AWSConceitos e procedimentos de detecção e resposta a incidentes

AWSGuia do usuário de detecção e resposta a incidentes

Versão July 3, 2024

AWSGuia do usuário de detecção e resposta a incidentes: AWSConceitos e procedimentos de detecção e resposta a incidentes

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. Uma equipe de engenheiros de gerenciamento de incidentes (IMEs) monitora suas cargas de trabalho integradas 24 horas por dia, 7 dias por semana, e envolve você em uma ponte de chamadas dentro de 5 minutos após um alarme crítico.

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 IMEs monitoram suas cargas de trabalho integradas 24 horas por dia, 7 dias por semana, para detectar incidentes críticos. Os IMEs respondem em até 5 minutos após o disparo de um alarme ou em resposta a um caso de Support crítico para os negócios que você encaminha para a Detecção e Resposta a Incidentes.
- Resolução mais rápida: os IMEs usam runbooks predefinidos e personalizados desenvolvidos para que suas cargas de trabalho respondam em 5 minutos, criem um caso de Support em seu nome e gerenciem 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.
- Gerenciamento de incidentes para AWS eventos: como entendemos o contexto de sua carga de trabalho crítica (por exemplo, contas, serviços e instâncias), podemos detectar e notificá-lo proativamente sobre um possível impacto em sua carga de trabalho durante um AWS evento de serviço. Se solicitado, os IMEs interagem com você durante os eventos do AWS serviço e fornecem atualizações sobre os eventos. Embora a Detecção e Resposta a Incidentes não possam priorizar sua recuperação durante um evento de serviço, a Detecção e Resposta a Incidentes fornece orientação de Support para ajudá-lo a implementar seu plano de mitigação.
- 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.

Termos do produto de detecção e resposta a incidentes

- O AWS Incident Detection and Response está disponível para contas diretas e revendidas por parceiros do Enterprise Support.
- 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.

Disponibilidade de detecção e resposta a incidentes

Atualmente, o AWS Incident Detection and Response está disponível no idioma inglês para contas do Enterprise Support hospedadas em qualquer um dos seguintes Regiões da AWS:

Nome	Região da AWS
us-east-1	Leste dos EUA (Virgínia)
us-east-2	Leste dos EUA (Ohio)

Nome	Região da AWS
us-west-1	Oeste dos EUA (N. da Califórnia)
us-west-2	Oeste dos EUA (Oregon)
ca-central-1	Canadá (Central)
sa-east-1	América do Sul (São Paulo)
eu-central-1	Europa (Frankfurt)
eu-west-1	Europa (Irlanda)
eu-west-2	Europa (Londres)
eu-west-3	Europa (Paris)
eu-north-1	Europa (Estocolmo)
ap-south-1	Ásia-Pacífico (Mumbai)
ap-northeast-1	Ásia-Pacífico (Tóquio)
ap-northeast-2	Ásia-Pacífico (Seul)
ap-southeast-1	Ásia-Pacífico (Singapura)
ap-southeast-2	Ásia-Pacífico (Sydney)

Detecção e resposta a incidentes da AWS (RACI)

A tabela a seguir mostra os responsáveis, responsáveis, consultados e informados pela AWS Incident Detection and Response ou o RACI.

Atividades	Cliente	Detecção e resposta a incidentes
Coleta de dados		
Introdução ao cliente e à carga de trabalho	C	R
Arquitetura	R	A
Operações	R	A
Determine CloudWatch os alarmes a serem configurados	R	A
Defina o plano de resposta a incidentes	R	A
Preenchendo o questionário de integração	R	A
Análise da prontidão operacional		
Conduza uma análise bem arquitetada (WAR) da carga de trabalho	C	R
Valide a resposta a incidentes	C	R
Validar matriz de alarmes	C	R
Identifique AWS os principais serviços que estão sendo usados pela carga de trabalho	A	R
Configuração da conta		
Crie a função do IAM na conta do cliente	R	I
Instalar a EventBridge regra gerenciada usando a função criada	I	R
CloudWatch Alarmes de teste	R	A

Atividades	Cliente	Detecção e resposta a incidentes
Verifique se os alarmes do cliente envolvem a detecção e a resposta a incidentes	I	R
Atualizar alarmes	R	C
Atualizar runbooks	C	R
Gerenciamento de incidentes		
Notifique proativamente os incidentes detectados pela Detecção e Resposta a Incidentes	I	R
Forneça resposta a incidentes	I	R
Forneça resolução de incidentes e restauração da infraestrutura	R	C
Análise pós-incidente		
Solicitar análise pós-incidente	R	I
Forneça uma análise pós-incidente	I	R

Arquitetura de detecção e resposta a incidentes da AWS

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 diagramas de arquitetura de carga de trabalho, detalhes de alarmes e seus respectivos runbooks de gerenciamento de incidentes em AWS Systems Manager documentos (para obter detalhes, consulte Documentos).AWS Systems Manager 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.

Comece a usar a Detecção e Resposta a AWS Incidentes

Você pode selecionar cargas de trabalho específicas para monitoramento e gerenciamento de incidentes críticos usando a Detecção e Resposta a AWS Incidentes. Uma carga de trabalho é uma coleção de recursos e códigos que trabalham juntos para oferecer 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 AWS conta ou múltipla AWS contas.

Por exemplo, você pode ter um aplicativo monolítico hospedado em uma única conta (por exemplo, Employee Performance App na Fig.1). Ou você pode ter um aplicativo (por exemplo, o Storefront Webapp na Fig. 1) 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 na Figura 1.

> **Note**
>
> Para fazer alterações em seus runbooks, nas informações da carga de trabalho ou nos alarmes monitorados na Detecção e Resposta a AWS Incidentes, crie um. Solicitar alterações em uma carga de trabalho integrada

Integração

AWS trabalha com você para integrar sua carga de trabalho e alarmes à Detecção e Resposta a AWS Incidentes. Você fornece informações importantes para AWS no Questionários de integração da carga de trabalho e ingestão de alarmes É uma prática recomendada que você também registre suas cargas de trabalho. AppRegistry Para obter mais informações, consulte o Guia AppRegistry do usuário.

O diagrama a seguir mostra o fluxo de integração da carga de trabalho e ingestão de alarmes na Detecção e Resposta a Incidentes:

Integração da carga de trabalho

Durante a integração da carga de trabalho, AWS trabalha com você para entender sua carga de trabalho e como apoiá-lo durante incidentes e AWS Eventos de serviço. Você fornece informações importantes sobre sua carga de trabalho que ajudam na mitigação do impacto.

Principais saídas:

- Informações gerais sobre a carga de trabalho
- Detalhes da arquitetura, incluindo diagramas
- Informações sobre o Runbook
- Incidentes iniciados pelo cliente
- AWS Eventos de serviço

Ingestão de alarmes

AWS trabalha com você para integrar seus alarmes. AWSO Incident Detection and Response pode ingerir alarmes da Amazon CloudWatch e de ferramentas de monitoramento de desempenho de aplicativos (APM) de terceiros por meio da Amazon. EventBridge Os alarmes de integração permitem a detecção proativa de incidentes e o engajamento automatizado. Para obter mais informações, consulte Alarmes de ingestão APMs que tenham integração direta com a Amazon. EventBridge

Principais saídas:

- Matriz de alarme

A tabela a seguir lista as etapas necessárias para integrar uma carga de trabalho à Detecção e Resposta a AWS Incidentes. Esta tabela mostra exemplos de durações de cada tarefa. As datas reais de cada tarefa são definidas com base na disponibilidade da sua equipe e do cronograma.

Assinatura da conta

Para inscrever uma carga de trabalho no 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 integrar 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 de pagador.
- Para integrar uma carga de trabalho que abrange várias AWS contas, crie o caso de suporte a partir da sua conta de pagador. No corpo do caso de suporte, liste todas as contas IDs a bordo.

> **Important**
>
> Se você criar um caso de suporte para inscrever uma carga de trabalho no Incident Detection and Response a partir da conta incorreta, poderá enfrentar atrasos e solicitações de informações adicionais antes que suas cargas de trabalho possam ser inscritas.

Para assinar uma carga de trabalho

1. Vá para o AWS SupportCentralize e, em seguida, selecione Criar caso, conforme mostrado no exemplo a seguir. Você só pode assinar cargas de trabalho de contas inscritas no Enterprise Support.

2. Preencha o formulário do caso de suporte:
   - Selecione Suporte técnico.
   - Em Serviço, escolha Detecção e resposta a incidentes.
   - Em Categoria, escolha Integrar nova carga de trabalho.
   - Em Severidade, escolha Orientação geral.
3. Insira um assunto para essa alteração. Por exemplo:

   [A bordo] Detecção e resposta a AWS incidentes - *workload_name*
4. Insira uma Descrição para essa alteração. Por exemplo, digite “Esta solicitação é para integrar uma carga de trabalho à Detecção e Resposta a AWS Incidentes”. 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. Essas são as contas que você deseja integrar à Detecção e Resposta a AWS Incidentes.
   - Data de início da assinatura: a data em que você deseja iniciar a assinatura de Detecção e Resposta a AWS Incidentes.

5. Na seção Contatos adicionais - opcional, insira qualquer e-mail IDs que você queira receber correspondência sobre essa solicitação.

   A seguir está um exemplo da seção Contatos adicionais - opcional:

   > **Important**
   >
   > A não adição de e-mail IDs na seção Contatos adicionais - opcional pode atrasar o processo de integração de Detecção e Resposta a AWS Incidentes.

6. Selecione Enviar.

   Depois de enviar a solicitação, você pode adicionar outros e-mails da sua organização. Para adicionar e-mails, responda ao caso e adicione o e-mail IDs na seção Contatos adicionais - opcional.

   A seguir está um exemplo da seção Contatos adicionais - opcional:

Depois de criar um caso de suporte para a solicitação de assinatura, mantenha os dois documentos a seguir prontos para continuar com o processo de integração da carga de trabalho:

- AWS diagrama da arquitetura da carga de trabalho.
- Questionários de integração da carga de trabalho e ingestão de alarmes: preencha todas as informações do questionário relacionadas à carga de trabalho que você está integrando. Se você tiver várias cargas de trabalho a serem integradas, crie um novo questionário de integração para cada carga de trabalho. Se você tiver dúvidas sobre como preencher o questionário de integração, entre em contato com seu gerente técnico de contas ()TAM.

> **Note**
>
> NOTAnexe esses dois documentos à caixa usando a opção Anexar arquivos. AWSA equipe de detecção e resposta a incidentes responderá ao caso com um link do Amazon Simple Storage Service Uploader para você fazer o upload dos documentos.

Para obter informações sobre como criar um caso com Detecção e Resposta a AWS Incidentes para solicitar alterações em uma carga de trabalho integrada existente, consulte. Solicitar alterações em uma carga de trabalho integrada Para obter informações sobre como desativar uma carga de trabalho, consulte. Desembarcar de uma carga de trabalho

Descoberta da carga de trabalho

AWS trabalha com você para entender o máximo possível de contexto sobre sua carga de trabalho. AWSA Detecção e Resposta a Incidentes usam essas informações para criar runbooks para apoiá-lo durante incidentes e AWS Eventos de serviço. As informações necessárias são capturadas noQuestionários de integração da carga de trabalho e ingestão de alarmes. É uma prática recomendada registrar suas cargas de trabalho. AppRegistry Para obter mais informações, consulte o Guia AppRegistry do usuário.

Principais saídas:

- Informações da carga de trabalho, como descrição da carga de trabalho, diagramas de arquitetura, detalhes de contato e escalonamento.
- Detalhes de como a carga de trabalho é empregada AWS serviços em cada AWS Região.
- Informações específicas sobre como AWS apoia você durante um evento de serviço.
- Alarmes usados por sua equipe que detectam o impacto crítico da carga de trabalho.

Configuração de alarme

AWS trabalha com você para definir métricas e alarmes para fornecer visibilidade do desempenho de seus aplicativos e de seus aplicativos subjacentes AWS infraestrutura. Solicitamos que os alarmes sigam os seguintes critérios ao definir e configurar limites:

- Os alarmes só entram no estado “Alarme” quando há um impacto crítico na carga de trabalho monitorada (perda de receita ou degradação da experiência do cliente que reduz significativamente o desempenho) que requer atenção imediata do operador.
- Os alarmes também devem envolver seus resolvedores especificados para a carga de trabalho ao mesmo tempo ou antes de engajar a equipe de gerenciamento de incidentes. Os engenheiros de gerenciamento de incidentes devem colaborar com seus solucionadores específicos no processo de mitigação, não servir como respondedores de primeira linha e depois encaminhar até você.

- Os limites de alarme devem ser definidos com um limite e uma duração apropriados para que, sempre que um alarme disparar, uma investigação ocorra. Se um alarme estiver oscilando entre o estado “Alarme” e “OK”, um impacto suficiente está ocorrendo para garantir a resposta e a atenção do operador.

Tipos de alarmes:

- Alarmes que retratam o nível de impacto nos negócios e transmitem informações relevantes para uma simples detecção de falhas.
- CloudWatch Canários da Amazônia. Para obter mais informações, consulte Canaries and X-Ray tracing e X-Ray.
- Alarme agregado (monitoramento de dependências)

Exemplo de alarme, todos usando o sistema CloudWatch de monitoramento

Nome da métrica// Limite de alarme	ID do alarme ARN ou do recurso	Se esse alarme disparar	Se contratado, solicite um Premium Support Case para esses serviços
APIerros/ Nº de erros >= 10 para 10 pontos de dados	arn:aws:cloudwatch:us-west- 2:000000000000:alarm:E2 - Erros MPmimLambda	Redução de tíquetes para a equipe de administrador do banco	Lambda, Gateway API

Nome da métrica// Limite de alarme	ID do alarme ARN ou do recurso	Se esse alarme disparar	Se contratado, solicite um Premium Support Case para esses serviços
		de dados (DBA)	
ServiceUnavailable (Código de status Http 503) Nº de erros >=3 para 10 pontos de dados (clientes diferentes) em uma janela de 5 minutos	arn: aws: cloudwatch: us-west-2: xxxxx: alarme: código de erro http 503	Tíquete reduzido para a equipe de serviço	Lambda, Gateway API
ThrottlingException (Código de status Http 400) Nº de erros >=3 para 10 pontos de dados (clientes diferentes) em uma janela de 5 minutos	arn: aws: cloudwatch: us-west-2: xxxxx: alarme: código de erro http 400	Tíquete reduzido para a equipe de serviço	EC2, Amazon Aurora

Para obter mais detalhes, consulte Monitoramento e observabilidade do AWS Incident Detection and Response.

Principais saídas:

- Definição e configuração de alarmes em suas cargas de trabalho.
- Preenchimento dos detalhes do alarme no questionário de integração.

Crie CloudWatch alarmes que atendam às necessidades de sua empresa em Detecção e Resposta a Incidentes

Quando você cria CloudWatch alarmes da Amazon, há várias etapas que você pode seguir para garantir que seus alarmes atendam melhor às necessidades da sua empresa.

Revise seus CloudWatch alarmes propostos

Analise os alarmes propostos para garantir que eles só entrem no estado “Alarme” quando houver um impacto crítico na carga de trabalho monitorada (perda de receita ou degradação da experiência do cliente, o que reduz significativamente o desempenho). Por exemplo, você considera esse alarme crítico o suficiente para reagir imediatamente se ele entrar no estado “Alarme”?

A seguir estão sugestões de métricas que podem representar um impacto crítico nos negócios, como afetar a experiência dos usuários finais com um aplicativo:

- CloudFront: Para obter mais informações, consulte Visualização CloudFront e métricas da função de borda.
- Balanceadores de carga de aplicativos: é uma prática recomendada criar os seguintes alarmes para balanceadores de carga de aplicativos, se possível:
  - HTTPCode_ ELB _5xx_Contagem
  - HTTPCode_TARGET_5xx_count

  Os alarmes anteriores permitem monitorar as respostas de alvos que estão por trás do Application Load Balancer ou por trás de outros recursos. Isso facilita a identificação da origem dos erros 5XX. Para obter mais informações, consulte CloudWatch as métricas do seu Application Load Balancer.
- Amazon API Gateway: Se você usa WebSocket API no Elastic Beanstalk, considere usar as seguintes métricas:
  - Taxas de erro de integração (filtradas para erros 5XX)
  - Latência de integração
  - Erros de execução

  Para obter mais informações, consulte Monitoramento WebSocket API da execução com CloudWatch métricas.

- Amazon Route 53: monitore a EndPointUnhealthyENICountmétrica. Essa métrica é o número de interfaces de rede elásticas no status de recuperação automática. Esse status indica tentativas do resolvedor de recuperar uma ou mais das interfaces de rede da Amazon Virtual Private Cloud associadas ao endpoint (especificado por EndpointId). No processo de recuperação, o endpoint funciona com capacidade limitada. O endpoint não pode processar DNS consultas até que seja totalmente recuperado. Para obter mais informações, consulte Monitoramento dos endpoints do Route 53 Resolver com a Amazon CloudWatch.

Valide suas configurações de alarme

Depois de confirmar que os alarmes propostos atendem às suas necessidades comerciais, valide a configuração e o histórico dos alarmes:

- Valide o limite da métrica para entrar no estado de “Alarme” em relação à tendência gráfica da métrica.
- Valide o período usado para pontos de dados de pesquisa. A pesquisa de pontos de dados em 60 segundos ajuda na detecção precoce de incidentes.
- Valide a DatapointToAlarmconfiguração. Na maioria dos casos, é uma prática recomendada definir isso como 3 de 3 ou 5 de 5. Em um incidente, o alarme é acionado após 3 minutos quando definido como [métrica de 60 segundos com 3 de 3 DatapointToAlarm] ou 5 minutos quando definido como [métrica de 60 segundos com 5 de 5 DatapointToAlarm]. Use essa combinação para eliminar alarmes ruidosos.

> **Note**
>
> As recomendações anteriores podem variar dependendo de como você usa um serviço. Cada AWS serviço opera de forma diferente dentro de uma carga de trabalho. Além disso, o mesmo serviço pode operar de forma diferente quando usado em vários lugares. Você deve ter certeza de que entendeu como sua carga de trabalho utiliza os recursos que alimentam o alarme, bem como os efeitos a montante e a jusante.

Valide como seus alarmes lidam com dados perdidos

Algumas fontes métricas não enviam dados CloudWatch em intervalos regulares. Para essas métricas, é uma prática recomendada tratar os dados perdidos como notBreaching. Para obter mais

informações, consulte Configurando como CloudWatch os alarmes tratam dados perdidos e Como evitar transições prematuras para o estado de alarme.

Por exemplo, se uma métrica monitora uma taxa de erro e não há erros, a métrica não relata pontos de dados (nulos). Se você configurar o alarme para tratar os dados ausentes como ausentes, um único ponto de dados de violação seguido por dois pontos de dados sem dados (nulos) fará com que a métrica entre no estado “Alarme” (para 3 dos 3 pontos de dados). Isso ocorre porque a configuração de dados ausentes avalia o último ponto de dados conhecido no período de avaliação.

Nos casos em que as métricas monitoram uma taxa de erro, na ausência de degradação do serviço, você pode presumir que nenhum dado é bom. É uma prática recomendada tratar os dados ausentes de notBreachingforma que os dados ausentes sejam tratados como “OK” e a métrica não entre no estado “Alarme” em um único ponto de dados.

Revise o histórico de cada alarme

Se o histórico de um alarme mostrar que ele entra frequentemente no estado “Alarme” e depois se recupera rapidamente, o alarme pode se tornar um problema para você. Certifique-se de ajustar o alarme para evitar ruídos ou alarmes falsos.

Valide métricas para recursos subjacentes

Certifique-se de que suas métricas analisem recursos subjacentes válidos e usem as estatísticas corretas. Se um alarme estiver configurado para revisar nomes de recursos inválidos, talvez o alarme não consiga rastrear os dados subjacentes. Isso pode fazer com que o alarme entre no estado “Alarme”.

Crie alarmes compostos

Se você fornecer às operações de Detecção e Resposta a Incidentes um grande número de alarmes para integração, talvez seja necessário criar alarmes compostos. Os alarmes compostos reduzem o número total de alarmes que precisam ser integrados.

Use AWS CloudFormation modelos para criar CloudWatch alarmes em Detecção e Resposta a Incidentes

Para acelerar a integração da Detecção e Resposta a AWS Incidentes e reduzir o esforço necessário para criar alarmes, AWS fornece a você AWS CloudFormation modelos. Esses modelos incluem configurações de alarme otimizadas para serviços comumente integrados, como Application Load Balancer, Network Load Balancer e Amazon. CloudFront

Crie CloudWatch alarmes com modelos CloudFormation

1. Faça o download de um modelo usando os links fornecidos:

NameSpac	Metrics	ComparisonOperator (Limite)	Período	DatapointsToAlarm	TreatMissingData	Estatística	Link do modelo
Aplicação: Elastic Load Balancer	(m1+m2)/(m1+m2+mm4) *100 m1=_target_2xx_count m2=_target_3xx_count m3=_target_4xx_count m4=_target_5xx_count HTTPCode HTTPCode HTTPCode HTTPCode	LessThanThreshold(95)	60	3 de 3	desaparecido	Soma	Modelo
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3 de 3	notBreaching	Média	Modelo
Aplicação: Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 de 3	notBreaching	Máximo	Modelo

NameSpac	Metrics	Compariso nOperator (Limite)	Período	Datapoint sToAlarm	TreatMiss ingData	Estatísti ca	Link do modelo
Elastic Load Balancer de rede	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3 de 3	notBreach ing	Máximo	Modelo

2. Revise o JSON arquivo baixado para garantir que ele atenda aos processos operacionais e de segurança da sua organização.
3. Crie uma CloudFormation pilha:

> **Note**
>
> As etapas a seguir usam o processo padrão de criação de CloudFormation pilhas. Para obter etapas detalhadas, consulte Criação de uma pilha no AWS CloudFormation console.

   a. Abra as AWS CloudFormation console em https://console.aws.amazon.com/cloudformation.
   b. Selecione Criar pilha.
   c. Escolha O modelo está pronto e, em seguida, carregue o arquivo de modelo da sua pasta local.

      Veja a seguir um exemplo da tela Criar pilha.

   d. Escolha Próximo.
   e. Insira as seguintes informações obrigatórias:

      - AlarmNameConfige AlarmDescriptionConfig: Insira um nome e uma descrição para seu alarme.
      - ThresholdConfig: revise o valor limite para atender aos requisitos do seu aplicativo.

- D istributionIDConfig: Certifique-se de que o ID de distribuição aponte para os recursos corretos na conta em que você está criando o AWS CloudFormation empilhe.

f. Escolha Próximo.

g. Revise os valores padrão DatapointsToAlarmConfignos campos PeriodConfigEvalutionPeriodConfig, e. É uma prática recomendada usar os valores padrão para esses campos. Você pode fazer ajustes, se necessário, para atender aos requisitos do seu aplicativo.

h. Opcionalmente, insira tags e informações SNS de notificação conforme necessário. É uma prática recomendada ativar a Proteção de rescisão para evitar a exclusão acidental do alarme. Para ativar a proteção contra terminação, selecione o botão de rádio Ativado, conforme mostrado no exemplo a seguir:

i. Escolha Próximo.

j. Revise as configurações da pilha e escolha Criar pilha.

k. Depois de criar a pilha, você vê o alarme listado na lista de CloudWatch alarmes da Amazon, conforme mostrado no exemplo a seguir:

4. Depois de criar todos os seus alarmes na conta correta e AWS Região, notifique seu gerente técnico de contas (TAM). A equipe de detecção e resposta a AWS incidentes analisa o status de seus novos alarmes e, em seguida, continua sua integração.

Exemplos de casos de uso para CloudWatch alarmes em Detecção e Resposta a Incidentes

Analise os seguintes casos de uso para ver exemplos de como você pode usar os CloudWatch alarmes da Amazon em Detecção e Resposta a Incidentes.

Exemplo de caso de uso A: Application Load Balancer

Crie o seguinte CloudWatch alarme que sinaliza um possível impacto na carga de trabalho. Você pode criar uma métrica matemática que alerte quando conexões bem-sucedidas caem abaixo de um determinado limite. Para ver as CloudWatch métricas disponíveis, consulte as CloudWatch métricas do seu Application Load Balancer

Métrica: `HTTPCode_Target_3XX_Count;HTTPCode_Target_4XX_Count;HTTPCode_Target_5XX_Count.(m1+m2)/(m1+m2+m3+m4)*100 m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 = HTTP Code 4xx || m4 = HTTP Code 5xx`

NameSpace: AWS/Aplicação ELB

ComparisonOperator(Limite): Menos de x (x = limite do cliente).

Período: 60 segundos

DatapointsToAlarm: 3 de 3

Tratamento de dados perdidos: trate os dados perdidos como violação.

Estatística: soma

O diagrama a seguir mostra o fluxo para o caso de uso A:

Exemplo de caso de uso B: Amazon API Gateway

Crie o seguinte CloudWatch alarme que sinaliza um possível impacto na carga de trabalho. Você pode criar uma métrica composta que alerta quando há alta latência ou um número médio alto de erros 4XX no Gateway. API Para ver as métricas disponíveis, consulte as dimensões e métricas do Amazon API Gateway

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

NameSpace: AWS/APIPorta de entrada

ComparisonOperator(Limite): Maior que (limites x ou y do cliente)

Período: 60 segundos

DatapointsToAlarm: 1 de 1

Tratamento de dados perdidos: trate os dados perdidos como se não fossem uma violação.

Estatística:

O diagrama a seguir mostra o fluxo para o caso de uso B:

Exemplo de caso de uso C: Amazon Route 53

Você pode monitorar seus recursos criando verificações de saúde do Route 53 que são usadas CloudWatch para coletar e processar dados brutos em métricas legíveis e quase em tempo real. Você pode criar o seguinte CloudWatch alarme que sinaliza um possível impacto na carga de trabalho. Você pode usar as CloudWatch métricas para criar um alarme que é acionado quando ultrapassa o limite estabelecido. Para ver as CloudWatch métricas disponíveis, consulte CloudWatch métricas para verificações de saúde do Route 53

Métrica: `R53-HC-Success`

NameSpace: AWS/Rota 53

Limite HealthCheckStatus: HealthCheckStatus < x para 3 pontos de dados em 3 minutos (sendo x limite do cliente)

Período: 1 minuto

DatapointsToAlarm: 3 de 3

Tratamento de dados perdidos: trate os dados perdidos como violação.

Estatística: mínima

O diagrama a seguir mostra o fluxo para o caso de uso C:

Exemplo de caso de uso D: monitore uma carga de trabalho com um aplicativo personalizado

É fundamental que você reserve um tempo para definir uma verificação de saúde apropriada nesse cenário. Se você verificar apenas se a porta de um aplicativo está aberta, não verificou se o aplicativo está funcionando. Além disso, fazer uma chamada para a página inicial de um aplicativo não é necessariamente a maneira correta de determinar se o aplicativo está funcionando. Por exemplo, se um aplicativo depende de um banco de dados AND Amazon Simple Storage Service, a verificação de saúde deve validar todos os elementos. Uma maneira de fazer isso é criar uma página da web de monitoramento, como /monitor. A página de monitoramento faz uma chamada para o banco de dados para garantir que ele possa se conectar e obter dados. E a página de

monitoramento faz uma chamada para o Amazon S3. Em seguida, você aponta a verificação de integridade do balanceador de carga para a página /monitor.

O diagrama a seguir mostra o fluxo para o caso de uso D:

Ingira alertas na detecção e resposta a AWS incidentes

AWSA Detecção e Resposta a Incidentes suporta a ingestão de alarmes pela Amazon EventBridge. Esta seção descreve como integrar a detecção e resposta a AWS incidentes com diferentes ferramentas de monitoramento de desempenho de aplicativos (APM), incluindo a Amazon CloudWatch, APMs com integração direta com a Amazon EventBridge (por exemplo, DataDog e a New Relic) e APMs sem integração direta com a Amazon EventBridge. Para obter uma lista completa de APMs com integração direta com a Amazon EventBridge, consulte EventBridgeIntegrações com a Amazon.

Tópicos

- Provisionar acesso para ingestão de alertas para detecção e resposta a incidentes
- Integre a detecção e a resposta a incidentes com a Amazon CloudWatch
- Ingira alarmes APMs que tenham integração direta com a Amazon EventBridge
- Exemplo: integrar notificações do Datadog e do Splunk
- Use webhooks para ingerir alarmes APMs sem integração direta com a Amazon EventBridge

Provisionar acesso para ingestão de alertas para detecção e resposta a incidentes

Para permitir que a Detecção e Resposta a AWS Incidentes consumam alarmes da sua conta, instale a função `AWSServiceRoleForHealth_EventProcessor` vinculada ao serviço (). SLR AWS pressupõe SLR a criação de uma regra EventBridge gerenciada pela Amazon. A regra gerenciada envia notificações de suas contas para a Detecção e Resposta a AWS Incidentes. Para obter informações sobre issoSLR, incluindo as informações associadas AWS política gerenciada, consulte Uso de funções vinculadas a serviços no AWS Health Guia do usuário.

Você pode instalar essa função vinculada ao serviço em sua conta seguindo as instruções em Criar função vinculada ao serviço no AWS Identity and Access Management Guia do usuário. Ou você pode usar o seguinte AWS comando da interface de linha de comando (AWSCLI):

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

Principais saídas

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

Informações relacionadas

Para obter mais informações, consulte os tópicos a seguir.

- Usando funções vinculadas a serviços para Health AWS
- Criação de uma função vinculada ao serviço
- AWSpolítica gerenciada: AWSHealth_EventProcessorServiceRolePolicy

Integre a detecção e a resposta a incidentes com a Amazon CloudWatch

AWSA Detecção e Resposta a Incidentes usa a função vinculada ao serviço (SLR) que você ativou durante o provisionamento de acesso para criar uma regra gerenciada pela Amazon EventBridge em seu AWS conta nomeada`AWSHealthEventProcessor-DO-NOT-DELETE`. A Detecção e Resposta a Incidentes usa essa regra para ingerir CloudWatch alarmes da Amazon de suas contas. Não são necessárias etapas adicionais para ingerir alarmes. CloudWatch

Ingira alarmes APMs que tenham integração direta com a Amazon EventBridge

A ilustração a seguir mostra o processo de envio de notificações para Detecção e Resposta a AWS Incidentes a partir de ferramentas de monitoramento de desempenho de aplicativos (APM) que têm integração direta com a Amazon EventBridge, como Datadog e Splunk. Para obter uma lista completa dos APMs que têm integração direta com EventBridge, consulte EventBridge Integrações com a Amazon

Use as etapas a seguir para configurar a integração com a Detecção e Resposta a AWS Incidentes. Antes de executar essas etapas, verifique se o AWS service-linked role (SLR)`AWSServiceRoleForHealth_EventProcessor`, está instalado em suas contas.

Configure a integração com a Detecção e Resposta a AWS Incidentes

Você deve concluir as etapas a seguir para cada AWS conta e AWS Região. Os alertas devem vir do AWS conta e AWS Região em que residem os recursos do aplicativo.

1. Configure cada uma das suas fontes de eventos APMs como EventBridge parceiras da Amazon (por exemplo,`aws.partner/my_apm/integrationName`). Para obter diretrizes sobre como configurar você APM como fonte de eventos, consulte Recebimento de eventos de um parceiro de SaaS com a Amazon. EventBridge Isso cria um ônibus de eventos parceiro em sua conta.
2. Execute um destes procedimentos:
   - (Método recomendado) Crie um barramento de EventBridge eventos personalizado. AWSA Detecção e Resposta a Incidentes instala um barramento gerenciado de regras (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) por meio do `AWSServiceRoleForHealth_EventProcessor`SLR. A fonte da regra é o barramento de eventos personalizado. O destino da regra é Detecção e resposta a AWS incidentes. A regra corresponde ao padrão de ingestão de APM eventos de terceiros.
   - (Método alternativo) Use o barramento de eventos padrão em vez de um barramento de eventos personalizado. O barramento de eventos padrão exige que a regra gerenciada envie APM alertas para a Detecção e Resposta a AWS Incidentes.
3. Criar uma AWS Lambdafunção (por exemplo,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`) para transformar os eventos de ônibus de eventos de seu parceiro. Os eventos transformados correspondem à regra gerenciada`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
   a. Os eventos transformados incluem um identificador exclusivo de detecção e resposta a AWS incidentes e definem a fonte e o tipo de detalhe do evento com os valores necessários. O padrão corresponde à regra gerenciada.
   b. Defina o destino da função Lambda para o barramento de eventos personalizado criado na Etapa 2 (método recomendado) 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 a Detecção e Resposta a AWS Incidentes. A origem da regra é o barramento de eventos do parceiro que você define na etapa 1 (por exemplo, integrationName aws.partner/my_apm/). O alvo da regra é a função Lambda que você define na etapa 3 (por exemplo,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`). Para obter diretrizes sobre como definir sua EventBridge regra, consulte EventBridge as regras da Amazon.

Para obter exemplos de como configurar uma integração de barramento de eventos do parceiro para uso com Detecção e Resposta a AWS Incidentes, consulteExemplo: integrar notificações do Datadog e do Splunk.

Exemplo: integrar notificações do Datadog e do Splunk

Este exemplo fornece etapas detalhadas para integrar as notificações do Datadog e do Splunk à detecção e resposta a AWS incidentes.

1. Configure sua APM como fonte de eventos na Amazon EventBridge em sua AWS conta.
2. Crie um ônibus de eventos personalizado.
3. Crie um AWS Lambda função para transformação.
4. Crie sua EventBridge regra personalizada.

Etapa 1: configure seu APM como fonte de eventos na Amazon EventBridge

Configure cada um deles APMs como fonte de eventos na Amazon EventBridge em sua AWS conta. Para obter instruções sobre APM como configurar sua fonte de eventos, consulte as instruções de configuração da fonte do evento para sua ferramenta nos EventBridge parceiros da Amazon.

Ao configurá-lo APM como fonte de eventos, você pode ingerir notificações do seu ônibus APM para um evento em sua AWS conta. Após a configuração, a Detecção e Resposta a AWS Incidentes podem iniciar o processo de gerenciamento de incidentes quando o barramento de eventos recebe um evento. Esse processo adiciona a Amazon EventBridge como um destino em seuAPM.

Etapa 2: criar um ônibus de eventos personalizado

É uma prática recomendada usar um ônibus de eventos personalizado. AWSA Detecção e Resposta a Incidentes usa o barramento de eventos personalizado para ingerir eventos transformados. Uma AWS Lambda A função transforma o evento do ônibus de eventos do parceiro e o envia para o barramento de eventos personalizado. AWSA Detecção e Resposta a Incidentes instala uma regra gerenciada para ingerir eventos do barramento de eventos personalizado.

Você pode usar o barramento de eventos padrão em vez de um barramento de eventos personalizado. AWSA Detecção e Resposta a Incidentes modifica a regra gerenciada para ser ingerida a partir do barramento de eventos padrão em vez de um personalizado.

Crie um ônibus de eventos personalizado em seu AWS conta:

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/
2. Escolha Ônibus, ônibus de eventos.
3. Em Barramento de eventos personalizado, escolha Criar.
4. Forneça um nome para o ônibus do evento em Nome. O formato recomendado é APMName-AWSIncidentDetectionResponse - EventBus.

   Como exemplo, use uma das opções a seguir se você usa o Datadog ou o Splunk:

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

Etapa 3: criar um AWS Lambda função para transformação

A função Lambda transforma eventos entre o barramento de eventos do parceiro na Etapa 1 e o barramento de eventos personalizado (ou padrão) da Etapa 2. A transformação da função Lambda corresponde à regra gerenciada de Detecção e Resposta a AWS Incidentes.

Crie um AWS Lambda função em seu AWS conta

1. Abra a página Funções no AWS Lambda console.
2. Escolha a opção Criar função.
3. Escolha a guia Autor do zero.
4. Em Nome da função, insira um nome usando o formato`APMName-AWSIncidentDetectionResponse-LambdaFunction`.

   Veja a seguir exemplos do Datadog e do Splunk:

   - Datadog: Datadog - - AWSIncidentDetectionResponse LambdaFunction
   - Splunk: Splunk- - AWSIncidentDetectionResponse LambdaFunction
5. Em Runtime, insira Python 3.10.
6. Deixe os campos restantes com os valores padrão. Escolha a opção Criar função.
7. Na página de edição de código, substitua o conteúdo padrão da função Lambda pela função nos exemplos de código a seguir.

   Observe os comentários que começam com # nos exemplos de código a seguir. Esses comentários indicam quais valores devem ser alterados.

Modelo de código de transformação do Datadog:

```
import logging
import json
import boto3

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

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

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

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

Modelo de código de transformação do Splunk:

```
import logging
import json
import boto3

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

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

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

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

8. Escolha Implantar.

9. Adicione PutEventspermissão à função de execução do Lambda para o barramento de eventos para o qual você está enviando os dados transformados:

   a. Abra a página Funções no AWS Lambda console.
   b. Selecione a função e escolha Permissões na guia Configuração.
   c. Em Função de execução, selecione o nome da função para abrir a função de execução no AWS Identity and Access Management console.
   d. Em Políticas de permissões, selecione o nome da política existente para abrir a política.
   e. Em Permissões definidas nesta política, escolha Editar.
   f. Na página do editor de políticas, selecione Adicionar nova declaração:
   g. O editor de políticas adiciona uma nova declaração em branco semelhante à seguinte

   h. Substitua a nova declaração gerada automaticamente pela seguinte:

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

   i. O recurso é o barramento ARN de eventos personalizado que você criou Etapa 2: criar um ônibus de eventos personalizado ou o ARN do seu barramento de eventos padrão se você estiver usando o barramento de eventos padrão em seu código Lambda.

10. Revise e confirme se as permissões necessárias foram adicionadas à função.
11. Escolha Definir esta nova versão como padrão e escolha Salvar alterações.

O que é exigido de uma transformação da carga útil?

Os seguintes pares de JSON chave-valor são necessários em eventos de barramento de eventos ingeridos pela Detecção e Resposta a AWS Incidentes.

```
{
    "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.

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

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

Observe que, antes de o evento ser transformado, `detail-type` APM indica a origem do alerta, a origem é de um parceiro APM e a `incident-detection-response-identifier` chave não está presente.

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

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

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

```
    }
}
```

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

No exemplo anterior, o `incident-detection-response-identifier` valor é obtido do nome do alerta abaixo do caminho`$.detail.meta.monitor.name`. APMos caminhos dos nomes dos alertas são diferentes um APM para o outro. A função Lambda deve ser modificada para pegar o nome do alarme do JSON caminho correto do evento do parceiro e usá-lo como valor. `incident-detection-response-identifier`

Cada nome exclusivo definido no `incident-detection-response-identifier` é fornecido à equipe de detecção e resposta a AWS incidentes durante a integração. Eventos que têm um nome desconhecido para o `incident-detection-response-identifier` não são processados.

Etapa 4: criar uma EventBridge regra personalizada da Amazon

O barramento de eventos do parceiro criado na Etapa 1 exige uma EventBridge regra criada por você. A regra envia os eventos desejados do barramento de eventos do parceiro para a função Lambda criada na Etapa 3.

Para obter diretrizes sobre como definir sua EventBridge regra, consulte EventBridge as regras da Amazon.

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/
2. Escolha Regras e, em seguida, selecione o ônibus de eventos parceiro associado ao seuAPM. A seguir estão alguns exemplos de ônibus parceiros para eventos:
   - Cachorro de dados: aws.partner/datadog.com/eventbus-name
   - Splunk: aws.partner/signalfx.com/ RandomString
3. Escolha Criar regra para criar uma nova EventBridge regra.
4. Em nome da regra, insira um nome no formato `APMName-AWS Incident Detection and Response-EventBridgeRule` a seguir e escolha Avançar. Veja a seguir exemplos de nomes:
   - Datadog: Datadog- - AWSIncidentDetectionResponse EventBridgeRule
   - Splunk: Splunk- - AWSIncidentDetectionResponse EventBridgeRule

5. Em Origem do evento, selecione AWSeventos ou eventos de EventBridge parceiros.
6. Deixe o evento de amostra e o método de criação como os valores padrão.
7. Para Padrão de evento, escolha o seguinte:

    a. Fonte do evento: EventBridge parceiros.

    b. Parceiro: selecione seu APM parceiro.

    c. Tipo de evento: Todos os eventos.

    Veja a seguir exemplos de padrões de eventos:

    Exemplo de padrão de evento Datadog

    Exemplo de padrão de evento Splunk

8. Para Targets, escolha o seguinte:

    a. Tipos de alvo: AWS serviço

    b. Selecione um alvo: escolha a função Lambda.

    c. Função: O nome da função Lambda que você criou na Etapa 2.
9. Escolha Avançar, Salvar regra.

Use webhooks para ingerir alarmes APMs sem integração direta com a Amazon EventBridge

AWSO Incident Detection and Response suporta o uso de webhooks para ingestão de alarmes de terceiros APMs que não têm integração direta com a Amazon. EventBridge

Para obter uma lista de integrações diretas APMs com a Amazon EventBridge, consulte EventBridge Integrações com a Amazon.

Use as etapas a seguir para configurar a integração com a Detecção e Resposta a AWS Incidentes. Antes de executar essas etapas, verifique se a regra AWS gerenciada, AWSHealthEventProcessorEventSource-DO- NOT - DELETE, está instalada em suas contas

Ingira eventos usando webhooks

1. Defina um Amazon API Gateway para aceitar a carga útil do seuAPM.
2. Defina um AWS Lambda função para autorização usando um token de autenticação, conforme exibido na ilustração anterior.
3. Defina uma segunda função Lambda para transformar e anexar o identificador de detecção e resposta a AWS incidentes à sua carga. Você também pode usar essa função para filtrar os eventos que deseja enviar para a Detecção e Resposta a AWS Incidentes.
4. Configure seu APM para enviar notificações para as URL geradas pelo API Gateway.

Desenvolva runbooks para detecção e resposta a AWS incidentes

Você pode baixar um exemplo de runbook de detecção e resposta a incidentes: aws-idr-runbook-example.zip.

A Detecção e Resposta a Incidentes usa informações capturadas de seu questionário de integração para desenvolver runbooks e planos de resposta 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 descoberta da carga de trabalho, descritas anteriormente. Os planos de resposta são AWS Systems Manager (SSM) modelos de documentos usados para acionar incidentes. Para saber mais sobre SSM documentos, consulte AWS Systems Manager Documentos, para saber mais sobre o Incident Manager, consulte O que é AWS Systems Manager Incident Manager?

Principais saídas:

- Conclusão da definição de sua carga de trabalho sobre Detecção e Resposta a AWS Incidentes.
- Conclusão de alarmes, runbooks e definição do plano de resposta sobre detecção e resposta a AWS incidentes.

Você também pode baixar um exemplo de runbook de detecção e resposta a AWS incidentes: aws-idr-runbook-example.zip.

Exemplo de runbook:

Runbook template for AWS Incident Detection and Response

```
# Description
This document is intended for [CustomerName] [WorkloadName].

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

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

```
Hello,

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

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

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

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

Step: Information
Review of common information

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

```

```
**Engagement plans**

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

* **Initial engagement**

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


* **Engagement Escalation**

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

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

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

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


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

```
    Please join the Bridge below so we can start the steps outlined in your Runbook:
        Conference Number: <insert conference number>
        Conference URL : <insert bridgeURL>
    ```
  * 3 - Set the Case to Pending Customer Action
  * 4 - Follow **Engagement Escalation** plan as mentioned above.
  * 5 - If the customer does not respond within 30 minutes, disengage and continue to
 monitor until the alarm recovers.

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

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

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

---
Application architecture overview
```
```

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

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

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

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

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

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

---
* **Impact**
Impact is determined when either the customer's metrics do not recover, appear to be
 trending worse or if there is indication of AWS Service Impact.
```

```
  * 1 – Start **Communication plans - Impact Communication plan**
  * 2 - Start **Engagement plans - Engagement Escalation** if no response is received
 from the **Initial Engagement** contacts.
  * 3 - Start **Communication plans - Updates** if specified in **Communication plans**

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

## Step: Investigate
**Investigation**

  This section describes performing investigation of known and unknown symptoms.

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

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

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

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

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

**Identify action items**
* Record key decisions and actions taken, including temporary mitigation that might
 have been implemented.
* Ensure outstanding action items have assigned owners.
```

```
* Close out any Communication plans that were opened during the incident with a final
 confirmation of recovery notification.
```

Teste cargas de trabalho integradas

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

A última etapa do processo de integração é realizar um dia de jogo para sua nova carga de trabalho. Depois que a ingestão do alarme for concluída, a Detecção e Resposta a AWS Incidentes confirmará a data e a hora de sua escolha para iniciar o dia de jogo.

Seu dia de jogo tem dois propósitos principais:

- Validação funcional: confirma que a detecção e resposta a AWS incidentes podem receber corretamente seus eventos de alarme. Além disso, a validação funcional confirma que seus eventos de alarme acionam os runbooks apropriados e quaisquer outras ações desejadas, como a criação automática de casos, caso você os tenha selecionado durante a ingestão do alarme.
- Simulação: O dia de jogo é uma simulação completa do que pode acontecer durante um incidente real. AWSA Detecção e Resposta a Incidentes segue as etapas prescritas para fornecer uma visão de como um incidente real pode se desenrolar. O dia do jogo é uma oportunidade para você fazer perguntas ou refinar instruções para melhorar o engajamento.

Durante o teste de alarme, a Detecção e Resposta a AWS Incidentes trabalha com você para corrigir quaisquer problemas identificados.

CloudWatch alarmes

AWSA Detecção e Resposta a Incidentes testa seus CloudWatch alarmes da Amazon monitorando a mudança de estado do seu alarme. Para fazer isso, altere manualmente o alarme para o estado de alarme usando o AWS Command Line Interface. Você também pode acessar o AWS CLI from AWS CloudShell. AWSA Detecção e Resposta a Incidentes fornece uma lista de AWS CLI comandos para você usar durante o teste.

Exemplo AWS CLI comando para definir um estado de alarme:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --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 SetAlarmState.

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

APMAlarmes de terceiros

As cargas de trabalho que utilizam uma ferramenta de monitoramento de desempenho de aplicativos (APM) de terceiros DataDog, como Splunk ou Dynatrace NewRelic, exigem instruções diferentes para simular um alarme. No início do GameDay, a Detecção e Resposta a AWS Incidentes solicita que você altere temporariamente seus limites de alarme ou operadores de comparação para forçar o alarme a entrar no ALARMstatus. Esse status aciona uma carga útil para Detecção e Resposta a AWS Incidentes.

Principais saídas

Principais saídas:

- A ingestão de alarmes foi bem-sucedida e sua configuração de alarme está correta.
- Os alarmes são criados e recebidos com sucesso pela Detecção e Resposta a AWS Incidentes.
- Um caso de suporte é criado para sua contratação e seus contatos prescritos são notificados.
- AWSA Detecção e Resposta a Incidentes podem interagir com você pelos meios de conferência prescritos.
- Todos os alarmes e casos de suporte gerados como parte do Gameday foram resolvidos.
- Um e-mail do Go-Live é enviado confirmando que sua carga de trabalho agora está sendo monitorada pela Detecção e Resposta a AWS Incidentes.

Questionários de integração da carga de trabalho e ingestão de alarmes

Baixe o questionário de integração da carga de trabalho.

Baixe o questionário de ingestão de alarmes.

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.
Requisitos regulatórios e/ou de conformidade aplicáveis para essa carga de trabalho e quaisquer ações exigidas da AWS depois de um incidente.	A carga de trabalho trata dos registros de saúde do paciente, que devem ser mantidos em segurança e confidencialidade.

Questionário de integração da carga de trabalho - Perguntas sobre arquitetura

Perguntas sobre arquitetura

Pergunta	Exemplo de resposta
Uma lista de AWS tags de 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.	appName: Optimax ambiente: Produção

Pergunta	Exemplo de resposta
Note As tags diferenciam letras maiúsculas de minúsculas. Se você fornecer várias tags, todos os recursos usados por essa carga de trabalho deverão ter as mesmas tags.	
Uma lista de AWS Serviços utilizados por essa carga de trabalho e pela AWS Conta e regiões em que eles estão. **Note** Crie uma nova linha para cada serviço.	Rota 53: encaminha o tráfego da Internet para ALB o. Conta: 123456789101 Região: US- EAST -1, US- WEST -2
Uma lista de AWS Serviços utilizados por essa carga de trabalho e pela AWS Conta e regiões em que eles estão. **Note** Crie uma nova linha para cada serviço.	ALB: encaminha o tráfego de entrada para um grupo-alvo de ECS contêineres. Conta: 123456789101 Região: N/A
Uma lista de AWS Serviços utilizados por essa carga de trabalho e pela AWS Conta e regiões em que eles estão. **Note** Crie uma nova linha para cada serviço.	ECS: infraestrutura de computação para a principal frota lógica de negócios. Responsáv el por lidar com as solicitações recebidas do usuário e fazer consultas à camada de persistência. Conta: 123456789101 Região: US- EAST -1

Pergunta	Exemplo de resposta
Uma lista de AWS Serviços utilizados por essa carga de trabalho e pela AWS Conta e regiões em que eles estão. **Note** Crie uma nova linha para cada serviço.	RDS: O cluster Amazon Aurora armazena dados de usuários acessados pela camada lógica ECS de negócios. Conta: 123456789101 Região: US- EAST -1
Uma lista de AWS Serviços utilizados por essa carga de trabalho e pela AWS Conta e regiões em que eles estão. **Note** Crie uma nova linha para cada serviço.	S3: Armazena ativos estáticos do site. Conta: 123456789101 Região: N/A
Detalhe todos os componentes upstream/ downstream que não estão sendo integrados e que podem afetar essa carga de trabalho em caso de interrupção.	Microsserviço de autenticação: impedirá que os usuários carreguem seus registros de saúde, pois eles não serão autenticados.
Há algum local ou não AWS componentes para essa carga de trabalho? Em caso afirmativo, quais são e quais funções são executadas?	Todo o tráfego baseado na Internet de entrada/ saída de AWS é roteado por meio de nosso serviço de proxy local.
Forneça detalhes de qualquer plano manual ou automatizado de failover/recuperação de desastres na zona de disponibilidade e em nível regional.	Espera quente. Failover automatizado para US-WEST -2 durante uma queda sustentada na taxa de sucesso.

Questionário de integração da carga de trabalho - AWS Perguntas sobre eventos de serviço

AWS Perguntas sobre eventos de serviço

Pergunta	Exemplo de resposta
Forneça os detalhes de contato (nome/e-mail/telefone) da equipe interna de gerenciamento de incidentes graves/crises de TI da sua empresa.	Equipe de gerenciamento de incidentes graves mim@example.com +61 2 3456 7890
Forneça detalhes de qualquer ponte estática de gerenciamento de incidentes/crises estabelecida pela sua empresa. Se você utilizar pontes não estáticas, especifique sua aplicação preferida e AWS solicitará esses detalhes durante um incidente. **Note** Se um não for fornecido, então AWS entrará em contato durante um incidente e fornecerá uma ponte Chime para você entrar.	Amazon Chime https://chime.aws/1234567890

Questionário de ingestão de alarmes

Perguntas sobre o Runbook

Pergunta	Exemplo de resposta
AWS envolverá contatos de carga de trabalho por meio do AWS Support Caso. Quem é o contato principal quando um alarme é acionado para essa carga de trabalho?	Equipe de aplicação app@example.com +61 2 3456 7890

Pergunta	Exemplo de resposta
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 entrar.	
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 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
AWS comunica atualizações por meio do caso de suporte em intervalos regulares durante todo o incidente. Há contatos adicionais que devem receber essas atualizações?	john.smith@example.com, jane.smith@example.com

Matriz de alarme

Matriz de alarmes

Forneça as informações a seguir para identificar o conjunto de alarmes que acionará a Detecção e a Resposta a AWS Incidentes para criar incidentes em nome de sua carga de trabalho. Depois que os engenheiros da AWS Incident Detection and Response analisarem seus alarmes, etapas adicionais de integração serão fornecidas.

AWSCritérios críticos de detecção e resposta a incidentes para alarmes:

- AWSOs alarmes de detecção e resposta a incidentes só devem entrar no estado de “Alarme” se houver um impacto comercial significativo na carga de trabalho monitorada (perda de receita/ degradação da experiência do cliente), o que requer atenção imediata do operador.
- AWSOs alarmes de detecção e resposta a incidentes também devem envolver seus resolvedores para a carga de trabalho ao mesmo tempo ou antes da contratação. 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.
- AWSOs limites de alarme de detecção e resposta a incidentes devem ser definidos com um limite e uma duração apropriados para que, sempre que um alarme disparar, 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.

AWSPolítica de detecção e resposta a incidentes para violações de critérios:

Esses critérios só podem ser avaliados case-by-case com base na ocorrência dos eventos. 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 equipe de engenharia de confiabilidade do site (SRE) se quiser que a equipe de Detecção e Resposta a AWS Incidentes ligue para eles depois de enviar um e-mail de engajamento inicial.

Tabela de matriz de alarmes

Nome da métrica/ARN/Threshold	Descrição	Observações	Ações solicitadas
Volume da carga de trabalho/ *CW Alarm ARN* / CallCount < 100000 para 5 pontos de dados em 5 minutos, trate os dados perdidos como ausentes	Essa métrica representa o número de solicitações recebidas que chegam à carga de trabalho, medido no nível do Application Load Balancer. Esse alarme é importante porque quedas significativas nas solicitações recebidas podem indicar problemas com a conectividade de rede upstream ou problemas com nossa DNS implementação que fazem com que os usuários não consigam acessar a carga de trabalho.	O alarme entrou no estado “Alarme” 10 vezes na última semana. Esse alarme corre o risco de falsos positivos. A revisão dos limites está planejada. Problemas? Não ou Sim (se Não, deixe em branco): Esse alarme é acionado com frequência durante a execução de um determinado trabalho em lote. Resolvers: engenheiros de confiabilidade do site	Envolva a equipe de engenharia de confiabilidade do site enviando um e-mail para *SRE@xyz.com* Crie um caso de AWS Suporte Premium para nossos ELB serviços e para os do Route 53. Se for necessária uma IMMEDIATE ação: Verifique Memória/espaço EC2 livre em disco e informe o *XYZ* Forme uma equipe por e-mail para reiniciar a instância ou executar um log flush. (se a ação imediata não for necessária, deixe em branco)

Nome da métrica/ARN/Threshold	Descrição	Observações	Ações solicitadas
Latência da solicitação de carga de trabalho/ *CW Alarm ARN* / p90 Latência > 100 ms para 5 pontos de dados em 5 minutos, trate os dados perdidos como perdidos	Essa métrica representa a latência p90 para as HTTP solicitações a serem atendidas pela carga de trabalho. Esse alarme representa latência (medida important e da experiência do cliente no site).	O alarme entrou no estado “Alarme” 0 vezes na última semana. Problemas? Não ou Sim (se Não, deixe em branco): Esse alarme é acionado com frequência durante a execução de um determinado trabalho em lote. Resolvers: engenheiros de confiabilidade do site	Envolva a equipe de engenharia de confiabilidade do site enviando um e-mail para *SRE@xyz.com* Crie um case AWS Premium Support para nossos ECW serviçosRDS. Se for necessária uma IMMEDIATE ação: Verifique Memória/espaço EC2 livre em disco e informe o *XYZ* Forme uma equipe por e-mail para reiniciar a instância ou executar um log flush. (se a ação imediata não for necessária, deixe em branco)

Nome da métrica/ARN/Threshold	Descrição	Observações	Ações solicitadas
Disponibilidade da solicitação de carga de trabalho/ *CW Alarm ARN* / Disponibilidade < 95% para 5 pontos de dados em 5 minutos, trate os dados perdidos como perdidos.	Essa métrica representa a disponibilidade de HTTP solicitações a serem atendidas pela carga de trabalho. (nº de HTTP 200/Nº de solicitações) por período. Esse alarme representa a disponibilidade da carga de trabalho.	O alarme entrou no estado “Alarme” 0 vezes na última semana. Problemas? Não ou Sim (se Não, deixe em branco): Esse alarme é acionado com frequência durante a execução de um determinado trabalho em lote. Resolvers: engenheiros de confiabilidade do site	Envolva a equipe de engenharia de confiabilidade do site enviando um e-mail para *SRE@xyz.com* Crie um caso de AWS Suporte Premium para nossos ELB serviços e para os do Route 53. Se for necessária uma IMMEDIATE ação: Verifique Memória/espaço EC2 livre em disco e informe o *XYZ* Forme uma equipe por e-mail para reiniciar a instância ou executar um log flush. (se a ação imediata não for necessária, deixe em branco)
Exemplo de alarme New Relic			

Nome da métrica/ARN/Threshold	Descrição	Observações	Ações solicitadas
Teste de integração de ponta a ponta/ *CW Alarm ARN* / Taxa de falha de 3% para métricas de 1 minuto em 3 minutos de duração, trate os dados perdidos como perdidos Identificador de carga de trabalho: fluxo de trabalho de teste de ponta a ponta, AWS região: EUA EAST -1, ID da AWS conta: 012345678910	Essa métrica testa se uma solicitação pode atravessar cada camada da carga de trabalho. Se esse teste falhar, isso representa uma falha crítica no processamento de transações comerciais. Esse alarme representa a capacidade de processar transações comerciais para a carga de trabalho.	O alarme entrou no estado “Alarme” 0 vezes na última semana. Problemas? Não ou Sim (se Não, deixe em branco): Esse alarme é acionado com frequência durante a execução de um determinado trabalho em lote. Resolvers: engenheiros de confiabilidade do site	Envolva a equipe de engenharia de confiabilidade do site enviando um e-mail para *SRE@xyz.com* Crie um caso de AWS Suporte Premium para nossos ECS serviços e para os do DynamoDB. Se for necessária uma IMMEDIATE ação: Verifique Memória/espaço EC2 livre em disco e informe o *XYZ* Forme uma equipe por e-mail para reiniciar a instância ou executar um log flush. (se a ação imediata não for necessária, deixe em branco)

Solicitar alterações em uma carga de trabalho integrada

Para solicitar alterações em uma carga de trabalho integrada, conclua as etapas a seguir para criar um caso de suporte com Detecção e Resposta a AWS Incidentes.

1. Vá para o AWS SupportCentralize 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:

   AWSDetecção e resposta a incidentes - *`workload_name`*
7. Insira uma Descrição para essa alteração. Por exemplo, insira “Esta solicitação é para alterações em uma carga de trabalho existente integrada à Detecção e Resposta a AWS Incidentes”. 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 qualquer e-mail IDs que você deseja receber sobre essa alteração.

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

   > **Important**
   >
   > A falha ao adicionar e-mail IDs 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 o e-mail IDs na seção Contatos adicionais - opcional.

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

Desembarcar de uma carga de trabalho

Para remover uma carga de trabalho da Detecção e Resposta a AWS Incidentes, crie um novo caso de suporte para cada carga de trabalho. Ao criar o caso de suporte, lembre-se do seguinte:

- Para eliminar 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 de pagador.
- Para remover uma carga de trabalho que abrange várias AWS contas e, em seguida, crie o caso de suporte a partir da sua conta de pagador. No corpo do estojo de suporte, liste todas as contas IDs como externas.

> **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 Centralize e, em seguida, 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 AWS incidentes - *`workload_name`*
7. Insira uma Descrição para essa alteração. Por exemplo, insira “Esta solicitação é para excluir uma carga de trabalho existente integrada à Detecção e Resposta a AWS Incidentes”. 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 qualquer e-mail IDs que você queira receber 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.
- Fase pós-integração: 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 AWS incidentes com detecção e resposta a incidentes

AWSA Detecção e Resposta a Incidentes oferecem monitoramento proativo e gerenciamento de incidentes 24 horas por dia, 7 dias por semana, fornecidos por uma equipe designada de gerentes de incidentes.

1. Geração de alarmes: os alarmes acionados em suas cargas de trabalho são enviados pela Amazon EventBridge para a Detecção e Resposta a AWS Incidentes. AWSA Detecção e Resposta a Incidentes abre automaticamente o caderno 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 pela Detecção e Resposta a AWS Incidentes, você poderá criar um caso de suporte para solicitar uma Resposta a Incidentes. Para obter mais informações sobre como solicitar uma resposta a incidentes, consulteSolicitação de resposta a incidentes.
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 com Serviços da AWS usado 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 a pessoa certa AWS especialistas em suporte.

   Porque monitores de detecção e resposta a AWS incidentes Serviços da AWS especificamente para seus aplicativos, AWS a Detecção e Resposta a Incidentes podem determinar se o incidente está relacionado a um AWS service (Serviço da AWS) problema mesmo antes de um AWS service (Serviço da AWS) evento é declarado. Nesse cenário, o gerente de incidentes o aconselha sobre o status do AWS service (Serviço da AWS), aciona o AWS O gerenciamento de incidentes de eventos de serviço flui e acompanha a equipe de serviço na resolução. As informações fornecidas oferecem a oportunidade de implementar seus planos de recuperação ou soluções alternativas com antecedência para mitigar o impacto do AWS Evento de serviço. Para obter mais informações, consulte Gerenciamento de incidentes para eventos de serviço.
3. Resolução de incidentes: o gerente de incidentes coordena o incidente de acordo com o necessário AWS equipes e garante que você permaneça engajado com a pessoa certa AWS especialistas até que o incidente seja mitigado ou resolvido.

4. Análise pós-incidente (se solicitada): após um AWS incidente, a Detecção e Resposta a Incidentes podem 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 da causa raiz (RCA). Você pode solicitar uma RCA adição ao 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 AWS Support support case on
behalf of the customer.
 At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and AWS Support 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 a 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 an 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.
```

Provisionar acesso para equipes de aplicativos

AWSA Detecção e Resposta a Incidentes se comunica com você por meio de AWS Support casos durante o ciclo de vida de um incidente. Para se corresponder com os gerentes de incidentes, suas equipes devem ter acesso ao AWS Support Centro.

Para obter mais informações sobre o acesso de provisionamento, consulte Gerenciar o acesso a AWS Support Centro no AWS Support Guia do usuário.

Gerenciamento de incidentes para eventos de serviço

AWSA Detecção e Resposta a Incidentes notifica você sobre um evento de serviço contínuo em seu AWS Regiões, independentemente de sua carga de trabalho ser afetada ou não. Durante um AWS evento de serviço, Detecção e Resposta a AWS Incidentes cria um AWS Support Case, participe de sua teleconferência para receber feedback sobre impacto e sentimento e fornece orientação para invocar seus planos de recuperação durante o evento. Você também recebe uma notificação por meio de AWS Health contendo detalhes do evento. Clientes que não são afetados pelo AWS evento de serviço próprio (por exemplo, operando em um evento diferente AWS Região, não use o AWS serviços que estão prejudicados, etc.) continuam sendo apoiados pelo contrato padrão. Para obter mais informações sobre AWS Health, veja O que é AWS Health?.

Relatório pós-incidente para eventos de serviço (se solicitado): se um evento de serviço causar um incidente, você poderá solicitar a Detecção e Resposta a AWS Incidentes para realizar uma análise pós-incidente e gerar um Relatório Pós-Incidente. O Relatório Pós-Incidente para eventos de serviço inclui o seguinte:

- Uma descrição do problema
- O impacto do incidente
- Informações compartilhadas no AWS Health dashboard (painel)
- As equipes que estiveram envolvidas durante o incidente
- Soluções alternativas e ações tomadas para mitigar ou resolver o incidente

O Relatório Pós-Incidente para eventos de serviço pode conter informações que podem ser usadas para reduzir a probabilidade de recorrência de incidentes ou para melhorar o gerenciamento de uma ocorrência futura de um incidente semelhante. O relatório pós-incidente para eventos de serviço não é uma análise de causa raiz (RCA). Você pode solicitar uma RCA adição ao Relatório Pós-Incidente para eventos de serviço.

Veja a seguir um exemplo de um relatório pós-incidente para um evento de serviço:

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

Post Incident Report - LSE000123
Customer: Example Customer
AWS Support Case ID(s): 0000000000
Incident Start: Example: 1 January 2024, 3:30 PM UTC
Incident Resolved: Example: 1 January 2024, 3:30 PM UTC
Incident Duration: 1:02:00
Service(s) Impacted: Lists the impacted services such as EC2, ALB
Region(s): Lists the impacted AWS Regions, such as US-EAST-1
Alarm Identifiers: Lists any customer alarms that triggered during the Service Level Event

Problem Statement:
Outlines impact to end users and operational infrastructure impact during the Service Level Event.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a service outage...

Impact Summary for Service Level Event:
(This section is limited to approved messaging available on the AWS Health Dashboard)
Outline approved customer messaging as provided on the AWS Health Dashboard.
Between 1:14 PM and 4:33 PM UTC, we experienced increased error rates for the Amazon SNS Publish, Subscribe, Unsubscribe, Create Topic, and Delete Topic APIs in the EU-WEST-1 Region. The issue has been resolved and the service is operating normally.

Incident Summary:
Summary of the incident in chronological order and steps taken by AWS Incident Managers during the Service Level Event to direct the incident to a path to mitigation.
At 2024-01-04T01:25:00 UTC, the workload alarm triggered a critical incident...
At 2024-01-04T01:27:00 UTC, customer was notified via case 000000000 about the triggered alarm
At 2024-01-04T01:30:00 UTC, IDR team identified an ongoing service event which was related to the customer triggered alarm
At 2024-01-04T01:32:00 UTC, IDR team sent an impact case correspondence requesting for the incident bridge details
At 2024-01-04T01:32:00 UTC, customer provided the incident bridge details
At 2024-01-04T01:32:00 UTC, IDR team joined the incident bridge and provided information about the ongoing service outage

```
By 2024-01-04T02:35:00 UTC, customer failed over to the secondary region (EU-WEST-1) to
 mitigate impact...
At 2024-01-04T03:27:00 UTC, customer confirmed recovery, the call was spun down...

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not an Root Cause Analysis
 (RCA).
Back-off and retries yielded mild recovery. Full mitigation happened ...

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 ...
Work with AWS Support and TAM team to ensure ...
```

Solicitação de resposta a incidentes

Se ocorrer um incidente crítico em sua carga de trabalho que não seja detectado pelos alarmes monitorados pela Detecção e Resposta a AWS Incidentes, 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.

Para solicitar uma resposta a incidentes para um incidente que está afetando ativamente sua carga de trabalho, crie um AWS Support Caso. Depois que o caso de suporte for levantado, a Detecção e Resposta a AWS Incidentes envolverá você em uma ponte de conferência com o AWS especialistas necessários para acelerar a recuperação de sua carga de trabalho.

Solicite uma resposta a incidentes usando o AWS Support Center Console

1. Abra as AWS Support Center Consolee, em seguida, escolha Criar caso.
2. Escolha Técnico.
3. Em Serviço, escolha Detecção e resposta a incidentes.
4. Em Categoria, escolha Incidente ativo.
5. Em Severidade, escolha Sistema crítico para negócios inativo.
6. Insira um assunto para esse incidente. Por exemplo:

AWSDetecção e resposta a incidentes - Incidente ativo - workload_name

7. 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:
8. Na seção Contatos adicionais, insira os endereços de e-mail dos quais você deseja receber correspondências sobre esse incidente.

   A ilustração a seguir mostra a tela do console com o campo Contatos adicionais destacado.

9. Selecione Enviar.

   Depois de enviar uma solicitação de resposta a incidentes, você pode adicionar outros endereços de e-mail da sua organização. Para adicionar endereços adicionais, responda ao caso e adicione os endereços de e-mail na seção Contatos adicionais.

   A ilustração a seguir mostra a tela de detalhes do caso com o botão Responder destacado.

   A ilustração a seguir mostra o caso Responder com o campo Contatos adicionais e o botão Enviar destacados.

10. AWSA Detecção e Resposta a Incidentes confirma seu caso em cinco minutos e envolve você em uma ponte de conferência com o apropriado AWS especialistas.

Solicite uma resposta a incidentes usando o AWS Support API

Support cases podem ser criados programaticamente usando o AWS Support API.

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

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

```
/awssupport create
```

3. Insira um assunto para esse incidente. Por exemplo, insira Detecção e resposta a AWS incidentes - Incidente ativo - 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 Sistema crítico para negócios inativo.

10. Em Método de contato, escolha Notificações por e-mail e Slack.

> **Note**
>
> AWSA Detecção e Resposta a Incidentes não são compatíveis com o Live Chat no Slack. Se você selecionar essa opção, observará um atraso nas respostas à sua Solicitação de Resposta a Incidentes.

11. Você pode configurar contatos adicionais para os quais gostaria de receber cópias da correspondência por e-mail sobre esse incidente.

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

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

AWSAplicativo Support no Slack

AWS os clientes podem usar o AWS Support App in Slackpara gerenciar seus AWS Support casos no Slack.

AWS Os clientes de Detecção e Resposta a Incidentes podem usar o AWS Support App in Slack para receber notificações sobre novos incidentes iniciados por alarme em sua carga de trabalho ou para criar uma Solicitação de Resposta a Incidentes.

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

Important

- Quando você atualiza ou cria um caso de Support com AWS Detecção e resposta a incidentes por meio do AWS Support App in Slack, você deve escolher o método de contato por e-mail e notificações do Slack.

  AWS O Incident Detection and Response suporta somente correspondência por e-mail em casos de Support. O bate-papo ao vivo não é suportado.

- Para garantir que você receba notificações no Slack sobre todos os incidentes iniciados por alarme em sua carga de trabalho, você deve configurar o AWS Support App in Slack para todas as contas da sua carga de trabalho que estão integradas ao AWS Detecção e resposta a incidentes. Support cases são criados na conta na qual o alarme de carga de trabalho foi originado.
- Vários casos de Support de alta gravidade podem ser abertos em seu nome durante um incidente para entrar em contato AWS Support resolvedores. 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.
- Notificações que você recebe por meio do AWS Support App in Slack não substitua os contatos iniciais e de escalonamento de sua carga de trabalho que são contratados por e-mail ou telefonema por AWS Detecção e resposta a incidentes durante um incidente.

Notificações de incidentes iniciados por alarme no Slack

Quando o aplicativo AWS Support no Slack é configurado em seu canal do Slack, você é notificado sobre incidentes iniciados por alarme em sua carga de trabalho monitorada de Detecção e Resposta a AWS Incidentes.

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

Exemplo de notificação

Quando o incidente iniciado pelo alarme for reconhecido pela Detecção e Resposta a AWS Incidentes, uma notificação semelhante à abaixo será gerada no Slack:

Para ver a correspondência completa adicionada pela Detecção e Resposta a AWS Incidentes, escolha Ver detalhes.

Outras atualizações da Detecção e Resposta a AWS Incidentes aparecem no tópico do caso.

Escolha Ver detalhes para ver a correspondência completa adicionada pela Detecção e Resposta a AWS Incidentes.

Solicitações de resposta a incidentes no Slack

Para obter instruções sobre como criar uma solicitação de resposta a incidentes por meio do aplicativo AWS Support no Slack, consulte Solicitações de resposta a incidentes.

Relatórios de detecção e resposta a incidentes da AWS

A Detecção e Resposta a Incidentes fornece dados operacionais e de desempenho para ajudá-lo a entender como o serviço está configurado, o histórico de seus incidentes e o desempenho do serviço de Detecção e Resposta a Incidentes.

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 compartilhada da AWS se aplica à proteção de dados em AWS Support. 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 seu 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) para se comunicar com os recursos. AWS 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 obter mais informações, consulte AWS CloudTrail.
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços. Para obter informações, consulte serviços e ferramentas AWS criptográficas.
- 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 AWS Support ou Serviços da AWS usa o console, a API, a AWS CLI ou AWS os 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 IDR guia.

- Última atualização da documentação: 12 de junho de 2024

Alteração	Descrição	Data
Adicionou uma nova página AWS Support App in Slack Gerenciamento de incidentes atualizado com Detecção e resposta a AWS incidentes	Adicionou uma nova página para AWS Support App in Slack Gerenciamento de incidentes atualizado com Detecção e resposta a AWS incidentes 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: Assinatura da conta	12 de junho de 2024
Relatório pós-incidente para eventos de serviço agora disponível	A seção Gerenciamento de incidentes para eventos de serviço foi atualizada para incluir informações sobre o Relatório Pós-Incidente para eventos de serviço. Seção atualizada: Gerenciamento de incidentes para eventos de serviço	8 de maio 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	28 de março de 2024

Alteração	Descrição	Data
	Para obter mais informações, consulte Excluir uma carga de trabalho.	
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 Assinatura da conta	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	29 de fevereiro de 2024
Atualizado O que é detecção e resposta a AWS incidentes	A seção O que é detecção e resposta a AWS incidentes 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. Seção atualizada: Questionários de integração da carga de trabalho e ingestão de alarmes	2 de fevereiro de 2024

Alteração	Descrição	Data
Atualizado AWS Eventos de serviço e informações de integração	Várias seções foram atualizadas com novas informações para integração. Seções atualizadas: • Gerenciamento de incidentes para eventos de serviço • Descoberta da carga de trabalho • Integração • Assinatura da conta Novas seções • Provisionar acesso 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 alertas para detecção e resposta a incidentes	17 de janeiro de 2024
Etapas de exemplo atualizadas	Atualizou o procedimento para as etapas 2,3 e 4 em Exemplo: Integrando notificações do Datadog e do Splunk. Seção atualizada: Exemplo: integrar notificações do Datadog e do Splunk	21 de dezembro de 2023
Gráfico e texto de introdução atualizados	Gráfico atualizado nos alarmes do Ingest APMs que têm integração direta com a Amazon. EventBridge Seção atualizada: Desenvolva runbooks para detecção e resposta a AWS incidentes	21 de dezembro de 2023

Alteração	Descrição	Data
Modelo de runbook atualizado	Atualizou o modelo de runbook em Desenvolvendo runbooks para detecção e resposta a AWS incidentes. Seção atualizada: Desenvolva runbooks para detecção e resposta a AWS 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: Use AWS CloudFormation modelos para criar CloudWatch alarmes em Detecção e Resposta a Incidentes 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: Solicitar alterações em uma carga de trabalho integrada Seção atualizada: Assinatura da conta	05 de setembro de 2023
Nova seção em Getting Started	Foram adicionados alertas Ingira alertas na detecção e resposta a AWS incidentes de ingestão à detecção e resposta a AWS incidentes.	30 de junho de 2023

Alteração	Descrição	Data
Documento original	AWSDetecção e resposta a incidentes publicadas pela primeira vez	15 de março de 2023

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

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.