fonte de eventos, consulte Recebimento de eventos de um parceiro de SaaS com a Amazon. EventBridge
2. Execute um dos seguintes:
   - (Recomendado) Crie um barramento de eventos EventBridge personalizado chamado`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternativa) Use o barramento de EventBridge eventos padrão em vez de um barramento de eventos personalizado.

   O AWS Incident Detection and Response instalará uma regra gerenciada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) no barramento de eventos personalizado ou padrão por meio da `AWSServiceRoleForHealth_EventProcessor` SLR. A fonte da regra será o barramento de eventos personalizado ou padrão, o destino da regra será o AWS Incident Detection and Response, e a regra corresponderá ao padrão de ingestão de eventos de APM de terceiros.

3. Crie uma função Lambda chamada `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` para transformar os eventos de ônibus de eventos de seu parceiro. Os eventos transformados corresponderão à regra gerenciada`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
   - Os eventos transformados incluem um identificador exclusivo de detecção e resposta de incidentes da AWS e definem a fonte e o tipo de detalhe do evento com os valores necessários. Isso permite que a estrutura de carga útil JSON transformada corresponda ao padrão de regra gerenciada.
   - Defina o destino da função Lambda para o barramento de eventos personalizado (recomendado) criado na Etapa 2 ou para o barramento de eventos padrão.
4. Crie uma EventBridge regra e defina os padrões de eventos que correspondem à lista de eventos que você deseja enviar para o AWS Incident Detection and Response. A origem da regra é o barramento de eventos do parceiro que você criou na Etapa 1 (`aws.partner/apm_name/integrationName`). O alvo da regra é a função Lambda que você criou na Etapa 3 ()`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`. Para obter diretrizes sobre como definir sua EventBridge regra, consulte EventBridge as regras da Amazon.

Para ver um exemplo passo a passo de como configurar manualmente integrações de barramentos de eventos de parceiros com o AWS Incident Detection and Response, consulte Integração de notificações do Datadog e do Splunk.

Ingira alarmes de APMs sem integração direta com EventBridge

O AWS Incident Detection and Response oferece suporte ao uso de webhooks para ingestão de alarmes de APMs de terceiros que não têm integração direta com a Amazon. EventBridge

Você pode implantar um CloudFormation modelo ou configurar manualmente a integração. Antes de configurar a integração, verifique se a função AWS vinculada ao serviço (SLR) `AWSServiceRoleForHealth_EventProcessor` foi criada em suas contas.

Opção 1: Usando CloudFormation Modelo

Um CloudFormation modelo está disponível para simplificar o processo de criação da infraestrutura de integração necessária para ingerir alarmes para o AWS Incident Detection and Response do seu APM que não tem integração direta com a Amazon. EventBridge

Considerações antes de implantar este modelo CloudFormation

- Essa solução usa um API Gateway Lambda Authorizer para comparar um token secreto passado na carga do seu APM com um token de entrada. AWS Secrets Manager Se o token não corresponder, uma política com uma negação explícita será retornada. Para obter mais informações, consulte Autorizadores Lambda.
- No modelo de Responsabilidade AWS Compartilhada, é sua responsabilidade garantir o uso de uma abordagem de autenticação que atenda aos requisitos de segurança da sua organização. Recomendamos o uso AWS Secrets Manager de um serviço similar, em vez de armazenar informações confidenciais, como chaves de API ou tokens de autorização, como variáveis codificadas. Para obter mais informações, consulte Criar e gerenciar segredos com o AWS Secrets Manager.
- Para ver mais um exemplo de implementação do Código de Autenticação de Hash-Based Mensagens (HMAC), consulte receive-webhooks na página aws-samples do Github. Para obter mais informações sobre a implementação da autorização de token, consulte o exemplo da função Lambda do autorizador de TOKEN na documentação do API Gateway.
- A solução usa RateLimitBurstLimit, e a cota no API Gateway para controlar os volumes de solicitações. Essas ferramentas limitam quantas solicitações podem ser processadas em um determinado horário. Isso ajuda a evitar a sobrecarga do sistema e mantém o serviço estável. Para obter mais informações sobre limitação, consulte o Guia do desenvolvedor do API Gateway.
- Considere usar o AWS Web Application Firewall (WAF) para proteger o API Gateway de endereços IP inválidos conhecidos. Isso reduz o risco de invasores inundarem a API com solicitações falsas que podem bloquear eventos de log reais.
- AWS Secrets Manager os valores de token devem ser armazenados na ferramenta Application Performance Monitoring (APM) como um cabeçalho HTTP. Certifique-se de alternar o token regularmente como uma prática recomendada de segurança.
- Custos adicionais serão incorridos com recursos implantados por meio desse CloudFormation modelo (por exemplo: Lambda e). EventBridge Para obter mais informações sobre os preços desses serviços, consulte AWS Preços.
- Depois de testar a integração, remova as instruções logger.info () da (função `TransformLambdaFunction` Lambda) para evitar que as cargas apareçam no Amazon Logs. CloudWatch
- Implante esse CloudFormation modelo em todas as AWS contas e regiões das quais o AWS Incident Detection and Response precisa ingerir alarmes.

Preparando o CloudFormation modelo:

Observação: as etapas de integração usam o Dynatrace como exemplo. No entanto, esse modelo pode ser usado para qualquer APM que possa enviar cargas para um API Gateway.

1. Baixe e abra o CloudFormation modelo.
2. Localize `APIGWUsagePlan` no modelo. Revise os valores configurados para `RateLimitBurstLimit`, e `Quota Limit` que estão definidos como 20, 50 e 2000 por padrão. Ajuste os valores para atender às suas necessidades.
3. Localize `AuthorizerLambdaFunction` no modelo. Essa função Lambda serve como exemplo de mecanismo de autenticação. Ele extrai um valor de token de um cabeçalho chamado`authorizationToken`, que é passado do seu APM. Você pode modificar esse código para se alinhar às políticas de segurança e aos requisitos de APM da sua organização.
4. Localize o `TransformLambdaFunction` no modelo. Substitua o caminho do dicionário`raw_json["detail"]["ProblemTitle"]`,, pelo caminho para o nome do seu alarme que é enviado na carga JSON do seu APM. Deixe isso como está para a Dynatrace.

Implantando o CloudFormation modelo:

1. Abra o CloudFormation console em sua conta de destino Região da AWS e.
2. Escolha Criar pilha, com novos recursos (padrão).
   - Selecione Escolher um modelo existente, Carregar um arquivo de modelo, Escolher arquivo e, em seguida, carregue o CloudFormation modelo que você salvou localmente.
3. Especifique os detalhes da pilha:
   - Insira o nome da pilha (exemplo, *`DynatraceIntegrationForIDR`*.)
   - APMNameParameter (exemplo, *`Dynatrace`*.)
   - Escolha Próximo.
4. Configure as opções de pilha:
   - Role até o final da página e marque a caixa para permitir CloudFormation a criação de recursos do IAM com nomes personalizados.
5. Revisar e criar:
   - Verifique se os valores dos parâmetros estão configurados corretamente e escolha Enviar.
6. A CloudFormation pilha implanta os recursos necessários para integrar seus eventos de APM ao AWS Incident Detection and Response. Espere até que o status da CloudFormation pilha seja CREATE_COMPLETE.

7. A CloudFormation pilha cria os recursos abaixo, supondo que o valor do exemplo `Dynatrace` tenha sido inserido nos parâmetros e executado na US-EAST-1 região.
   - Nome secreto: DynatraceMySecretTokenName (um valor secreto aleatório será criado com base na chave secreta APMSecureToken)
   - Recursos do API Gateway:
     - Nome da API: Dynatrace-AWSIncidentDetectionResponse-APIGW
     - Nome artístico: Dynatrace-Stage-Prod
     - Autorizadores: Dynatrace-APIGW-Authorizer
     - Plano de uso: APIGW_ Throttling_Plan
   - Funções do Lambda:
     - Função para autorização: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - Função para transformação: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - EventBus Nome personalizado: Dynatrace-AWSIncidentDetectionResponse-EventBus
   - Função do IAM:
     - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
     - AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1
8. Registre o URL do Webhook e o valor do token:
   - Abra o console do API Gateway e escolha o nome da API criado como parte da CloudFormation pilha.
   - Escolha Estágios na navegação à esquerda, expanda o nome do palco usando o sinal + e escolha POST. Registre o URL de invocação. Configure esse URL em seu APM como o destino para enviar webhooks para eventos de alarme.
   - Abra o AWS Secrets Manager console e escolha o nome secreto criado como parte da CloudFormation pilha. (Exemplo: DynatraceMySecretTokenName.)
     - Na guia Valor secreto, escolha Recuperar valor secreto. Você verá a chave secreta como APMSecureToken. Registre o valor secreto. Não compartilhe esse valor secreto com ninguém.

Teste de integração

Depois de implantar a pilha, teste a integração enviando uma carga de teste do seu APM:

1. Navegue até o console Lambda e selecione `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` a função. Escolha a guia Monitor (Monitorar).
2. Procure uma invocação bem-sucedida nos gráficos métricos.
3. Escolha Exibir Amazon CloudWatch Logs para verificar a carga útil do teste ou verificar se há erros nos fluxos de log.

Compartilhando seu ARN do Event Bus com o AWS Incident Detection and Response

1. Abra o Amazon EventBridge Console. Selecione Ônibus de eventos.
2. Copie o ARN do barramento de eventos personalizados criado como parte da CloudFormation pilha, exemplo:. *`arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`*
   - Adicione esse ARN ao campo “ARN do EventBridge Event Bus” na seção “Alarmes do Third-Party APM” do seu. Questionário de ingestão de alarmes - Visão geral
3. Durante o processo de integração, o AWS Incident Detection and Response criará uma EventBridge regra gerenciada nesse barramento de eventos personalizado para ingerir seus alarmes de APM.

Opção 2: integração manual

Use as etapas a seguir para configurar a integração com o AWS Incident Detection and Response.

1. Crie um Amazon API Gateway para aceitar a carga do seu APM.
2. Defina uma função Lambda para autorização usando um token de autenticação.
3. Execute um dos seguintes:
   - (Recomendado) Crie um barramento de eventos EventBridge personalizado chamado`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternativa) Use o barramento de EventBridge eventos padrão em vez de um barramento de eventos personalizado.
4. Defina uma função Transform Lambda para anexar o identificador de detecção e resposta de incidentes da AWS à sua carga. Você também pode usar essa função para filtrar os eventos que deseja enviar para o AWS Incident Detection and Response.

- O API Gateway deve invocar a função Transform Lambda, que transformará a carga transmitida pelo API Gateway.
- A função Transform Lambda deve gravar eventos transformados no barramento de eventos definido no ponto 3 acima.

5. Configure seu APM para enviar notificações para o URL gerado pelo API Gateway.

Alarmes de ingestão de APMs com integração direta com o Amazon SNS

Se o seu APM suporta o envio de alarmes para tópicos do Amazon SNS, você pode seguir este guia para incluir seus alarmes de APM no AWS Incident Detection and Response.

Você pode implantar o CloudFormation modelo fornecido ou configurar manualmente essa integração. Antes de configurar a integração, verifique se a função AWS vinculada ao serviço (SLR) `AWSServiceRoleForHealth_EventProcessor` foi criada em suas contas.

Opção 1: Usando CloudFormation

Um CloudFormation modelo está disponível para simplificar o processo de criação da infraestrutura de integração necessária para ingerir alarmes para o AWS Incident Detection and Response do seu APM com a integração do Amazon SNS.

> **Note**
>
> - Custos adicionais serão incorridos com recursos implantados por meio desse CloudFormation modelo (por exemplo: Lambda e). EventBridge Para obter mais informações sobre os preços desses serviços, consulte AWS Preços.
> - Esse CloudFormation modelo deve ser implantado em todas as AWS contas e regiões das quais os alarmes precisam ser ingeridos pelo AWS Incident Detection and Response.
> - Os exemplos fornecidos neste documento são para Grafana, no entanto, esse modelo pode ser usado para qualquer APM que tenha integração direta com o Amazon Simple Notification Service.
> - Por motivos de segurança, AWS recomenda remover `logger.info()` as declarações do `TransformLambdaFunction` para evitar que a carga seja registrada no Amazon CloudWatch Logs.

Pré-requisitos para implantar esse modelo: CloudFormation

- Um tópico padrão do Amazon Simple Notification Service deve ser criado para receber eventos de alarme do seu APM. Crie um tópico do SNS no console do Amazon Simple Notification Service.
- O `TransformLambdaFunction` no modelo deve ser modificado `["detail"]["incident-detection-response-identifier"]` para definir o valor desejado com base no APM que está sendo usado.

Conclusão do pré-requisito:

1. Abra o console do Amazon SNS e selecione Tópicos. Copie o ARN do tópico padrão do Amazon SNS criado para receber eventos de alarme do seu APM.
   - Exemplo: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. Baixe e abra o CloudFormation modelo
   - Localize o `TransformLambdaFunction` no modelo
     - Em `def lambda_handler(event, context)` definido como `event["detail"]["incident-detection-response-identifier"]` o caminho json em que o nome do alarme aparece na carga JSON do registro SNS.
       - Qualquer evento enviado para o `TransformLambdaFunction` via SNS tem uma estrutura de carga principal como. `event["Records"][n]["Sns"]["Message"]` A origem real da carga útil da fonte (APM) é encapsulada dentro da estrutura principal.
       - Exemplo para Grafana: `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

Implantando o CloudFormation modelo:

1. Navegue até o CloudFormation console na conta e na região em que você precisa configurar a integração.
2. Navegue até CloudFormation.
   - Escolha Criar pilha, com novos recursos (padrão)
     - Selecione Escolher um modelo existente, Carregar um arquivo de modelo, Escolher arquivo e, em seguida, carregue o CloudFormation modelo que você salvou localmente.
3. Especifique os detalhes da pilha:
   - Digite um nome de pilha Exemplo: `<your-apm-name>IntegrationForIDR`
   - Especifique os valores dos parâmetros obtidos durante o preenchimento do pré-requisito

    - APMNameParameterExemplo: `Grafana`
    - Exemplo do parâmetro TriggerSNS: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
  - Escolha Próximo.
4. Configure as opções de pilha:
  - Role até o final da página e confirme a caixa de seleção para permitir CloudFormation a criação de recursos do IAM com nomes personalizados.
5. Revisar e criar:
  - Verifique se os valores dos parâmetros estão configurados corretamente e escolha Enviar.
6. A CloudFormation pilha implantará os recursos necessários para integrar seus eventos de APM ao AWS Incident Detection and Response. Espere até que o status da CloudFormation pilha seja CREATE_COMPLETE.
7. A CloudFormation pilha cria os recursos abaixo assumindo que os valores de exemplo foram inseridos nos parâmetros do Grafana e foram executados na região. EU-WEST-1
  - CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
  - Assinatura 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 - [seqüência_aleatória]

Teste de integração

Depois que a CloudFormation pilha for implantada com sucesso, você poderá validar a integração enviando uma carga de teste do seu APM. Depois que a carga de teste for enviada do seu APM:

1. Navegue até o console Lambda e selecione a `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` função. Em seguida, escolha a guia Monitor.
2. Uma invocação bem-sucedida deve ser observada nos gráficos métricos.
3. Selecione Exibir CloudWatch registros da Amazon. Você pode verificar a partir dos eventos de log nos fluxos de log para confirmar se a carga de teste enviada do seu APM está presente ou se algum erro foi encontrado.

Compartilhando seu ARN do Event Bus com o AWS Incident Detection and Response

1. Navegue até o Amazon EventBridge Console. Selecione Ônibus de eventos.
2. Registre o ARN do barramento de eventos personalizado implantado como parte da CloudFormation pilha, por exemplo:. `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`
   - Forneça o ARN desse barramento de eventos personalizado para o AWS Incident Detection and Response no campo “EventBridge Event Bus ARN” da seção “Third-Party APM Alarms” do. Questionário de ingestão de alarmes - Visão geral
3. Durante o processo de integração, o AWS Incident Detection and Response criará uma EventBridge regra gerenciada nesse barramento de eventos personalizado para ingerir seus alarmes de APM.

Opção 2: integração manual

1. Abra o console do Amazon SNS e crie um tópico padrão do Amazon SNS `[apm_name]-sns` chamado para receber eventos de alarme do seu APM. Certifique-se de selecionar Padrão (não FIFO) como o tipo de tópico. Observe o ARN do tópico do Amazon SNS criado.
2. Execute um dos seguintes:
   - (Recomendado) Crie um barramento de eventos EventBridge personalizado chamado`[apm_name]-AWSIncidentDetectionResponse-EventBus`.
   - (Alternativa) Use o barramento de EventBridge eventos padrão em vez de um barramento de eventos personalizado.

   O AWS Incident Detection and Response instalará uma regra gerenciada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) no barramento de eventos personalizado ou padrão por meio da `AWSServiceRoleForHealth_EventProcessor` SLR. A fonte da regra será o barramento de eventos personalizado ou padrão, o destino da regra será o AWS Incident Detection and Response, e a regra corresponderá ao padrão de ingestão de eventos de APM de terceiros.
3. Crie uma função Lambda chamada `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` para transformar suas cargas do SNS.
   - Os eventos transformados devem atender aos requisitos de carga útil, conforme estabelecido em Requisitos de carga útil para ingerir alertas de APM com EventBridge

- Defina o destino da função Lambda para o barramento de eventos personalizado (recomendado) criado na Etapa 2 ou para o barramento de eventos padrão.

4. Defina o tópico do SNS como um gatilho para sua função `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` Lambda.
   - Na página “Adicionar acionadores”, pesquise por “SNS”.
   - Adicione o ARN do seu tópico de SNS dedicado criado na Etapa 1.
   - Escolha “Adicionar”.
5. Siga sua documentação de APM para configurar um destino de SNS para suas cargas de APM que precisam ser ingeridas pelo AWS Incident Detection and Response.

O AWS Incident Detection and Response instalará uma regra gerenciada (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) no barramento de eventos personalizado ou padrão por meio da `AWSServiceRoleForHealth_EventProcessor` SLR. A fonte da regra será o barramento de eventos personalizado ou padrão, o destino da regra será o AWS Incident Detection and Response, e a regra corresponderá ao padrão de ingestão de eventos de APM de terceiros.

Otimização de alarmes e ajustes de monitoramento

Para garantir a precisão ideal na detecção de incidentes, nossos engenheiros de gerenciamento de incidentes avaliam continuamente o desempenho do alarme em relação às suas cargas de trabalho críticas. Fornecemos alterações recomendadas na configuração de alarmes, que você deve fazer, e colaboramos proativamente com você e seus gerentes técnicos de contas (TAMs) para refinar essas configurações.

Quando os dados de monitoramento indicam que os alarmes podem não estar alinhados com suas operações críticas de negócios, como quando os alertas são acionados sem o impacto correspondente no cliente ou quando os estados dos alarmes flutuam com frequência, recomendamos desativar os alarmes não críticos e os alarmes de integração que reflitam melhor o impacto crítico da carga de trabalho. Isso ajuda a manter a eficácia geral de sua cobertura de resposta a incidentes.

Análise e feedback de alarmes

O AWS Incident Detection and Response conduz análises abrangentes de seus alarmes antes de integrá-los para monitoramento. Os alarmes são avaliados de acordo com critérios de aceitação técnica, incluindo parâmetros de configuração, qualidade dos dados e eficácia do alerta.

Com base nessa análise, dois tipos de feedback são fornecidos:

- Requisitos de configuração obrigatórios - essas alterações devem ser implementadas para aceitação do alarme.
- Recomendações de melhoria opcionais - essas mudanças aumentam a eficácia do alarme, mas não são obrigatórias para a aceitação do alarme.

Depois de receber esse feedback, você pode decidir continuar apenas com a integração de alarmes aceitos e aqueles que precisam de melhorias opcionais, enquanto trabalha paralelamente nas alterações de configuração de alarmes com requisitos obrigatórios de configuração.

Como alternativa, você pode implementar todas as alterações antes de colocá-las no ar. Essa abordagem estende o cronograma de integração, com base no número de alarmes que exigem ajustes.

Os alarmes entram em operação

Após a conclusão da ingestão do alarme, o AWS Incident Detection and Response permite o monitoramento da sua carga de trabalho. Deste ponto em diante, seus alarmes integrados são monitorados ativamente e o AWS Incident Detection and Response envolve você de acordo com o caderno de execução da carga de trabalho quando seus alarmes integrados entram no estado ALARM.

Principais saídas

- Sua carga de trabalho é confirmada como ativa e monitorada pelo AWS Incident Detection and Response.

Próximas etapas

- Para validar se seus alarmes integrados envolvem o AWS Incident Detection and Response conforme o esperado, consulte. Teste cargas de trabalho integradas em Detecção e Resposta a Incidentes
- Para fazer alterações nos alarmes integrados, no caderno de execução ou nas informações da carga de trabalho, consulte. Solicite alterações em uma carga de trabalho integrada na Detecção e Resposta a Incidentes

Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes (caminho de exceção)

> **Note**
>
> Se você não puder usar a CLI do IDR para integrar sua carga de trabalho, use os seguintes questionários para integração de cargas de trabalho e alarmes.

Este tópico fornece os questionários que você precisa preencher ao integrar uma carga de trabalho ao AWS Incident Detection and Response e ao configurar alarmes a serem ingeridos no serviço. O questionário de integração da carga de trabalho abrange informações gerais sobre sua carga de trabalho, detalhes de sua arquitetura e contatos para resposta a incidentes. No questionário de ingestão de alarmes, você especifica os alarmes críticos que acionam a criação de incidentes em Detecção e Resposta a Incidentes para sua carga de trabalho, bem como informações do caderno de execução sobre quem contatar e quais ações tomar. O preenchimento adequado desses questionários é uma etapa fundamental na configuração dos processos de monitoramento e resposta a incidentes para suas AWS cargas de trabalho.

Baixe o questionário de integração da carga de trabalho:

- Versão em inglês
- Versão japonesa

Baixe o questionário de ingestão de alarmes:

- Versão em inglês

- Versão japonesa

Questionário de integração da carga de trabalho - Perguntas gerais

Perguntas gerais

Pergunta	Exemplo de resposta
Nome da empresa	Amazon Inc.
Nome dessa carga de trabalho (inclua quaisquer abreviações)	Operações de varejo da Amazon (ARO)
Usuário final primário e a função dessa carga de trabalho.	Essa carga de trabalho é um aplicativo de comércio eletrônico que permite que os usuários finais comprem vários itens. Essa carga de trabalho é o principal gerador de receita para nossos negócios.

Questionário de integração da carga de trabalho - Perguntas sobre arquitetura

Perguntas sobre arquitetura

Pergunta	Exemplo de resposta
Uma lista de tags de AWS recursos usadas para definir recursos que fazem parte dessa carga de trabalho. AWS usa essas tags para identificar os recursos dessa carga de trabalho para agilizar o suporte durante incidentes. **Note** As tags diferenciam letras maiúsculas de minúsculas. Se você fornecer várias tags, todos os recursos usados por	Nome do aplicativo: Optimax ambiente: Produção

Pergunta	Exemplo de resposta
essa carga de trabalho deverão ter as mesmas tags.	
Uma lista de AWS service (Serviço da AWS)(s) utilizados por essa carga de trabalho, os Conta da AWS(s) e Região da AWS(s) em que eles estão.	Serviços da AWS: Rota 53, ALB, ECS,... Contas: 123456789101, 123456789102,... Regiões: US-EAST-1, US-WEST-2,...

Questionário de ingestão de alarmes - Visão geral

No questionário de ingestão de alarmes, você especifica os alarmes críticos para sua carga de trabalho que deseja engajar no AWS Incident Detection and Response, bem como os contatos que você deseja que um engenheiro de gerenciamento de incidentes entre em contato quando esses alarmes forem acionados.

O questionário de ingestão de alarmes é dividido nas seguintes seções:

- Seção de contato: Primeiro, especifique os contatos principais a serem incluídos no Suporte caso criado com o AWS Incident Detection and Response quando um alarme é acionado, bem como seu aplicativo de conferência preferido para pontes de incidentes. Se nenhuma preferência de ponte for fornecida, o AWS Incident Detection and Response criará uma ponte de incidentes durante incidentes. Em seguida, especifique os contatos de escalonamento e os intervalos de tempo para envolvê-los quando os contatos principais estiverem inacessíveis. Por fim, liste todos os contatos que devem receber atualizações regulares do status do incidente por meio do caso de suporte durante o incidente.
- Matriz de alarmes: liste o conjunto de alarmes que acionarão o AWS Incident Detection and Response quando acionados. Consulte os “Critérios críticos de alarme” definidos pelo AWS Incident Detection and Response ao selecionar alarmes para integração. Para obter mais informações, consulte Definição de alarme.
  - CloudWatch Alarmes da Amazon (deixe esta seção em branco se você não tiver CloudWatch alarmes da Amazon)
  - Alarmes de APM de terceiros (deixe esta seção em branco se você não tiver alarmes de APM de terceiros)

- EventBridge EventBus ARN: Esse é o ARN do ARN personalizado que você criou em ou EventBus . Ingira alarmes de APMs com integração direta EventBridge Ingira alarmes de APMs sem integração direta com EventBridge
- Identificadores de alarme: compartilhe o número da conta, a região e o nome do alarme do APM.

Questionário de ingestão de alarmes - Perguntas do Runbook

Perguntas do Runbook

Pergunta	Exemplo de resposta
AWS envolve os contatos da carga de trabalho por meio do Suporte caso. Quem é o contato principal quando um alarme é acionado para essa carga de trabalho? Especifique seu aplicativo de conferência preferido e AWS solicitará esses detalhes durante um incidente. **Note** Se um aplicativo de conferência preferencial não for fornecido, AWS entrará em contato durante um incidente e fornecerá uma ponte Chime para você participar.	Equipe de aplicação app@example.com +61 2 3456 7890
Se o contato principal não estiver disponível durante um incidente, forneça os contatos de escalonamento e o cronograma na ordem de comunicação preferida.	1. Após 10 minutos, se não houver resposta do contato principal, entre em contato com: John Smith - Supervisor de aplicativos john.smith@example.com +61 2 3456 7890

Pergunta	Exemplo de resposta
	2. Após 10 minutos, se não houver resposta de John Smith, entre em contato com: Jane Smith - Gerente de operações jane.smith@example.com +61 2 3456 7890

Matriz de alarme

Forneça as seguintes informações para identificar o conjunto de alarmes que envolverá o AWS Incident Detection and Response para criar incidentes em nome da sua carga de trabalho. Depois que os engenheiros da AWS Incident Detection and Response analisarem seus alarmes, etapas adicionais de integração serão fornecidas.

Critérios críticos de detecção e resposta a incidentes da AWS:

- Os alarmes de detecção e resposta a incidentes da AWS só devem entrar no estado de “Alarme” se houver um impacto comercial significativo na carga de trabalho monitorada (perda da experiência do revenue/degraded cliente) que exija atenção imediata do operador.
- Os alarmes de detecção e resposta a incidentes da AWS também devem envolver seus resolvedores para a carga de trabalho ao mesmo tempo ou antes do engajamento. AWS Os gerentes de incidentes colaboram com seus solucionadores no processo de mitigação e não atuam como socorristas de primeira linha, que depois recorrem a você.
- Os limites de alarme de detecção e resposta de incidentes da AWS devem ser definidos com um limite e uma duração apropriados para que, sempre que um alarme for acionado, uma investigação ocorra. Se um alarme estiver se movendo entre o estado “Alarme” e “OK”, um impacto suficiente está ocorrendo para garantir a resposta e a atenção do operador.

Política de detecção e resposta a incidentes da AWS para violações de critérios:

Esses critérios só podem ser avaliados caso a caso, à medida que os eventos ocorrem. A equipe de gerenciamento de incidentes trabalha com seus gerentes técnicos de contas (TAMs) para ajustar os alarmes e, em casos raros, desativar o monitoramento se houver suspeita de que os alarmes do

cliente não cumprem esses critérios e esteja contratando a equipe de gerenciamento de incidentes desnecessariamente a uma taxa regular.

> **Important**
>
> Forneça endereços de e-mail de distribuição em grupo ao fornecer endereços de contato, para que você possa controlar as adições e exclusões de destinatários sem atualizações do runbook.
> Forneça o número de telefone de contato da sua equipe de engenharia de confiabilidade do site (SRE) se quiser que a equipe de Detecção e Resposta de Incidentes da AWS ligue para eles depois de enviar um e-mail de engajamento inicial.

Tabela de matriz de alarmes para CloudWatch alarmes

CloudWatch ARN de alarme	Contato principal para este alarme. (Se for diferente do contato principal da carga de trabalho)	Especifique o mais relevante AWS service (Serviço da AWS) para esse alarme para acionar o engenheiro certo. Insira N/A se não for necessário.
Exemplo: `arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response`	Exemplo: Sam Smith - Gerente de aplicativos sam.smith@example.com +61 2 3456 7890	Exemplo: ECS

Tabela de matriz de alarmes para alarmes de APM de terceiros

EventBridge Ônibus de eventos ARN (Isso é criado como parte da integração de APM de terceiros para rotear alertas para o AWS Incident Detection and Response.)	Exemplo: (Haverá um ônibus de eventos por Account/Region combinação) `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 alarme	O que essa métrica representa? Por que esse alarme é importante?	Contato principal para este alarme. (Se for diferente do contato principal da carga de trabalho)	Especifique o mais relevante AWS service (Serviço da AWS) para esse alarme para acionar o engenheiro certo. Insira N/A se não for necessário.
Exemplo: ALB_5xX_ Target_Response ID da conta: 123456789012 Região: us-east-1	Exemplo: Essa métrica representa as respostas das transações dos alvos por trás do ALB. Se os erros 5XX excederem o limite, isso representará uma falha crítica no processamento de transações comerciais.	Exemplo: Sam Smith - Gerente de aplicativos sam.smith@example.com +61 2 3456 7890	Exemplo: ECS

Gerencie cargas de trabalho em Detecção e Resposta a Incidentes

Uma parte fundamental do gerenciamento eficaz de incidentes é ter os processos e procedimentos corretos para integrar, testar e manter suas cargas de trabalho monitoradas. Esta seção aborda as etapas essenciais, incluindo o desenvolvimento de runbooks e planos de resposta abrangentes para orientar suas equipes em incidentes, testar e validar exaustivamente novas cargas de trabalho, solicitar alterações para atualizar o monitoramento da carga de trabalho e desligar adequadamente as cargas de trabalho quando necessário.

Tópicos

Desenvolva runbooks e planos de resposta para responder a um incidente em Detecção e Resposta a Incidentes

O AWS Incident Detection and Response usa informações capturadas da integração do IDR CLI para desenvolver runbooks para o gerenciamento de incidentes que afetam suas cargas de trabalho. Os runbooks documentam as etapas que os gerentes de incidentes realizam ao responder a um incidente. Um plano de resposta é mapeado para pelo menos uma de suas cargas de trabalho. A equipe de gerenciamento de incidentes cria esses modelos a partir das informações fornecidas por você durante a integração da carga de trabalho.

Principais saídas:

- Conclusão da definição de sua carga de trabalho no AWS Incident Detection and Response.
- Conclusão de alarmes e runbooks sobre o AWS Incident Detection and Response.

Você também pode baixar um exemplo do AWS Incident Detection and Response Runbook: aws-idr-runbook-example.zip.

Exemplo de runbook

Example Exemplo de runbook

Description

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

Etapa: Prioridade

Ações prioritárias

1. Envie a primeira correspondência sobre o Suporte caso para o cliente conforme abaixo.

```
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>
```

Etapa: Informações

Planos de engajamento

Esta seção descreve os planos de engajamento aplicáveis a este runbook e contém somente detalhes de contato. Os planos de engajamento serão referenciados nos Planos de Comunicação passo a passo.

- Engajamento inicial

  A equipe de detecção e resposta a incidentes da AWS adiciona os endereços das partes interessadas do cliente abaixo ao Suporte caso. AWS as partes interessadas são para outras partes interessadas que talvez precisem ser informadas sobre quaisquer problemas.

  - Partes interessadas do cliente: e-mail do cliente 1; e-mail do cliente 2; celular 1

- AWS Partes interessadas: aws-idr-oncall@amazon.com; e-mail da equipe de equipe; etc.
- Contatos únicos: [Esses são contatos de e-mail incluídos somente na primeira comunicação. Remova esses contatos após o término da primeira comunicação. Podem ser endereços de e-mail de paginação de clientes, como pager-duty, que não devem ser paginados em todas as correspondências. Adicione explicitamente instruções na seção “Prioridade”, “Planos de comunicação” sobre como usá-los somente se os Contatos Únicos estiverem disponíveis.]

- Configuração de chamada de incidente

  Indique se o cliente precisa do AWS Incident Detection and Response para criar uma ponte, se o cliente usa uma ponte estática ou se o cliente fornecerá uma ponte quando um incidente for aberto.

  (Escolha uma opção com base na preferência do cliente)

  - AWS Incident Detection and Response criam uma Amazon Chime/Zoom Bridge
  - Ponte estática fornecida pelo cliente
    - Número da conferência: **<** Insert Conference number **>**
  - O cliente fornece detalhes sobre cada incidente respondendo à comunicação enviada pela equipe de detecção e resposta a incidentes da AWS.
  - Outros - Especifique os detalhes.

- Escalonamento do engajamento

  O AWS Incident Detection and Response entrará em contato com os seguintes contatos quando os contatos do plano de engajamento inicial não responderem aos incidentes.

  Para cada contato de escalonamento, indique se eles devem ser adicionados ao Suporte caso, telefonados ou ambos.

  - Certifique-se de ter ligado para o contato inicial de engajamento, se aplicável, antes de escalar.
  - Primeiro contato de escalonamento: [escalation EmailAddress #1]/[PhoneNumber] - Aguarde XX minutos antes de escalar para esse contato.
    - [Adicionar contato ao caso/telefone] esse contato.
  - Segundo contato de escalonamento: [escalation EmailAddress #2]/[PhoneNumber] - Aguarde XX minutos antes de escalar para esse contato.
    - [Adicionar contato ao caso/telefone] este contato.
  - etc.

Planos de comunicação

Esta seção descreve como os engenheiros de gerenciamento de incidentes se comunicam com as partes interessadas designadas fora dos canais de comunicação e chamada de incidentes.

- Plano de comunicação de impacto

  Esse plano é iniciado quando o AWS Incident Detection and Response determinou, a partir da etapa de triagem, que um alerta indica um impacto potencial para o cliente.

  O AWS Incident Detection and Response solicitará que o cliente participe da ponte predeterminada, conforme indicado em Planos de engajamento — Configuração de chamadas de incidentes.

  (Escolha um, dependendo se os Contatos Somente Uma Vez estão disponíveis ou não.)

  1. Garanta que as partes interessadas do cliente usem os planos de engajamento - o engajamento inicial é adicionado ao CC do caso.

  OU

  1. Garanta que as partes interessadas do cliente e os contatos únicos dos planos de engajamento - o engajamento inicial sejam adicionados ao CC do caso.
  2. Envie a notificação de engajamento ao cliente com base no seguinte modelo:

     (Escolha um)

     Modelo 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/
     ```

     Modelo de impacto - Ponte fornecida pelo 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.
```

Modelo 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 o caso como Ação pendente do cliente.
4. REMOVA os contatos únicos do estojo após enviar a Comunicação de impacto acima. (Se somente contatos ocasionais estiverem disponíveis.)
5. Siga o plano de escalonamento de engajamento conforme mencionado acima.
6. Se o cliente não responder em 30 minutos, desative e continue monitorando até que o alarme se recupere.

- Plano de comunicação sem impacto

Esse plano é iniciado quando um alarme é recuperado antes que a Detecção e a Resposta a Incidentes concluam a triagem inicial.

1. Antes de enviar a notificação sem impacto, verifique e, em seguida, remova a and/or adição de contatos do cliente do Suporte Case CC com base nos contatos listados em Planos de engajamento - Plano de engajamento inicial.

   ["NÃO adicione contatos únicos."] (Aplicável se somente contatos ocasionais estiverem disponíveis.)

2. Envie uma notificação de não engajamento ao cliente com base no modelo abaixo:

   Modelo sem 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. Coloque o caso em Ação pendente do cliente.
4. Se o cliente não responder em 30 minutos, resolva o caso.

Visão geral da arquitetura de aplicativos

Esta seção fornece uma visão geral da application/workload arquitetura para conscientização do engenheiro de gerenciamento de incidentes e do engenheiro de operações.

- AWS Contas e regiões com os principais serviços - lista de AWS contas com regiões que suportam este aplicativo. Auxilia os engenheiros na avaliação da infraestrutura subjacente que dá suporte ao aplicativo.
  - 123456789012
    - US-EAST-1 - breve descrição, conforme apropriado
      - Amazon EC2 — breve descrição, conforme apropriado
      - DynamoDB - breve descrição, conforme apropriado
      - etc.
    - US-WEST-1 - breve descrição, conforme apropriado
      - etc.
  - outra conta
    - etc.

Teste cargas de trabalho integradas em Detecção e Resposta a Incidentes

Depois de Ingestão de alarmes concluído, o AWS Incident Detection and Response habilita a monitorar sua carga de trabalho e envia uma Go-Live confirmação. Sua carga de trabalho é monitorada ativamente a partir de agora.

O teste de alarme valida que seus alarmes integrados ativam o AWS Incident Detection and Response conforme o esperado, acionam os runbooks apropriados e quaisquer outras ações desejadas, como a criação automática de casos, caso você a tenha selecionado durante a ingestão do alarme.

O teste é opcional, mas altamente recomendado. Você é responsável por validar seus arranjos de resposta antes que ocorra um incidente real.

Opções de teste

O AWS Incident Detection and Response oferece duas opções de teste.

Opção 1: Programado GameDay (recomendado)

Um agendado GameDay é uma simulação ao vivo de ponta a ponta do que pode acontecer durante um incidente real. O AWS Incident Detection and Response segue as etapas prescritas pelo runbook para fornecer uma visão de como um incidente real pode se desenrolar. GameDay É uma oportunidade para você fazer perguntas ou refinar instruções para melhorar o engajamento.

Para agendar um GameDay, conclua as seguintes etapas:

1. Notifique o AWS Incident Detection and Response com uma data preferida e uma janela horária de 1 hora, incluindo fuso horário. Forneça pelo menos 48 horas de prazo de entrega.
2. Planeje recursos para o GameDay, incluindo sua SRE/Ops equipe e contatos de escalonamento.

GameDay cronograma:

1. Você e o AWS Incident Detection and Response participam da chamada.
2. Você desativa as ações de alarme, se aplicável.

3. Você configura manualmente seus alarmes para o estado ALARME usando as instruções emComo testar seus alarmes.
4. O AWS Incident Detection and Response confirma o recebimento da notificação de alarme.
5. O AWS Incident Detection and Response responde ao alarme e se junta à ponte prescrita em seu runbook.
6. Você e o AWS Incident Detection and Response confirmam o GameDay resultado.

Opção 2: teste de alarme off-line

Você pode testar seus alarmes de forma independente a qualquer momento, sem agendar uma chamada. O acionamento de um alarme ativa o AWS Incident Detection and Response de acordo com seu runbook, da mesma forma que faria durante um incidente real.

Para realizar o teste de alarme off-line, conclua as seguintes etapas:

1. Para evitar ações não intencionais, desative todas as ações de CloudWatch alarme da Amazon.
2. Acione seus alarmes usando as instruções emComo testar seus alarmes.
3. Em 5 minutos, um caso de suporte é criado em seu nome e o AWS Incident Detection and Response envolve com você conforme especificado em seu runbook.
4. Notifique o Incident Manager de que você está realizando testes de alarme off-line.
5. O gerente de incidentes confirma quais mudanças no estado do alarme foram recebidas e valida os arranjos de resposta.

Se um caso de suporte não for criado em 5 minutos, envie uma solicitação de incidente para contratar manualmente o AWS Incident Detection and Response para solucionar problemas.

Como testar seus alarmes

CloudWatch Alarmes da Amazon

> **Note**
>
> O AWS Identity and Access Management usuário ou a função que você usa para o teste de alarme deve ter `cloudwatch:SetAlarmState` permissão.

Use o AWS Command Line Interface ou AWS CloudShellpara definir manualmente o alarme para o estado ALARME. Esses comandos alteram o estado do alarme sem afetar sua carga de trabalho.

Para evitar ações não intencionais, por exemplo, reinicializações de instâncias do Amazon EC2, desative CloudWatch todas as ações de alarme antes de alterar o estado do alarme. Você pode reativar as ações CloudWatch de alarme após a conclusão do teste. Para saber mais sobre como desativar ou ativar ações de alarme, consulte DisableAlarmActionse EnableAlarmActionsna Amazon CloudWatch API Reference.

Desative as ações de alarme:

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

Defina o estado do alarme para ALARM:

```
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 ações de alarme após o teste:

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

O estado do alarme é revertido para OK automaticamente em alguns segundos.

Alarmes compostos

O **`set-alarm-state`** comando não garante que os alarmes compostos voltem ao estado OK. Como prática recomendada, verifique o estado dos alarmes compostos após o teste. Para redefinir manualmente um alarme composto, use o seguinte 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 saber mais sobre como alterar manualmente o estado dos CloudWatch alarmes, consulte SetAlarmStatea Amazon CloudWatch API Reference.

Para saber mais sobre as permissões necessárias para operações de CloudWatch API, consulte a referência de CloudWatch permissões da Amazon.

Third-party Alarmes APM

As cargas de trabalho que usam uma ferramenta de monitoramento de desempenho de aplicativos (APM) de terceiros, como Datadog, Splunk, New Relic ou Dynatrace, exigem instruções diferentes para simular um alarme.

1. Desative as ações de alarme em seu APM para evitar ações não intencionais.
2. Modifique seu limite de alarme ou operador de comparação para forçar o alarme a entrar no status ALARM. Isso aciona uma carga para o AWS Incident Detection and Response.
3. Após a conclusão do teste, reverta o limite ou as alterações do operador de comparação para restaurar o status OK do alarme.

Principais resultados

Após o teste bem-sucedido:

- A ingestão de alarmes foi confirmada e sua configuração de alarme está correta.
- Os alarmes são recebidos pelo AWS Incident Detection and Response.
- Um caso de suporte é criado e seus contatos prescritos são notificados.
- O AWS Incident Detection and Response envolve você de acordo com os meios de conferência prescritos.
- Todos os alarmes e casos de suporte gerados durante o teste são resolvidos.

Perguntas frequentes

O teste de alarme é obrigatório?

Não. O teste é opcional, mas é altamente recomendável para validar seus arranjos de resposta de ponta a ponta antes que ocorra um incidente real.

Minha carga de trabalho será afetada?

Não. No entanto, durante o teste, todas as ações de alarme configuradas em seus alarmes são acionadas, a menos que você as desative. Desative as ações de alarme antes do teste para evitar impactos não intencionais.

Quem é notificado durante o teste?

Durante um agendamento GameDay, todos os contatos e caminhos de escalonamento em seu runbook são contatados para verificação. Durante o teste de alarme off-line, somente o contato inicial especificado durante a integração do alarme é notificado.

Posso responder por e-mail às atualizações do caso?

Não. Cópias por e-mail das correspondências do Suporte caso são enviadas de um endereço sem resposta. Para atualizar um caso, use AWS Support Center Console.

Como faço para solicitar um GameDay after go-live?

Responda ao seu caso de suporte de integração existente, se ele existir, ou crie umSolicite alterações em uma carga de trabalho integrada na Detecção e Resposta a Incidentes.

Solicite alterações em uma carga de trabalho integrada na Detecção e Resposta a Incidentes

Para solicitar alterações em uma carga de trabalho integrada, conclua as etapas a seguir para criar um caso de suporte com o AWS Incident Detection and Response.

1. Vá até o AWS Support Centro e selecione Criar caso, conforme mostrado no exemplo a seguir:

2. Escolha Técnico.
3. Em Serviço, escolha Detecção e resposta a incidentes.
4. Em Categoria, escolha Solicitação de alteração de carga de trabalho.
5. Em Severidade, escolha Orientação geral.
6. Insira um assunto para essa alteração. Por exemplo:

   Detecção e resposta a incidentes da AWS — *`workload_name`*
7. Insira uma Descrição para essa alteração. Por exemplo, insira “Esta solicitação é para alterações em uma carga de trabalho existente integrada ao AWS Incident Detection and Response”. Certifique-se de incluir as seguintes informações em sua solicitação:

   - Nome da carga de trabalho: o nome da sua carga de trabalho.
   - ID (s) da conta: ID1, ID2, ID3 e assim por diante.

- Detalhes da alteração: insira os detalhes da alteração solicitada.

8. Na seção Contatos adicionais - opcional, insira os IDs de e-mail que você deseja receber correspondência sobre essa alteração.

   Veja a seguir um exemplo da seção Contatos adicionais - opcional.

   > **Important**
   >
   > A falha ao adicionar IDs de e-mail na seção Contatos adicionais - opcional pode atrasar o processo de alteração.

9. Selecione Enviar.

   Depois de enviar a solicitação de alteração, você pode adicionar outros e-mails da sua organização. Para adicionar e-mails, escolha Responder nos detalhes do caso, conforme mostrado no exemplo a seguir:

   Em seguida, adicione os IDs de e-mail na seção Contatos adicionais - opcional.

   Veja a seguir um exemplo da página de resposta mostrando onde você pode inserir e-mails adicionais.

Impeça que os alarmes ativem a Detecção e a Resposta a Incidentes

Especifique quais dos seus alarmes de carga de trabalho integrados interagem com o monitoramento de detecção e resposta de incidentes da AWS, suprimindo-os temporariamente ou de forma programada. Por exemplo, você pode suprimir temporariamente os alarmes de carga de trabalho durante a manutenção planejada para evitar que os alarmes ativem a Detecção e a Resposta a Incidentes. Ou você pode suprimir os alarmes de forma programada se tiver uma atividade diária de reinicialização. Você pode suprimir os alarmes na fonte do alarme, como a Amazon CloudWatch, ou enviar uma solicitação de alteração da carga de trabalho.

Tópicos

- Suprimir alarmes na fonte de alarme
- Envie uma solicitação de alteração da carga de trabalho para suprimir os alarmes
- Tutorial: Use uma função matemática métrica para suprimir um alarme
- Tutorial: Remova uma função matemática métrica para cancelar a supressão de um alarme

Suprimir alarmes na fonte de alarme

Especifique quais alarmes interagem com a Detecção e Resposta a Incidentes e quando isso acontece, suprimindo os alarmes na fonte do alarme.

Tópicos

- Use uma função matemática métrica para suprimir um alarme CloudWatch
- Remova uma função matemática métrica para cancelar a supressão de um alarme CloudWatch
- Exemplos de funções matemáticas métricas e casos de uso associados
- Suprimir alarmes de um APM de terceiros

Use uma função matemática métrica para suprimir um alarme CloudWatch

Para suprimir o monitoramento de detecção e resposta a incidentes dos CloudWatch alarmes da Amazon, use uma função matemática métrica para impedir que CloudWatch os alarmes entrem no `ALARM` estado durante uma janela designada.

> **Note**
>
> Desativar as ações de alarme em um CloudWatch alarme não suprime o monitoramento de seus alarmes pela detecção e resposta a incidentes. As mudanças no estado do alarme são ingeridas pela Amazon EventBridge, não por meio de ações CloudWatch de alarme.

Para usar uma função matemática métrica para suprimir um CloudWatch alarme, conclua as seguintes etapas:

1. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.

2. Escolha Alarmes e, em seguida, localize o alarme ao qual você deseja adicionar a função matemática métrica.
3. Escolha Ações e, em seguida, selecione Editar para alterar o alarme.
4. Escolha Editar métrica para modificar a métrica do alarme.
5. Escolha Adicionar matemática, Comece com uma expressão vazia.
6. Insira sua expressão matemática e escolha Aplicar.
7. Desmarque a métrica existente que o alarme monitorou.
8. Selecione a expressão que você acabou de criar e escolha Selecionar métrica.
9. Escolha Ir para visualizar e criar.
10. Revise suas alterações para garantir que sua função matemática métrica seja aplicada conforme o esperado e, em seguida, escolha Atualizar alarme.

Para obter um exemplo passo a passo da supressão de um CloudWatch alarme com uma função matemática métrica, consulteTutorial: Use uma função matemática métrica para suprimir um alarme.

Para obter mais informações sobre sintaxe e funções disponíveis, consulte Sintaxe matemática métrica e funções no Guia CloudWatch do usuário da Amazon.

Remova uma função matemática métrica para cancelar a supressão de um alarme CloudWatch

Cancele a supressão de um CloudWatch alarme removendo a função matemática métrica. Para remover uma função matemática métrica de um alarme, conclua as seguintes etapas:

1. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Alarmes e, em seguida, localize o alarme ou alarmes dos quais você deseja remover a expressão matemática métrica.
3. Na seção matemática métrica, escolha Editar.
4. Para remover a métrica do alarme, escolha Editar na métrica e, em seguida, escolha o botão x ao lado da expressão matemática métrica.
5. Selecione a métrica original e escolha Selecionar métrica.
6. Escolha Ir para visualizar e criar.

7. Revise suas alterações para garantir que sua função matemática métrica seja aplicada conforme o esperado e escolha Atualizar alarme.

Exemplos de funções matemáticas métricas e casos de uso associados

A tabela a seguir contém exemplos de funções matemáticas métricas, além de casos de uso associados e uma explicação de cada componente métrico.

Função matemática métrica	Caso de uso	Explicação
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	Suprima o alarme entre 1h e 3h UTC todas as terças-feiras substituindo pontos de dados reais por 0 durante essa janela.	• DIA (m1) == 2: Garante que seja terça-feira (segunda-feira = 1, domingo = 7). • HORA (m1) >= 1 && HORA (m1) > 3: especifica o intervalo de tempo de 1h às 3h UTC. • IF (condition, value_if_true, value_if_false :Se as condições forem verdadeiras, substitua o valor da métrica por 0. Caso contrário, retorne o valor original (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	Suprima o alarme entre 23h e 4h UTC, diariamente, substituindo pontos de dados reais por 0 durante essa janela.	• HORA (m1) >= 23: captura as horas a partir das 23:00 UTC. • HORA (m1) < 4: captura as horas até (mas não incluindo) 04:00 UTC. • ||: O OR lógico garante que a condição se aplique em dois intervalos: madrugada e madrugada.

Função matemática métrica	Caso de uso	Explicação
		• IF (condition, value_if_true, value_if_false): retorna 0 durante o intervalo de tempo especificado. Mantém o valor métrico original m1 fora desse intervalo.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	Suprima o alarme entre 11h e 13h UTC diariamente substituindo pontos de dados reais por 0 durante essa janela.	• HORA (m1) >= 11 && HORA (m1) < 13: captura o intervalo de tempo das 11:00 às 13:00 UTC. • IF (condition, value_if_true, value_if_false): Se a condição for verdadeira (por exemplo, o horário estiver entre 11:00 e 13:00 UTC), retorne 0. Se a condição for falsa, retenha o valor métrico original (m1).

Função matemática métrica	Caso de uso	Explicação
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	Suprima o alarme entre 1h e 3h UTC todas as terças-feiras substituindo pontos de dados reais por 99 durante essa janela.	• DIA (m1) == 2:: Garante que seja terça-feira (segunda-feira = 1, domingo = 7). • HORA (m1) >= 1 && HORA (m1) < 3: especifica o intervalo de tempo de 1h às 3h UTC. • IF (condition, value_if_true, value_if_false): Se as condições forem verdadeiras, substitua o valor da métrica por 99. Caso contrário, retorne o valor original (m1).
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	Suprima o alarme entre 23h e 4h UTC, diariamente, substituindo pontos de dados reais por 100 durante essa janela.	• HORA (m1) >= 23: captura as horas a partir das 23:00 UTC. • HORA (m1) < 4: captura as horas até (mas não incluindo) 04:00 UTC. • ||: O OR lógico garante que a condição se aplique em dois intervalos: madrugada e madrugada. • IF (condition, value_if_true, value_if_false): retorna 100 durante o intervalo de tempo especificado. Mantém o valor métrico original m1 fora desse intervalo.

Função matemática métrica	Caso de uso	Explicação
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	Suprima o alarme entre 11h e 13h UTC diariamente, substituindo pontos de dados reais por 99 durante essa janela.	• HORA (m1) >= 11 && HORA (m1) < 13: captura o intervalo de tempo das 11:00 às 13:00 UTC. • IF (condition, value_if_ true, value_if_false): Se a condição for verdadeira (por exemplo, o horário é entre 11:00 e 13:00 UTC), retorne 99. Se a condição for falsa, mantenha o valor métrico original (m1).

Suprimir alarmes de um APM de terceiros

Consulte a documentação do seu fornecedor terceirizado de APM para obter instruções sobre como suprimir alarmes. Exemplos de fornecedores terceirizados de APM são New Relic, Splunk, Dynatrace, Datadog e. SumoLogic

Envie uma solicitação de alteração da carga de trabalho para suprimir os alarmes

Se você não conseguir suprimir os alarmes na fonte conforme descrito na seção anterior, envie uma Solicitação de Alteração da Carga de Trabalho para instruir a Detecção e Resposta a Incidentes a suprimir manualmente o monitoramento de alguns ou de todos os alarmes da sua carga de trabalho.

Para obter instruções detalhadas sobre como criar uma solicitação de alteração de carga de trabalho, consulte Solicitar alterações em uma carga de trabalho integrada em Detecção e resposta a incidentes. Ao gerar uma solicitação de alteração de carga de trabalho para solicitar a supressão de seus alarmes, certifique-se de fornecer as seguintes informações obrigatórias

- Nome da carga de trabalho: o nome da sua carga de trabalho.
- ID (s) da conta: ID1, ID2, ID3, e assim por diante.
- Detalhes da alteração: Supressão de alarme

- Hora de início da supressão: data, hora e fuso horário.
- Hora de término da supressão: data, hora e fuso horário.
- Alarmes a serem suprimidos: uma lista de identificadores de CloudWatch alarmes ARNs ou eventos de APM de terceiros a serem suprimidos.

Depois de criar a solicitação de alteração da carga de trabalho de supressão de alarmes, você recebe as seguintes notificações da Detecção e Resposta a Incidentes:

- Confirmação de sua solicitação de alteração de carga de trabalho.
- Notificação quando os alarmes são suprimidos.
- Notificação quando os alarmes são reativados para monitoramento.

Tutorial: Use uma função matemática métrica para suprimir um alarme

O tutorial a seguir explica como suprimir um CloudWatch alarme usando matemática métrica.

Exemplo de cenário

Há uma atividade planejada que acontece entre 1h e 3h UTC na próxima terça-feira. Você deseja criar uma função matemática CloudWatch métrica que substitua os pontos de dados reais durante esse período por 0 (um ponto de dados que fica abaixo do limite definido).

1. Avalie os critérios que fazem com que o alarme seja acionado. A captura de tela a seguir fornece um exemplo de critérios de alarme:

   O alarme mostrado na captura de tela anterior monitora a `UnHealthyHostCount` métrica de um grupo-alvo do Application Load Balancer. Esse alarme entra no `ALARM` estado em que a `UnHealthyHostCount` métrica é maior ou igual a 3 para 5 dos 5 pontos de dados. O alarme trata os dados perdidos como ruins (violando o limite configurado).
2. Crie a função matemática métrica.

   Neste exemplo, a atividade planejada ocorre entre 1h e 3h UTC na próxima terça-feira. Portanto, crie uma função matemática CloudWatch métrica que substitua os pontos de dados reais durante esse tempo por 0 (um ponto de dados que fica abaixo do limite definido).

Observe que o ponto de dados de substituição que você deve configurar difere dependendo da configuração do alarme. Por exemplo, se você tiver um alarme que monitora a taxa de sucesso de HTTP, com um limite menor que 98, substitua seus pontos de dados reais durante a atividade planejada por um valor acima do limite configurado, 100. Veja a seguir um exemplo de função matemática métrica para esse cenário.

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

A função matemática métrica anterior contém os seguintes elementos:

- DIA (m1) == 2: Garante que seja terça-feira (segunda-feira = 1, domingo = 7).
- HORA (m1) >= 1 && HORA (m1) < 3: especifica o intervalo de tempo de 1h às 3h UTC.
- IF (condition, value_if_true, value_if_false): Se as condições forem verdadeiras, a função substituirá o valor da métrica por 0. Caso contrário, o valor original (m1) será retornado.

Para obter informações adicionais sobre sintaxe e funções disponíveis, consulte Funções e sintaxe matemática métricas no Guia do usuário da Amazon CloudWatch

3. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
4. Escolha Alarmes e, em seguida, localize o alarme ao qual você deseja adicionar a função matemática métrica.
5. Na seção matemática métrica, escolha Editar.
6. Escolha Adicionar matemática, Comece com uma expressão vazia.
7. Insira sua expressão matemática e, em seguida, escolha Aplicar.

   A métrica existente que o alarme monitora automaticamente se torna m1 e sua expressão matemática é e1, conforme mostrado no exemplo a seguir:

8. (Opcional) Edite o rótulo da expressão matemática métrica para ajudar outras pessoas a entender sua função e por que ela foi criada, conforme mostrado no exemplo a seguir:

9. Desmarque m1, selecione e1 e, em seguida, escolha Selecionar métrica. Isso configura o alarme para monitorar diretamente a expressão matemática em vez da métrica subjacente.
10. Escolha Ir para visualizar e criar.

11. Confirme se o alarme está configurado conforme o esperado e escolha Atualizar alarme para salvar a alteração.

No exemplo anterior, sem a função matemática métrica aplicada, a `UnHealthyHostCount` métrica real teria sido relatada durante a atividade planejada. Isso teria resultado na entrada do CloudWatch alarme no `ALARM` estado e na ativação da Detecção e Resposta a Incidentes, conforme mostrado no exemplo a seguir:

Com a função matemática métrica instalada, os pontos de dados reais são substituídos por 0 durante a atividade e o alarme permanece no `OK` estado, suprimindo o engajamento de detecção e resposta a incidentes.

Tutorial: Remova uma função matemática métrica para cancelar a supressão de um alarme

Se você suprimir um CloudWatch alarme para uma atividade única, remova a função matemática métrica do alarme após a conclusão da atividade para retomar o monitoramento regular do alarme. Para suprimir o alarme regularmente, por exemplo, se você tiver uma rotina de correção semanal programada que resulte em reinicializações de instâncias no mesmo dia e horário todas as semanas, deixe a função matemática métrica no lugar.

O tutorial a seguir explica como remover uma função matemática métrica para cancelar a supressão de um alarme CloudWatch

1. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Alarmes e, em seguida, localize o alarme ao qual você deseja adicionar a função matemática métrica.
3. Na seção matemática métrica, escolha Editar.
4. Para remover a supressão do alarme, selecione o botão x ao lado da expressão matemática métrica.

5. Selecione a métrica para retomar o monitoramento da métrica real. Em seguida, escolha Selecionar métrica.

6. Escolha Ir para visualizar e criar.
7. Confirme se o alarme está configurado conforme o esperado e escolha Atualizar alarme para salvar a alteração.

Remova uma carga de trabalho da Detecção e Resposta a Incidentes

Para remover uma carga de trabalho do AWS Incident Detection and Response, crie um novo caso de suporte para cada carga de trabalho. Ao criar o caso de suporte, lembre-se do seguinte:

- Para reduzir uma carga de trabalho que está em uma única AWS conta, crie o caso de suporte a partir da conta da carga de trabalho ou da sua conta pagadora.
- Para reduzir uma carga de trabalho que abrange várias AWS contas, crie o caso de suporte a partir da sua conta pagadora. No corpo do caso de suporte, liste todas as IDs de conta como off-board.

> **Important**
>
> Se você criar um caso de suporte para remover uma carga de trabalho da conta incorreta, poderá enfrentar atrasos e solicitações de informações adicionais antes que suas cargas de trabalho possam ser transferidas.

Solicitação para desembarcar uma carga de trabalho

1. Vá para o AWS Support Centro e selecione Criar caso.
2. Escolha Técnico.
3. Em Serviço, escolha Detecção e resposta a incidentes.
4. Em Categoria, escolha Desligamento da carga de trabalho.
5. Em Severidade, escolha Orientação geral.
6. Insira um assunto para essa alteração. Por exemplo:

   [Offboard] Detecção e resposta a incidentes da AWS — *`workload_name`*

7. Insira uma Descrição para essa alteração. Por exemplo, insira “Esta solicitação é para desvincular uma carga de trabalho existente integrada ao AWS Incident Detection and Response”. Certifique-se de incluir as seguintes informações em sua solicitação:

   - Nome da carga de trabalho: o nome da sua carga de trabalho.
   - ID (s) da conta: ID1, ID2, ID3 e assim por diante.
   - Motivo da desativação: forneça um motivo para a redução da carga de trabalho.
8. Na seção Contatos adicionais - opcional, insira os IDs de e-mail que você deseja que recebam correspondência sobre essa solicitação de desligamento.
9. Selecione Enviar.

Monitoramento e observabilidade do AWS Incident Detection and Response

O AWS Incident Detection and Response oferece orientação especializada sobre como definir a observabilidade em suas cargas de trabalho, desde a camada de aplicação até a infraestrutura subjacente. O monitoramento indica que algo está errado. A observabilidade usa a coleta de dados para dizer o que está errado e por que isso aconteceu.

O sistema de detecção e resposta a incidentes monitora suas AWS cargas de trabalho em busca de falhas e degradação do desempenho, aproveitando AWS serviços nativos, como Amazon e CloudWatch Amazon, EventBridge para detectar eventos que possam afetar sua carga de trabalho. O monitoramento fornece notificações de falhas iminentes, contínuas, recorrentes ou potenciais ou de degradação do desempenho. Ao integrar sua conta à Detecção e Resposta a Incidentes, você seleciona quais alarmes em sua conta devem ser monitorados pelo sistema de monitoramento de Detecção e Resposta a Incidentes e associa esses alarmes a um aplicativo e a um runbook usados durante o gerenciamento de incidentes.

A Detecção e Resposta a Incidentes usa a Amazon CloudWatch e outras empresas Serviços da AWS para criar sua solução de observabilidade. O AWS Incident Detection and Response ajuda você com a observabilidade de duas maneiras:

- Métricas de resultados comerciais: a observabilidade na detecção e resposta de incidentes da AWS começa com a definição das principais métricas que monitoram os resultados de suas cargas de trabalho ou da experiência do usuário final. AWS os especialistas trabalham com você para entender os objetivos de sua carga de trabalho, os principais resultados ou fatores que podem afetar a experiência do usuário e para definir as métricas e alertas que capturam qualquer degradação nessas métricas principais. Por exemplo, uma métrica comercial importante para um aplicativo de chamadas móveis é a taxa de sucesso da configuração de chamadas (monitora a taxa de sucesso das tentativas de chamadas do usuário), e uma métrica importante para um site é a velocidade da página. O engajamento de incidentes é acionado com base nas métricas de resultados comerciais.
- Métricas de nível de infraestrutura: nesse estágio, identificamos a base Serviços da AWS e a infraestrutura que suporta seu aplicativo e definimos métricas e alarmes para monitorar o desempenho desses serviços de infraestrutura. Isso pode incluir métricas como `ApplicationLoadBalancerErrorCount` para instâncias do Application Load Balancer. Isso começa depois que a carga de trabalho é integrada e o monitoramento é configurado.

Implementando a observabilidade na detecção e resposta a incidentes da AWS

Como a observabilidade é um processo contínuo que pode não ser concluído em um exercício ou período de tempo, o AWS Incident Detection and Response implementa a observabilidade em duas fases:

- Fase de integração: a observabilidade durante a integração se concentra em detectar quando os resultados comerciais do seu aplicativo estão prejudicados. Para esse fim, a observabilidade durante a fase de integração se concentra na definição das principais métricas de resultados de negócios na camada de aplicativos para notificar interrupções em suas cargas AWS de trabalho. Dessa forma, AWS pode responder prontamente a essas interrupções e fornecer ajuda na recuperação. Para saber mais sobre como usar a interface de linha de comando do cliente do AWS Incident Detection and Response para ajudar a automatizar essas etapas, consulte a CLI do AWS Incident Detection and Response.
- Post-onboarding fase: o AWS Incident Detection and Response oferece vários serviços proativos de observabilidade, incluindo a definição de métricas no nível da infraestrutura, o ajuste de métricas e a configuração de rastreamentos e registros, dependendo do nível de maturidade do cliente. A implementação desses serviços pode durar vários meses e envolver várias equipes. O AWS Incident Detection and Response fornece orientação sobre a configuração da observabilidade e os clientes devem implementar as mudanças necessárias em seu ambiente de carga de trabalho. Para obter ajuda com a implementação prática de recursos de observabilidade, faça uma solicitação aos seus gerentes técnicos de contas (TAMs).

Gerenciamento de incidentes com detecção e resposta a incidentes

O AWS Incident Detection and Response oferece 24 horas por dia, 7 dias por semana, monitoramento proativo e gerenciamento de incidentes fornecidos por uma equipe designada de gerentes de incidentes. O diagrama a seguir descreve o processo padrão de gerenciamento de incidentes quando um alarme de aplicativo aciona um incidente, incluindo geração de alarmes, engajamento do AWS Incident Manager, resolução de incidentes e revisão pós-incidente.

1. Geração de alarmes: os alarmes acionados em suas cargas de trabalho são enviados pela Amazon para o EventBridge AWS Incident Detection and Response. O AWS Incident Detection and Response acessa automaticamente o runbook associado ao seu alarme e notifica um gerente de incidentes. Se ocorrer um incidente crítico em sua carga de trabalho que não seja detectado pelos alarmes monitorados pelo AWS Incident Detection and Response, você poderá criar um caso de suporte para solicitar uma resposta a incidentes. Para obter mais informações sobre como solicitar uma resposta a incidentes, consulteSolicitar uma resposta a um incidente.
2. AWS Engajamento do gerente de incidentes: o gerente de incidentes responde ao alarme e envolve você em uma teleconferência ou conforme especificado no runbook. O gerente de incidentes verifica a integridade do Serviços da AWS para determinar se o alarme está relacionado a problemas Serviços da AWS usados pela carga de trabalho e aconselha sobre o status dos serviços subjacentes. Se necessário, o gerente de incidentes cria um caso em seu nome e contrata os AWS especialistas certos para obter suporte. Como o AWS Incident Detection and Response monitora Serviços da AWS especificamente seus aplicativos, o AWS Incident Detection and Response pode determinar que o incidente está relacionado a um AWS service (Serviço da AWS) problema antes que um AWS service (Serviço da AWS) evento seja declarado. Nesse cenário, o gerente de incidentes aconselha você sobre o status do AWS service (Serviço da AWS), aciona o fluxo de trabalho de gerenciamento de incidentes de AWS service (Serviço da AWS) eventos e acompanha a equipe de serviço sobre a resolução. As informações fornecidas oferecem a oportunidade de implementar seus planos de recuperação ou soluções alternativas com antecedência para mitigar o impacto do evento. AWS service (Serviço da AWS)

   Às vezes, os alarmes são acionados e se recuperam rapidamente. Nesse cenário, o gerente de incidentes envia uma correspondência informando que o alarme foi recuperado, mas não envolve

você. No entanto, se um alarme disparar mais de uma vez em 15 minutos, o gerente de incidentes interage com você de acordo com as instruções do runbook, mesmo que o alarme se recupere.

3. Resolução de incidentes: o gerente de incidentes coordena o incidente entre AWS as equipes necessárias e garante que você permaneça envolvido com os AWS especialistas certos até que o incidente seja mitigado ou resolvido.
4. Análise pós-incidente (se solicitada): após um incidente, o AWS Incident Detection and Response pode realizar uma análise pós-incidente conforme sua solicitação e gerar um relatório pós-incidente. O Relatório Pós-Incidente inclui uma descrição do problema, do impacto, das equipes envolvidas e das soluções alternativas ou ações tomadas para mitigar ou resolver o incidente. O Relatório Pós-Incidente pode conter informações que podem ser usadas para reduzir a probabilidade de recorrência do incidente ou para melhorar o gerenciamento de uma ocorrência futura de um incidente semelhante. O relatório pós-incidente não é uma análise de causa raiz (RCA). Você pode solicitar um RCA além do Relatório Pós-Incidente. Um exemplo de relatório pós-incidente é fornecido na seção a seguir.

> **Important**
>
> O modelo de relatório a seguir é apenas um exemplo.

```
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 Suporte support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and Suporte 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.

Tópicos

Provisionar acesso a AWS Support Center Console para equipes de aplicativos

O AWS Incident Detection and Response se comunica com você por meio de Suporte casos durante o ciclo de vida de um incidente. Para se corresponder com os gerentes de incidentes, suas equipes devem ter acesso ao Suporte Centro.

Para obter mais informações sobre o provisionamento de acesso, consulte Gerenciar o acesso ao Suporte Centro no Guia do Suporte Usuário.

Solicitar uma resposta a um incidente

Se ocorrer um incidente crítico em sua carga de trabalho que não seja detectado por alarmes monitorados pelo AWS Incident Detection and Response, você poderá criar um caso de suporte para solicitar uma resposta a incidentes. Você pode solicitar uma resposta a incidentes para qualquer carga de trabalho inscrita no AWS Incident Detection and Response, incluindo cargas de trabalho em processo de integração, usando a AWS Support Center Console API ou. AWS Support AWS Support App in Slack

O diagrama a seguir ilustra o fluxo de trabalho de ponta a ponta para um AWS cliente que solicita assistência a incidentes da equipe de Detecção e Resposta a Incidentes, detalhando as etapas desde a solicitação inicial até a investigação, mitigação e resolução.

Para solicitar uma resposta a um incidente que está afetando ativamente sua carga de trabalho, crie um Suporte caso. Depois que o caso de suporte é levantado, o AWS Incident Detection and Response envolve com você em uma ponte de conferência com os AWS especialistas necessários para acelerar a recuperação da sua carga de trabalho.

Solicite uma resposta a incidentes usando o AWS Support Center Console

Para solicitar uma resposta a um incidente, conclua as seguintes etapas:

1. Abra o AWS Support Center Consolepara criar um novo caso de suporte.
2. Em Assunto, insira um breve resumo do incidente. Por exemplo, .`AWS Incident Detection and Response - Active Incident - workload_name`
3. Em Descrição, insira os detalhes do incidente. Recomendamos que você inclua os seguintes detalhes em seu caso de suporte:
   - ARN (s) do AWS recurso afetado, nome da carga de trabalho e sua função
   - Descrição do impacto nos negócios
   - (Opcional) Sua URL de ponte de conferência preferida. Se você não fornecer detalhes da ponte, o AWS Incident Detection and Response cria uma ponte de AWS conferência e envia um convite com a URL da ponte.
4. (Opcional) Anexe arquivos que possam ajudar a descrever o incidente, como capturas de tela ou trechos de registros.
5. Configure os seguintes campos de classificação de casos:
   - Tipo de caixa: Técnico
   - Serviço: Detecção e resposta a incidentes
   - Categoria: Incidente ativo
   - Severidade: Business-critical sistema inativo
6. Forneça contexto adicional para ajudar o AWS Incident Detection and Response a engajar AWS especialistas com mais rapidez, como os recursos afetados AWS service (Serviço da AWS), impactados Região da AWS, impacto comercial, horário de início do impacto e recursos afetados.
7. Selecione Enviar.
8. O AWS Incident Detection and Response reconhece seu caso em cinco minutos e envolve você em uma ponte de conferência com os especialistas apropriados AWS .

Solicite uma resposta a incidentes usando o AWS Support solicitações de

Você pode usar a AWS Support API para criar casos de suporte de forma programática. Para obter mais informações, consulte Sobre a AWS Support API no Guia AWS Support do usuário.

Solicite uma resposta a incidentes usando o AWS Support App in Slack

Para usar o AWS Support App in Slack para solicitar uma resposta a incidentes, conclua as seguintes etapas:

1. Abra o canal do Slack AWS Support App in Slack em que você configurou.
2. Digite o comando:

```
/awssupport create
```

3. Insira um assunto para esse incidente. Por exemplo, insira AWS Incident Detection and Response - Active Incident - workload_name.
4. Insira a descrição do problema para esse incidente. Adicione os seguintes detalhes:

   Informações técnicas:

   Serviço (s) afetado (s):

   Recurso (s) afetado (s):

   Região (s) afetada (s):

   Nome da carga de trabalho:

   Informações comerciais:

   Descrição do impacto no negócio:

   [Opcional] Detalhes do Customer Bridge:
5. Escolha Próximo.
6. Em Tipo de problema, escolha Suporte técnico.
7. Em Serviço, escolha Detecção e resposta a incidentes.
8. Em Categoria, escolha Incidente ativo.
9. Em Severidade, escolha Business-critical sistema inativo.

10. Opcionalmente, insira até 10 contatos adicionais no campo Contatos adicionais a serem notificados, separados por vírgulas. Esses contatos adicionais recebem cópias da correspondência por e-mail sobre esse incidente.

11. Escolha Revisar.
12. Uma nova mensagem que só é visível para você aparece no canal do Slack. Revise os detalhes do caso e escolha Criar caso.

13. Seu ID de caso é fornecido em uma nova mensagem do AWS Support App in Slack.
14. A Detecção e Resposta a Incidentes confirma seu caso em 5 minutos e envolve você em uma ponte de conferência com os especialistas apropriados AWS .
15. A correspondência do Incident Detection and Response é atualizada no tópico do caso.

Gerencie casos de suporte de detecção e resposta a incidentes com o AWS Support App in Slack

Com o AWS Support App in Slack, você pode gerenciar seus Suporte casos no Slack, receber notificações sobre novos incidentes iniciados por alarme em sua carga de trabalho de detecção e resposta a incidentes da AWS e criar solicitações de resposta a incidentes.

Para configurar o AWS Support App in Slack, siga as instruções fornecidas no Guia do Suporte usuário.

> **Important**
>
> - Para receber notificações no Slack sobre todos os incidentes iniciados por alarme em sua carga de trabalho, você deve configurá-los AWS Support App in Slack para todas as contas da sua carga de trabalho que estão integradas ao AWS Incident Detection and Response. Support cases são criados na conta na qual o alarme de carga de trabalho foi originado.
> - Vários casos de suporte de alta gravidade podem ser abertos em seu nome durante um incidente para envolver os Suporte solucionadores. Você recebe notificações no Slack para todos os casos de suporte abertos durante um incidente que correspondam à sua configuração de notificação no canal do Slack.

- As notificações que você recebe por meio do AWS Support App in Slack não substituem os contatos iniciais e de escalonamento de sua carga de trabalho que são contratados por e-mail ou telefonema pela Detecção e Resposta a Incidentes durante um AWS incidente.

Tópicos

Notificações de incidentes iniciadas por alarme no Slack

Depois de configurar o AWS Support App in Slack em seu canal do Slack, você recebe notificações sobre incidentes iniciados por alarme em sua carga de trabalho monitorada do AWS Incident Detection and Response.

O exemplo a seguir mostra como as notificações de incidentes iniciados por alarme aparecem no Slack.

Exemplo de notificação

Quando seu incidente iniciado por alarme é reconhecido pelo AWS Incident Detection and Response, uma notificação semelhante à seguinte é gerada no Slack:

Para ver a correspondência completa adicionada pelo AWS Incident Detection and Response, escolha Ver detalhes.

Outras atualizações do AWS Incident Detection and Response aparecem no tópico do caso.

Escolha Ver detalhes para ver a correspondência completa adicionada pelo AWS Incident Detection and Response.

Crie uma solicitação de resposta a incidentes no Slack

Para obter instruções sobre como criar uma Solicitação de Resposta a Incidentes por meio do AWS Support App in Slack, consulteSolicitar uma resposta a um incidente.

Relatórios em detecção e resposta a incidentes

O AWS Incident Detection and Response fornece dados operacionais e de desempenho para ajudar você a entender como o serviço está configurado, o histórico de seus incidentes e o desempenho do serviço de Detecção e Resposta a Incidentes. Esta página aborda os tipos de dados disponíveis, incluindo dados de configuração, dados de incidentes e dados de desempenho.

Dados de configuração

- Todas as contas integradas
- Nomes de todos os aplicativos
- Os alarmes, runbooks e perfis de suporte associados a cada aplicativo

Dados do incidente

- As datas, o número e a duração dos incidentes para cada aplicativo
- As datas, o número e a duração dos incidentes associados a um alarme específico
- Relatório pós-incidente

Dados de desempenho

- Desempenho do objetivo de nível de serviço (SLO)

Entre em contato com seu gerente técnico de contas para obter os dados operacionais e de desempenho que você possa precisar.

Segurança e resiliência de detecção e resposta a incidentes

O Modelo de Responsabilidade AWS Compartilhada se aplica à proteção de dados em Suporte. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa.

Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados.

Para obter informações sobre proteção de dados na Europa, consulte a postagem do blog sobre o Modelo de Responsabilidade AWS Compartilhada e o GDPR no Blog AWS de Segurança.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da AWS conta e configure contas de usuário individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use certificados Secure Sockets Layer/Transport Layer Security (SSL/TLS (soquetes) para se comunicar com AWS os recursos. Recomendamos usar o TLS 1.2 ou posterior. Para obter informações, consulte O que é um certificado SSL/TLS? .
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para ter mais informações, consulte AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3. Para obter informações sobre o Amazon Macie, consulte Amazon Macie.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com Suporte ou Serviços da AWS usa o console, a API, a AWS CLI ou o. AWS SDKs Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Acesso ao AWS Incident Detection and Response às suas contas

AWS Identity and Access Management (IAM) é um serviço web que ajuda você a controlar com segurança o acesso aos AWS recursos. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos.

AWS Incident Detection and Response e seus dados de alarme

Por padrão, o Incident Detection and Response recebe o nome de recurso da Amazon (ARN) e o estado de cada CloudWatch alarme em sua conta e, em seguida, inicia o processo de detecção e resposta a incidentes quando o alarme integrado muda para o estado ALARM. Se você quiser personalizar as informações que a detecção e a resposta a incidentes recebem sobre os alarmes de sua conta, entre em contato com seu gerente técnico de contas.

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação desde a última versão do guia do IDR.

Alteração	Descrição	Data
Tópico padrão esclarecido do Amazon SNS para integração de APM	Esclareceu que os clientes devem criar um tópico padrão do Amazon Simple Notificat ion Service (não FIFO) ao integrar alarmes de APM de terceiros com o AWS Incident Detection and Response. Para obter mais informações, consulte Alarmes de ingestão de APMs com integração direta com o Amazon SNS.	26 de maio de 2026
GameDay agora é opcional, questionário de integraçã o simplificado e desenvolv imento atualizado do runbook	Teste de alarme atualizado (GameDay) para ser opcional depois Go-Live, com duas opções de teste: teste de alarme programad o GameDay ou offline. Simplificou a integraçã o da carga de trabalho e os questionários de ingestão de alarmes. Desenvolvimento atualizado do runbook para remover referênci as a AWS Systems Manager documentos. Para obter mais informações, consulte Teste cargas de trabalho integradas em Detecção e Resposta a Incidentes, Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes (caminho de exceção) e Desenvolva runbooks e planos de resposta para responder a um incidente em Detecção e Resposta a Incidente s.	26 de maio de 2026

Alteração	Descrição	Data
Procedimento de solicitação de resposta a incidentes atualizado	Atualizou o procedimento Solicitar uma resposta a um incidente para corresponder à AWS Support Center Console interface de usuário atual, adicionou orientação de URL de ponte e removeu capturas de tela desatualizadas. Para obter mais informações, consulte Solicite uma resposta a incidentes usando o AWS Support Center Console.	12 de maio de 2026
Integração atualizada para abordar CLI-first	Atualizou o capítulo Get Started para promover a interface de linha de comando do cliente de detecção e resposta a incidentes da AWS como o principal método de integração e descontinuou o questionário de integração da carga de trabalho e o questionário de ingestão de alarmes como o caminho de integração padrão. Os questionários permanecem disponíveis somente como uma opção excepcional para clientes que não podem usar a CLI do IDR. Para obter mais informações, consulte Integre cargas de trabalho para detecção e resposta a incidentes e Ingestão de alarmes.	12 de maio de 2026

Alteração	Descrição	Data
Links de questionário em japonês adicionados	Foram adicionados links de Japanese-language download para o questionário de integração da carga de trabalho e o questionário de ingestão de alarmes. Para obter mais informações, consulte Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes (caminho de exceção).	20 de abril de 2026
Referências de arquitetura atualizadas	As referências aos diagramas de arquitetura foram removidas e substituídas por detalhes da arquitetura. Para obter mais informações, consulte Arquitetura de detecção e resposta a incidentes e Sobre cargas de trabalho em Detecção e Resposta a Incidentes.	31 de março de 2026
Teste atualizado: cargas de trabalho integradas em Detecção e Resposta a Incidentes	Foram adicionadas informações sobre como desativar as ações CloudWatch de alarme antes de alterar o estado do alarme durante o teste. Para obter mais informações, consulte Teste cargas de trabalho integradas em Detecção e Resposta a Incidentes.	2 de março de 2026
Gerenciamento de incidentes atualizado com detecção e resposta a incidentes	Foram adicionadas informações sobre o comportamento repetido de alarmes e o engajamento do gerente de incidentes. Para obter mais informações, consulte Gerenciamento de incidentes com detecção e resposta a incidentes.	2 de março de 2026

Alteração	Descrição	Data
Etapas atualizadas na seção Usar uma função matemátic a métrica para suprimir um CloudWatch alarme	Etapas atualizadas na seção Usar uma função matemática métrica para suprimir um CloudWatch alarme. Para obter mais informações, consulte Suprimir alarmes na fonte de alarme.	3 de fevereiro de 2026
Adicionado coreano como idioma suportado	Foi adicionado coreano como idioma suportado . Para obter mais informações, consulte Disponibilidade regional para detecção e resposta a incidentes.	22 de janeiro de 2026
Adicionado o mandarim como idioma suportado	Foi adicionado o mandarim como idioma suportado. Para obter mais informações, consulte Disponibilidade regional para detecção e resposta a incidentes.	13 de janeiro de 2026
Foi adicionada uma nova seção: AWS Incident Detection and Response Customer Command Line Interface	Foi adicionada a seção IDR CLI e atualizou o capítulo Get Started para incluir informaçõ es sobre a interface de linha de comando do cliente do AWS Incident Detection and Response. Para obter mais informações, consulte CLI for AWS Incident Detection and Response.	8 de dezembro de 2025

Alteração	Descrição	Data
Várias seções atualizadas: questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e resposta a incidentes e Introdução à detecção e resposta a incidentes	O processo de tratamento de AWS service (Serviço da AWS) eventos não faz mais parte do AWS Incident Detection and Response. As seções deste guia do usuário foram atualizadas para remover referências a esse processo. Você continuará recebendo notificações de eventos de serviço por meio do AWS Service Health Dashboard. Os clientes do AWS Incident Detection and Response podem usar uma solicitação de resposta a incidentes para receber ajuda durante eventos de serviço, conforme necessário. Para obter mais informações, consulte Solicitar uma resposta a um incidente.	14 de outubro de 2025
Seção excluída: Gerenciamento de incidentes para eventos de serviço	O processo de tratamento de AWS service (Serviço da AWS) eventos não faz mais parte do AWS Incident Detection and Response. Esta seção do guia do usuário foi removida para refletir essa alteração. Você continuará recebendo notificações de eventos de serviço por meio do AWS Service Health Dashboard. Os clientes do AWS Incident Detection and Response podem usar uma solicitação de resposta a incidentes para receber ajuda durante eventos de serviço, conforme necessário. Para obter mais informações, consulte Solicitar uma resposta a um incidente.	14 de outubro de 2025
Seção atualizada: Disponibilidade da região para detecção e resposta a incidentes	O AWS Incident Detection and Response agora está disponível em AWS GovCloud (US-East) e AWS GovCloud (US-West). Para obter mais informações, consulte Disponibilidade regional para detecção e resposta a incidentes.	05 de outubro de 2025

Alteração	Descrição	Data
Seção atualizada: Questionários de integração da carga de trabalho e ingestão de alarmes em Detecção e Resposta a Incidentes	Exemplo de endereço de e-mail atualizado para a tabela de matriz de alarmes.	26 de agosto de 2025
Seção atualizada: Inscrever uma carga de trabalho no AWS Incident Detection and Response	Foi removida a referência ao campo Data de início da assinatura na seção Descrição da janela Criar caso. Seção atualizada: Inscrever uma carga de trabalho no AWS Incident Detection and Response	4 de agosto de 2025
Nova função: impedir que os alarmes ativem a Detecção e a Resposta a Incidentes	Foram adicionadas novas seções às cargas de trabalho gerenciadas que fornecem informaçõ es sobre como suprimir alarmes temporari amente ou de acordo com um cronograma Nova seção: Impeça que os alarmes ativem a Detecção e a Resposta a Incidentes	9 de abril de 2025
Instruções atualizadas para solicitar uma resposta a incidentes usando o AWS Support Center Console	Foram adicionados detalhes sobre quais informações inserir no campo Descrição do problema. Seção atualizada: Solicitar uma resposta a um incidente	6 de fevereiro de 2025
Regiões da AWS Adicionado adicional	Outros Regiões da AWS foram adicionados à seção Detecção de incidentes e disponibilidade de respostas. Seção atualizada: Disponibilidade regional para detecção e resposta a incidentes	1.º de novembro de 2024

Alteração	Descrição	Data
Atualizações para gerenciar casos de suporte de detecção e resposta a incidentes com a AWS Support App in Slack página	Moveu a página para Gerenciamento de incidentes, revisou o texto e substituiu as capturas de tela. Seção atualizada: Gerencie casos de suporte de detecção e resposta a incidentes com o AWS Support App in Slack	10 de outubro de 2024
Adicionou uma nova página AWS Support App in Slack Gerenciamento de incidente s atualizado com o AWS Incident Detection and Response	Adicionou uma nova página para AWS Support App in Slack Gerenciamento de incidentes atualizado com o AWS Incident Detection and Response para adicionar uma nova seção, “Solicitar uma resposta a incidentes usando o AWS Support App in Slack”.	10 de setembro de 2024
Assinatura de conta atualizada	A seção de assinatura da conta foi atualizada para incluir detalhes sobre onde abrir um caso de suporte ao solicitar a assinatura de uma conta. Seção atualizada: Inscrever uma carga de trabalho no AWS Incident Detection and Response	12 de junho de 2024
Foi adicionada uma nova seção: Excluir uma carga de trabalho	Foi adicionada a seção Descarregar uma carga de trabalho em Introdução para incluir informações sobre a desativação de cargas de trabalho Para obter mais informações, consulte Remova uma carga de trabalho da Detecção e Resposta a Incidentes.	28 de março de 2024

Alteração	Descrição	Data
Assinatura de conta atualizada	A seção de assinatura da conta foi atualizada para incluir informações sobre a transferência de cargas de trabalho Para obter mais informações, consulte Inscrever uma carga de trabalho no AWS Incident Detection and Response	28 de março de 2024
Teste atualizado	A seção de testes foi atualizada para incluir informações sobre os testes do dia de jogo como a última etapa do processo de integraçã o. Seção atualizada: Teste cargas de trabalho integradas em Detecção e Resposta a Incidentes	29 de fevereiro de 2024
Atualizado O que é AWS Incident Detection and Response	A seção O que é AWS Incident Detection and Response foi atualizada. Seção atualizada: O que é o AWS Incident Detection and Response?	19 de fevereiro de 2024
Seção de questionário atualizada	Atualizou o questionário de integração da carga de trabalho e adicionou o questionário de ingestão de alarmes. A seção foi renomeada de Questionário de integração para Questioná rios de integração de carga de trabalho e ingestão de alarmes.	2 de fevereiro de 2024

Alteração	Descrição	Data
Eventos AWS de serviço atualizados e informações de integração	Várias seções foram atualizadas com novas informações para integração. Seções atualizadas: • Integre cargas de trabalho para detecção e resposta a incidentes • Inscreva uma carga de trabalho no AWS Incident Detection and Response Novas seções • Provisionar acesso a AWS Support Center Console para equipes de aplicativos	31 de janeiro de 2024
Foi adicionada uma seção de informações relacionadas	Foi adicionada uma seção de informações relacionadas no provisionamento do Access. Seção atualizada: Provisionar acesso para ingestão de alarmes à detecção e resposta a incidentes	17 de janeiro de 2024
Etapas de exemplo atualizad as	Atualizou o procedimento para as etapas 2,3 e 4 em Exemplo: Integrando notificações do Datadog e do Splunk. Seção atualizada: Exemplo: integração de notificações do Datadog e do Splunk	21 de dezembro de 2023
Gráfico e texto de introdução atualizados	Gráfico atualizado nos alarmes do Ingest de APMs que têm integração direta com a Amazon. EventBridge Seção atualizada: Desenvolva runbooks e planos de resposta para responder a um incidente em Detecção e Resposta a Incidentes	21 de dezembro de 2023

Alteração	Descrição	Data
Modelo de runbook atualizado	Atualizou o modelo de runbook em Developin g runbooks for AWS Incident Detection and Response. Seção atualizada: Desenvolva runbooks e planos de resposta para responder a um incidente em Detecção e Resposta a Incidentes	4 de dezembro de 2023
Configurações de alarme atualizadas	Configurações de alarme atualizadas com informações detalhadas sobre a configuração do CloudWatch alarme. Nova seção: Crie CloudWatch alarmes que atendam às necessidades de sua empresa em Detecção e Resposta a Incidentes Nova seção: Crie CloudWatch alarmes em Detecção e Resposta a Incidentes com modelos CloudFormation Nova seção: Exemplos de casos de uso para CloudWatch alarmes em Detecção e Resposta a Incidentes	28 de setembro de 2023
Introdução atualizada	Introdução atualizada com informações sobre solicitações de alteração da carga de trabalho. Nova seção: Solicite alterações em uma carga de trabalho integrada na Detecção e Resposta a Incidentes Seção atualizada: Inscrever uma carga de trabalho no AWS Incident Detection and Response	05 de setembro de 2023
Nova seção em Introdução	Foram adicionados alertas de ingestão ao AWS Incident Detection and Response.	30 de junho de 2023

Alteração	Descrição	Data
Documento original	AWS Incident Detection and Response foi publicado pela primeira vez	15 de março de 2023

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.