



AWSKonzepte und Verfahren zur Erkennung und Reaktion auf Vorfälle

AWSBenutzerleitfaden zur Erkennung und Reaktion auf Vorfälle



Version November 1, 2024

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWSBenutzerleitfaden zur Erkennung und Reaktion auf Vorfälle: AWSKonzepte und Verfahren zur Erkennung und Reaktion auf Vorfälle

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Incident Detection and Response?	1
Nutzungsbedingungen	2
Architektur	3
Rollen und Zuständigkeiten	4
Verfügbarkeit in Regionen	6
Erste Schritte	9
Workloads	9
Alarmer	9
Onboarding	10
Onboarding von Arbeitslasten	10
Verschlucken von Alarmen	11
Fragebögen zur Einführung	11
Fragebogen zum Onboarding zur Arbeitslast — Allgemeine Fragen	12
Fragebogen zum Onboarding der Arbeitslast — Fragen zur Architektur	12
Fragebogen zum Onboarding von Workloads — Fragen zum AWS Service Event	15
Fragebogen zur Erfassung von Alarmen	16
Alarmmatrix	17
Erkennung von Arbeitslasten	23
Abonnieren Sie einen Workload	23
Definieren und konfigurieren Sie Alarmer	26
CloudWatch Alarmer erstellen	29
Erstellen Sie CloudWatch Alarmer mit CloudFormation Vorlagen	32
Beispielhafte Anwendungsfälle für CloudWatch Alarmer	35
Alarmer aufnehmen	37
Zugriff bereitstellen	38
Integrieren Sie mit CloudWatch	38
Alarmer von APMs mit Integration aufnehmen EventBridge	39
Beispiel: Integration von Benachrichtigungen von Datadog und Splunk	40
Alarmer ohne Integration aufnehmen APMs EventBridge	50
Workloads verwalten	52
Entwickeln Sie Runbooks und Reaktionspläne	52
Testen Sie integrierte Workloads	59
CloudWatch Alarmer	60
APMAlarmer von Drittanbietern	60

Die wichtigsten Ausgaben	60
Fordern Sie Änderungen an einem Workload an	61
Einen Workload auslagern	62
Überwachung und Beobachtbarkeit	64
Implementierung der Beobachtbarkeit	65
Vorfallmanagement	66
Bereitstellen des Zugriffs für Anwendungsteams	69
Störungsmanagement für Serviceereignisse	69
Fordern Sie eine Reaktion auf einen Vorfall an	71
Anfrage über AWS Support Center Console	72
Anfrage über AWS Support API	73
Anfrage über AWS Support App in Slack	73
Verwalten Sie Supportfälle bei der Erkennung und Reaktion auf Vorfälle mit dem AWS Support App in Slack	75
Benachrichtigungen über einen durch einen Alarm ausgelösten Vorfall in Slack	76
Erstelle eine Anfrage zur Reaktion auf einen Vorfall in Slack	76
Berichterstellung	77
Sicherheit und Resilienz	78
Zugriff auf Ihre Konten	79
Ihre Alarmdaten	79
Dokumentverlauf	80
.....	lxxxvi

Was ist AWS Incident Detection and Response?

AWS Incident Detection and Response bietet berechtigten AWS Enterprise Support-Kunden eine proaktive Reaktion auf Vorfälle, um das Ausfallpotenzial zu verringern und die Wiederherstellung kritischer Workloads nach einer Unterbrechung zu beschleunigen. Incident Detection and Response erleichtert Ihnen die Zusammenarbeit bei AWS der Entwicklung von Runbooks und Reaktionsplänen, die auf jeden integrierten Workload zugeschnitten sind.

Incident Detection and Response bietet die folgenden Hauptfunktionen:

- **Verbesserte Beobachtbarkeit:** AWS Experten unterstützen Sie bei der Definition und Korrelation von Kennzahlen und Alarmen zwischen den Anwendungs- und Infrastrukturebenen Ihres Workloads, um Störungen frühzeitig zu erkennen.
- **Reaktionszeit von 5 Minuten:** IMEs Überwachen Sie Ihre integrierten Workloads rund um die Uhr, um kritische Vorfälle zu erkennen. Sie IMEs reagieren innerhalb von 5 Minuten nach Auslösung eines Alarms oder als Reaktion auf einen geschäftskritischen Support-Fall, den Sie an Incident Detection and Response richten.
- **Schnellere Problemlösung:** IMEs Verwenden Sie vordefinierte und benutzerdefinierte Runbooks, die für Ihre Workloads entwickelt wurden, um innerhalb von 5 Minuten zu antworten, in Ihrem Namen eine Support-Anfrage zu erstellen und Vorfälle auf Ihrem Workload zu verwalten. IMEs Sorgen Sie dafür, dass alle Vorfälle in einem einzigen Thread bearbeitet werden, und sorgen Sie dafür, dass Sie die richtigen AWS Experten kontaktieren, bis der Vorfall gelöst ist.
- **Vorfallmanagement für AWS Ereignisse:** Da wir den Kontext Ihrer kritischen Arbeitslast (z. B. Konten, Services und Instanzen) verstehen, können wir potenzielle Auswirkungen auf Ihre Arbeitslast während eines AWS Serviceereignisses erkennen und Sie proaktiv darüber informieren. Falls gewünscht, kontaktieren IMEs wir Sie während der AWS Serviceveranstaltungen und informieren Sie über die Ereignisse auf dem Laufenden. Incident Detection and Response kann Ihnen bei der Wiederherstellung während eines Serviceereignisses zwar keine Priorität einräumen, aber Incident Detection and Response bietet Unterstützung beim Support, der Sie bei der Umsetzung Ihres Risikominderungsplans unterstützt.
- **Geringeres Ausfallpotenzial:** Nach der Behebung des Vorfalls IMEs bieten sie Ihnen (auf Anfrage) eine Überprüfung an. Und AWS Experten arbeiten mit Ihnen zusammen, um die gewonnenen Erkenntnisse anzuwenden, um den Notfallplan und die Runbooks zu verbessern. Sie können auch die kontinuierliche AWS Resilience Hub Überwachung der Ausfallsicherheit Ihrer Workloads nutzen.

Themen

- [Nutzungsbedingungen für die Erkennung und Reaktion auf Vorfälle](#)
- [Architektur der Erkennung und Reaktion auf Vorfälle](#)
- [Rollen und Verantwortlichkeiten bei der Erkennung und Reaktion auf Vorfälle](#)
- [Regionale Verfügbarkeit für Incident Detection and Response](#)

Nutzungsbedingungen für die Erkennung und Reaktion auf Vorfälle

In der folgenden Liste werden die wichtigsten Anforderungen und Einschränkungen für die Nutzung von AWS Incident Detection and Response beschrieben. Es ist wichtig, dass Sie sich mit diesen Informationen vertraut machen, bevor Sie den Service nutzen, da sie Aspekte wie die Anforderungen an den Supportplan, den Onboarding-Prozess und die Mindestdauer des Abonnements abdecken.

- AWS Incident Detection and Response ist für direkte und von Partnern weiterverkaufte Enterprise Support-Konten verfügbar.
- AWS Incident Detection and Response ist für Konten beim partnergeführten Support nicht verfügbar.
- Sie müssen den AWS Enterprise Support während der Laufzeit Ihres Incident Detection and Response Service jederzeit aufrechterhalten. Weitere Informationen finden Sie unter [Enterprise Support](#). Die Kündigung des Enterprise Support führt zur gleichzeitigen Entfernung aus dem AWS Incident Detection and Response Service.
- Alle Workloads im Bereich AWS Incident Detection and Response müssen den Workload-Onboarding-Prozess durchlaufen.
- Die Mindestdauer, um ein Konto bei AWS Incident Detection and Response zu abonnieren, beträgt neunzig (90) Tage. Alle Stornierungsanfragen müssen dreißig (30) Tage vor dem geplanten Datum des Inkrafttretens der Kündigung eingereicht werden.
- AWS behandelt Ihre Daten wie in der [AWS Datenschutzerklärung](#) beschrieben.

Note

Fragen zur Abrechnung von Incident Detection and Response finden Sie [unter Hilfe bei der AWS Abrechnung](#).

Architektur der Erkennung und Reaktion auf Vorfälle

AWS Incident Detection and Response lässt sich in Ihre bestehende Umgebung integrieren, wie in der folgenden Grafik dargestellt. Die Architektur umfasst die folgenden Dienste:

- **Amazon EventBridge:** Amazon EventBridge dient als einziger Integrationspunkt zwischen Ihren Workloads und AWS Incident Detection and Response. Alarme werden über Amazon EventBridge mithilfe vordefinierter Regeln, die von verwaltet werden CloudWatch, von AWS Ihren Überwachungstools wie Amazon aufgenommen. Damit Incident Detection and Response die EventBridge Regel erstellen und verwalten kann, installieren Sie eine servicebezogene Rolle. Weitere Informationen zu diesen Diensten finden Sie unter [Was ist Amazon EventBridge und EventBridge Amazon-Regeln](#), [Was ist Amazon CloudWatch](#) und [Verwenden von serviceverknüpften Rollen](#). AWS Health
- **AWS Health:** AWS Health bietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer AWS-Services Konten. Incident Detection and Response dient AWS Health dazu, Ereignisse auf den von Ihren Workloads AWS-Services genutzten Workloads nachzuverfolgen und Sie zu benachrichtigen, wenn eine Warnung von Ihrem Workload eingeht. Weitere Informationen dazu finden Sie AWS Health unter [Was ist AWS Health](#).
- **AWS Systems Manager:** Systems Manager bietet eine einheitliche Benutzeroberfläche für die Automatisierung und Aufgabenverwaltung Ihrer AWS Ressourcen. AWS Incident Detection and Response speichert Informationen über Ihre Workloads, einschließlich Workload-Architekturdiagramme, Alarmdetails und die entsprechenden Runbooks für das Incident-Management in AWS Systems Manager Dokumenten (weitere Informationen finden Sie unter [AWS Systems Manager Dokumente](#)). Weitere Informationen dazu finden Sie AWS Systems Manager unter [Was ist](#). AWS Systems Manager
- **Ihre spezifischen Runbooks:** Ein Runbook für das Incident-Management definiert die Aktionen, die AWS Incident Detection and Response während des Incident Managements durchführt. Ihre spezifischen Runbooks teilen AWS Incident Detection and Response mit, an wen sie sich wenden können, wie sie Kontakt aufnehmen können und welche Informationen weitergegeben werden müssen.

Rollen und Verantwortlichkeiten bei der Erkennung und Reaktion auf Vorfälle

In der Tabelle Erkennung und Reaktion auf AWS Vorfälle RACI (verantwortlich, rechenschaftspflichtig, konsultiert und informiert) sind die Rollen und Zuständigkeiten für die verschiedenen Aktivitäten im Zusammenhang mit der Erkennung und Reaktion auf Vorfälle aufgeführt. Anhand dieser Tabelle lässt sich die Beteiligung des Kunden und des Teams für die Erkennung und Reaktion auf AWS Vorfälle bei Aufgaben wie Datenerfassung, Überprüfung der Betriebsbereitschaft, Kontokonfiguration, Störfallmanagement und Überprüfung nach dem Vorfall definieren.

Aktivität	Kunde	Erkennung und Reaktion auf Vorfälle
Erfassung von Daten		
Einführung in den Kunden und die Arbeitslast	Konsultiert	Verantwortlich
Architektur	Verantwortlich	Rechenschaftspflichtig
Operationen	Verantwortlich	Rechenschaftspflichtig
Legen Sie fest, welche CloudWatch Alarmer konfiguriert werden sollen	Verantwortlich	Rechenschaftspflichtig
Definieren Sie einen Plan zur Reaktion auf Vorfälle	Verantwortlich	Rechenschaftspflichtig

Aktivität	Kunde	Erkennung und Reaktion auf Vorfälle
Ausfüllen des Fragebogens zum Onboarding	Verantwortlich	Rechenschaftspflichtig
Überprüfung der Betriebsbereitschaft		
Führen Sie eine gut durchdachte Überprüfung (WAR) der Arbeitslast durch	Konsultiert	Verantwortlich
Überprüfen Sie die Reaktion auf Vorfälle	Konsultiert	Verantwortlich
Alarmmatrix validieren	Konsultiert	Verantwortlich
Identifizieren Sie die wichtigsten AWS Dienste, die vom Workload genutzt werden	Rechenschaftspflichtig	Verantwortlich
Konfiguration des Kontos		
IAMRolle im Kundenkonto erstellen	Verantwortlich	Informiert
Installieren Sie die verwaltete EventBridge Regel mithilfe der erstellten Rolle	Informiert	Verantwortlich
CloudWatch Alarme testen	Verantwortlich	Rechenschaftspflichtig
Stellen Sie sicher, dass Kundenalarme die Erkennung und Reaktion auf Vorfälle aktivieren	Informiert	Verantwortlich

Aktivität	Kunde	Erkennung und Reaktion auf Vorfälle
Alarme aktualisieren	Verantwortlich	Konsultiert
Runbooks aktualisieren	Konsultiert	Verantwortlich
Verwaltung von Zwischenfällen		
Melden Sie proaktiv Vorfälle, die durch Incident Detection and Response entdeckt wurden	Informiert	Verantwortlich
Reaktion auf Vorfälle bereitstellen	Informiert	Verantwortlich
Bereitstellung von Problembhebung/Wiederherstellung der Infrastruktur	Verantwortlich	Konsultiert
Überprüfung nach dem Vorfall		
Beantragen Sie eine Überprüfung nach dem Vorfall	Verantwortlich	Informiert
Führen Sie eine Überprüfung nach dem Vorfall durch	Informiert	Verantwortlich

Regionale Verfügbarkeit für Incident Detection and Response

AWS Incident Detection and Response ist derzeit auf Englisch und Japanisch für Enterprise Support-Konten verfügbar, die in einem der folgenden Länder gehostet werden AWS-Regionen:

Name	AWS-Region
us-east-1	USA Ost (Virginia)
us-east-2	USA Ost (Ohio)
us-west-1	USA West (Nordkalifornien)
us-west-2	USA West (Oregon)
ca-central-1	Kanada (Zentral)
ca-west-1*	Kanada West (Calgary)
sa-east-1	Südamerika (São Paulo)
eu-central-1	Europa (Frankfurt)
eu-west-1	Europa (Irland)
eu-west-2	Europa (London)
eu-west-3	Europa (Paris)
eu-north-1	Europa (Stockholm)
eu-central-2*	Europa (Zürich)
EU-Süd-1*	Europa (Milan)
EU-Süd-2*	Europa (Spain)
ap-south-1	Asien-Pazifik (Mumbai)
ap-northeast-1	Asien-Pazifik (Tokio)
ap-northeast-2	Asien-Pazifik (Seoul)
ap-southeast-1	Asien-Pazifik (Singapur)
ap-southeast-2	Asien-Pazifik (Sydney)

Name	AWS-Region
ap-ost-1*	Asien-Pazifik (Hongkong)
ap-nordost-3*	Asien-Pazifik (Osaka)
ap-Süd-2*	Asien-Pazifik (Hyderabad)
ap-Südost-3*	Asien-Pazifik (Jakarta)
ap-Südost-4*	Asien-Pazifik (Melbourne)
ap-Southeast-5*	Asien-Pazifik (Malaysia)
af-Süd-1*	Afrika (Kapstadt)
il-central-1*	Israel (Tel Aviv)
me-central-1*	Naher Osten () UAE
mir-Süd-1*	Naher Osten (Bahrain)

*Die daraus AWS-Region resultierenden Daten werden auf eine AWS-Region von Ihnen bevorzugte Weise verarbeitet, bevor sie an AWS Incident Detection and Response gesendet werden.

Erste Schritte mit Incident Detection and Response

Workloads und Alarme sind für die Erkennung und Reaktion auf AWS Vorfälle von zentraler Bedeutung. AWS arbeitet eng mit Ihnen zusammen, um spezifische Workloads zu definieren und zu überwachen, die für Ihr Unternehmen von entscheidender Bedeutung sind. AWS hilft Ihnen bei der Einrichtung von Alarmen, die Ihr Team schnell über erhebliche Leistungsprobleme oder Auswirkungen auf Kunden informieren. Richtig konfigurierte Alarme sind für die proaktive Überwachung und schnelle Reaktion auf Vorfälle im Rahmen von Incident Detection and Response unerlässlich.

Workloads

Mithilfe von Incident Detection and Response können Sie bestimmte Workloads für die Überwachung und das Management kritischer AWS Vorfälle auswählen. Ein Workload ist eine Sammlung von Ressourcen und Code, die zusammenarbeiten, um einen geschäftlichen Nutzen zu erzielen. Ein Workload kann aus allen Ressourcen und dem Code bestehen, aus denen Ihr Bankzahlungsportal oder ein Kundenbeziehungsmanagementsystem (CRM) besteht. Sie können einen Workload in einem einzelnen AWS Konto oder in mehreren AWS Konten hosten.

Beispielsweise könnten Sie eine monolithische Anwendung in einem einzigen Konto hosten (z. B. Employee Performance App im folgenden Diagramm). Oder Sie haben eine Anwendung (z. B. Storefront Webapp im Diagramm), die in Microservices aufgeteilt ist, die sich über verschiedene Konten erstrecken. Ein Workload kann Ressourcen, wie z. B. eine Datenbank, mit anderen Anwendungen oder Workloads gemeinsam nutzen, wie im Diagramm dargestellt.

Informationen zu den ersten Schritten mit dem Workload-Onboarding finden Sie unter [Workload-Onboarding und Fragebogen zum Workload-Onboarding](#).

Alarme

Alarme sind ein wichtiger Bestandteil von Incident Detection and Response, da sie Einblick in die Leistung Ihrer Anwendungen und der zugrunde liegenden Infrastruktur bieten. AWS arbeitet mit Ihnen zusammen, um geeignete Metriken und Alarmschwellenwerte zu definieren, die nur ausgelöst werden, wenn es kritische Auswirkungen auf Ihre überwachten Workloads gibt. Ziel ist es, dass Alarme die von Ihnen angegebenen Problemlöser einbeziehen, die dann mit dem Incident-

Management-Team zusammenarbeiten können, um Probleme schnell zu beheben. Alarme sollten so konfiguriert werden, dass sie nur dann in den Alarmstatus wechseln, wenn die Leistung oder das Kundenerlebnis erheblich beeinträchtigt sind und sofortige Maßnahmen erforderlich sind. Zu den wichtigsten Arten von Alarmen gehören Alarme, die auf geschäftliche Auswirkungen hinweisen, Amazon CloudWatch Canaries und aggregierte Alarme, die Abhängigkeiten überwachen.

[Informationen zu den ersten Schritten mit der Erfassung von Alarmen finden Sie unter Alarmeingang und Fragebogen zur Alarmerfassung.](#)

Note

Informationen zum Ändern Ihrer Runbooks, Workload-Informationen oder der im Rahmen von Incident Detection and Response überwachten Alarme finden Sie unterAWS. [Fragen Sie in Incident Detection and Response nach Änderungen an einem integrierten Workload](#)

Einführung in die Erkennung und Reaktion auf Vorfälle

AWS arbeitet mit Ihnen zusammen, um Ihre Workloads und Alarme in AWS Incident Detection and Response zu integrieren. Sie stellen wichtige Informationen zur Verfügung AWS in der[Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen in Incident Detection and Response](#). Es hat sich bewährt, dass Sie Ihre Workloads auch unter AppRegistry registrieren. Weitere Informationen finden Sie im [AppRegistry Benutzerhandbuch](#).

Das folgende Diagramm zeigt den Ablauf für das Onboarding von Workloads und die Erfassung von Alarmen in Incident Detection and Response:

Onboarding von Arbeitslasten

AWS Arbeitet beim Onboarding von Workloads mit Ihnen zusammen, um sich ein Bild von Ihrer Arbeitslast zu machen und herauszufinden, wie wir Sie bei Vorfällen und AWS Serviceereignissen unterstützen können. Sie stellen wichtige Informationen über Ihre Arbeitslast bereit, die Sie bei der Minderung der Auswirkungen unterstützen.

Die wichtigsten Ergebnisse:

- Allgemeine Informationen zur Arbeitslast

- Architekturdetails, einschließlich Diagrammen
- Runbook-Informationen
- Vom Kunden ausgelöste Vorfälle
- AWS Serviceereignisse

Einnahme von Alarmen

AWS arbeitet mit Ihnen zusammen, um Ihre Alarme zu integrieren. AWS Incident Detection and Response kann Alarme von Amazon CloudWatch und Tools zur Überwachung der Anwendungsleistung (APM) von Drittanbietern über Amazon EventBridge aufnehmen. Onboarding-Alarme ermöglichen eine proaktive Erkennung von Vorfällen und automatisiertes Eingreifen. Weitere Informationen finden Sie unter [Ingest-Alarme von APMs, die direkt mit Amazon EventBridge integriert sind](#).

Die wichtigsten Ausgaben:

- Alarmmatrix

In der folgenden Tabelle sind die Schritte aufgeführt, die erforderlich sind, um einen Workload in AWS Incident Detection and Response zu integrieren. In dieser Tabelle sind Beispiele für die Dauer der einzelnen Aufgaben aufgeführt. Die tatsächlichen Termine für jede Aufgabe werden auf der Grundlage der Verfügbarkeit Ihres Teams und Ihres Zeitplans definiert.

Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen in Incident Detection and Response

Auf dieser Seite finden Sie die Fragebögen, die Sie ausfüllen müssen, wenn Sie einen Workload in AWS Incident Detection and Response integrieren und wenn Sie Alarme für die Aufnahme in den Service konfigurieren. Der Fragebogen zum Onboarding von Workloads enthält allgemeine Informationen über Ihren Workload, dessen Architekturdetails und Ansprechpartner für die Reaktion auf Vorfälle. Im Fragebogen zur Erfassung von Alarmen geben Sie in Incident Detection and Response für Ihren Workload die kritischen Alarme an, die zur Entstehung von Vorfällen führen sollen. Außerdem geben Sie Runbook-Informationen darüber an, wer kontaktiert werden soll und welche Maßnahmen ergriffen werden sollten. Das korrekte Ausfüllen dieser Fragebögen ist ein

wichtiger Schritt bei der Einrichtung von Überwachungs- und Reaktionsprozessen für Ihre Workloads.
AWS

Laden Sie den Fragebogen zum [Onboarding von Workloads](#) herunter.

Laden Sie den Fragebogen zur [Erfassung von Alarmen herunter](#).

Fragebogen zum Onboarding zum Workload — Allgemeine Fragen




Allgemeine Fragen




Frage	Beispielantwort
Name des Unternehmens	Amazon Inc.
Name dieses Workloads (einschließlich aller Abkürzungen)	Amazon-Einzelhandelsgeschäfte (ARO)
Primärer Endbenutzer und die Funktion dieses Workloads.	Bei diesem Workload handelt es sich um eine E-Commerce-Anwendung, die es Endbenutzern ermöglicht, verschiedene Artikel zu kaufen. Dieser Workload ist der Hauptumsatzgenerator für unser Unternehmen.
Geltende Compliance- und/oder behördliche Anforderungen für diese Arbeitslast und alle Maßnahmen, die AWS nach einem Vorfall erforderlich sind.	Der Arbeitsaufwand bezieht sich auf Patientenakten, die sicher und vertraulich aufbewahrt werden müssen.

Fragebogen zum Onboarding der Arbeitslast — Fragen zur Architektur

Fragen zur Architektur

Frage	Beispielantwort
Eine Liste von AWS Ressourcen-Tags, die zur Definition von Ressourcen verwendet werden, die Teil dieser Arbeitslast sind. AWS verwendet diese Tags, um die Ressourcen	appName: Optimax Umgebung: Produktion

Frage	Beispielantwort
<p>dieses Workloads zu identifizieren, um den Support bei Vorfällen zu beschleunigen.</p> <div data-bbox="115 331 792 699" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Bei Tags muss die Groß- und Kleinschreibung beachtet werden. Wenn Sie mehrere Tags angeben, müssen alle von diesem Workload verwendeten Ressourcen dieselben Tags haben.</p></div>	
<p>Eine Liste der AWS Dienste, die von diesem Workload genutzt werden, sowie das AWS Konto und die Regionen, in denen sie sich befinden.</p> <div data-bbox="115 955 792 1176" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Erstellen Sie für jeden Dienst eine neue Zeile.</p></div>	<p>Route 53: Leitet den Internetverkehr an die weiterALB.</p> <p>Konto: 123456789101</p> <p>Region: US-1, US-2 EAST WEST</p>
<p>Eine Liste der AWS Dienste, die von diesem Workload genutzt werden, sowie das AWS Konto und die Regionen, in denen sie sich befinden.</p> <div data-bbox="115 1434 792 1654" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Erstellen Sie für jeden Dienst eine neue Zeile.</p></div>	<p>ALB: Leitet eingehenden Traffic an eine Zielgruppe von ECS Containern weiter.</p> <p>Konto: 123456789101</p> <p>Region: N/A</p>


Frage	Beispielantwort
<p>Eine Liste der AWS Dienste, die von diesem Workload genutzt werden, sowie das AWS Konto und die Regionen, in denen sie sich befinden.</p> <div data-bbox="115 447 792 667"><p> Note</p><p>Erstellen Sie für jeden Dienst eine neue Zeile.</p></div>	<p>ECS: Recheninfrastruktur für die Hauptflotte der Geschäftslogik. Verantwortlich für die Bearbeitung eingehender Benutzeranfragen und für Abfragen an die Persistenzschicht.</p> <p>Konto: 123456789101</p> <p>Region: US-1 EAST</p>
<p>Eine Liste der AWS Dienste, die von diesem Workload genutzt werden, sowie das AWS Konto und die Regionen, in denen sie sich befinden.</p> <div data-bbox="115 926 792 1146"><p> Note</p><p>Erstellen Sie für jeden Dienst eine neue Zeile.</p></div>	<p>RDS: Der Amazon Aurora Aurora-Cluster speichert Benutzerdaten, auf die über die ECS Geschäftslogikschicht zugegriffen wird.</p> <p>Konto: 123456789101</p> <p>Region: US-1 EAST</p>
<p>Eine Liste der AWS Dienste, die von diesem Workload genutzt werden, sowie das AWS Konto und die Regionen, in denen sie sich befinden.</p> <div data-bbox="115 1400 792 1621"><p> Note</p><p>Erstellen Sie für jeden Dienst eine neue Zeile.</p></div>	<p>S3: Speichert statische Inhalte der Website.</p> <p>Konto: 123456789101</p> <p>Region: N/A</p>
<p>Geben Sie alle Upstream-/Downstream-Komponenten an, die nicht integriert wurden und die sich bei einem Ausfall auf diese Arbeitslast auswirken könnten.</p>	<p>Authentifizierungs-Microservice: Verhindert, dass Benutzer ihre Gesundheitsdaten laden, da diese nicht authentifiziert werden.</p>

Frage	Beispielantwort
Gibt es On-Premise-Komponenten oder AWS Komponenten für diesen Workload? Falls ja, was sind sie und welche Funktionen werden ausgeführt?	Der gesamte ein-/ausgehende internetbasierte Datenverkehr AWS wird über unseren lokalen Proxy-Service geleitet.
Geben Sie Einzelheiten zu allen manuellen oder automatisierten Failover-/Disaster-Recovery-Plänen auf Availability Zone- und regionaler Ebene an.	Warmer Bereitschaftsmodus. Automatischer Failover auf WEST US-2 bei anhaltendem Rückgang der Erfolgsquote.

Fragebogen zum Onboarding von Workloads — Fragen zum AWS Service Event

AWS Fragen zu Serviceereignissen

Frage	Beispielantwort
Geben Sie die Kontaktdaten (Name/E-Mail/Telefon) des internen Teams für schwere Vorfälle/IT-Krisenmanagement Ihres Unternehmens an.	Team für das Management schwerer Vorfälle mim@example.com +61 2 3456 7890
Geben Sie Einzelheiten zu jeder statischen Brücke zwischen Vorfällen und Krisenmanagement an, die von Ihrem Unternehmen eingerichtet wurden. Wenn Sie nichtstatische Brücken verwenden, geben Sie Ihre bevorzugte Anwendung an und AWS wird diese Informationen bei einem Vorfall anfordern.	Amazon Chime https://chime.aws/1234567890


 **Note**

Wenn keine bereitgestellt wird, wird sich während eines Vorfalls mit AWS Ihnen in Verbindung setzen und Ihnen

Frage	Beispielantwort
eine Chime-Bridge zur Verfügung stellen, an der Sie teilnehmen können.	

Fragebogen zur Erfassung von Alarmen

Runbook-Fragen

Frage	Beispielantwort
<p>AWS wird im Rahmen des AWS Support Falls Ansprechpartner für die Arbeitslast ansprechen. Wer ist der Hauptansprechpartner, wenn ein Alarm für diese Arbeitslast ausgelöst wird?</p> <p>Geben Sie Ihre bevorzugte Konferenzanwendung an und AWS wird Sie bei einem Vorfall nach diesen Informationen fragen.</p> <div data-bbox="142 1165 181 1203" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 5px; display: inline-block;">  </div> Note Wenn keine bevorzugte Konferenzanwendung zur Verfügung gestellt wird, AWS wird sie sich während eines Vorfalls mit einer Chime-Bridge in Verbindung setzen, an der Sie teilnehmen können.	

Frage	Beispielantwort
	<p>+61 2 3456 7890</p> <p>2. Wenn nach 10 Minuten keine Antwort von John Smith vorliegt, wenden Sie sich an:</p> <p>Jane Smith - Betriebsleiterin</p> <p>jane.smith@example.com</p> <p>+61 2 3456 7890</p>
<p>AWS informiert während des gesamten Vorfalls in regelmäßigen Abständen über den Support-Fall über Updates. Gibt es weitere Ansprechpartner, die diese Updates erhalten sollten?</p>	<p>john.smith@example.com, jane.smith@example.com</p>

Alarmmatrix

Geben Sie die folgenden Informationen an, um die Gruppe von Alarmen zu identifizieren, die mithilfe von AWS Incident Detection and Response Vorfälle für Ihren Workload auslösen. Sobald die Techniker von AWS Incident Detection and Response Ihre Alarme überprüft haben, werden weitere Onboarding-Schritte durchgeführt.

AWSKriterien für die Erkennung und Reaktion auf kritische Alarme bei Vorfällen:

- AWSAlarme zur Erkennung und Reaktion auf Vorfälle sollten nur dann in den Status „Alarm“ übergehen, wenn erhebliche Auswirkungen auf die zu überwachende Arbeitslast (Umsatzeinbußen/Beeinträchtigung des Kundenerlebnisses) bestehen und sofortige Aufmerksamkeit des Bedieners erforderlich ist.
- AWSBei Alarmen zur Erkennung und Reaktion auf Vorfälle müssen außerdem Ihre für die Arbeitslast zuständigen Mitarbeiter gleichzeitig oder vor dem Einsatz eingeschaltet werden. AWS Incident Manager arbeiten bei der Schadensbegrenzung mit Ihren Problemlösern zusammen und agieren nicht als Ersthelfer, die dann an Sie weiterleiten.
- AWSDie Schwellenwerte für die Erkennung und Reaktion auf Alarme müssen auf einen angemessenen Schwellenwert und eine angemessene Dauer festgelegt werden, sodass bei jeder Auslösung eines Alarms eine Untersuchung durchgeführt werden muss. Wenn ein Alarm

zwischen dem Zustand „Alarm“ und „OK“ wechselt, ist die Wirkung so groß, dass die Reaktion und Aufmerksamkeit des Bedieners gewährleistet ist.

AWSRichtlinie zur Erkennung und Reaktion auf Vorfälle bei Verstößen gegen Kriterien:

Diese Kriterien können nur dann bewertet werden, wenn Ereignisse eintreten. case-by-case Das Incident-Management-Team arbeitet mit Ihren technischen Kundenbetreuern (TAMs) zusammen, um Alarme anzupassen und in seltenen Fällen die Überwachung zu deaktivieren, wenn der Verdacht besteht, dass Kundenalarme diese Kriterien nicht erfüllen und das Incident-Management-Team unnötig regelmäßig einbezieht.

Important

Geben Sie bei der Angabe von Kontaktadressen E-Mail-Adressen für die Gruppenverteilung an, sodass Sie das Hinzufügen und Löschen von Empfängern ohne Runbook-Updates kontrollieren können.

Geben Sie die Kontakttelefonnummer Ihres Site Reliability Engineering (SRE) -Teams an, wenn Sie möchten, dass das AWS Incident Detection and Response-Team das Team nach dem Senden einer ersten Kontakt-E-Mail anruft.

Alarmmatrixtabelle

Name der MetrikARN //Schwellenwert	Beschreibung	Hinweise	Angeforderte Aktionen
Umfang der Arbeitslast/ <i>CW Alarm ARN /</i> CallCount < 100.000 für 5 Datenpunkte innerhalb von 5 Minuten, fehlende Daten als fehlend behandeln	Diese Metrik stellt die Anzahl der eingehenden Anfragen für den Workload dar, gemessen auf Application Load Balancer Balancer-Ebene. Dieser Alarm ist wichtig, da ein erheblicher Rückgang	Der Alarm ist in der letzten Woche zehnmal in den Zustand „Alarm“ übergegangen. Bei diesem Alarm besteht die Gefahr von Fehlalarmen. Eine Überprüfung der Schwellenwerte ist geplant.	Wenden Sie sich an das Site Reliability Engineering-Team, indem Sie eine E-Mail an senden <i>SRE@xyz.com</i> Erstellen Sie eine AWS Premium-Supportanfrage für unsere ELB und Route 53-Services.

Name der MetrikARN //Schwellenwert	Beschreibung	Hinweise	Angeforderte Aktionen
	<p>der eingehenden Anfragen auf Probleme mit der Upstream-Netzwerkonnektivität oder auf Probleme mit unserer DNS Implementierung hinweisen kann, die dazu führen, dass Benutzer nicht auf den Workload zugreifen können.</p>	<p>Probleme? Nein oder Ja (wenn Nein, leer lassen): Dieser Alarm wird während der Ausführung eines bestimmten Batch-Jobs häufig ausgelöst.</p> <p>Problemlöser: Zuverlässigkeitsingenieure vor Ort</p>	<p>Falls IMMEDIATE Maßnahmen erforderlich sind: Aktivieren Sie die Option EC2 Freier Arbeitsspeicher/Festplatten und informieren Sie den XYZ. Führen Sie ein Team per E-Mail durch, um die Instanz neu zu starten, oder führen Sie eine Protokollbereinigung durch. (wenn kein sofortiges Eingreifen erforderlich ist, lassen Sie das Feld leer)</p>

Name der MetrikARN //Schwellenwert	Beschreibung	Hinweise	Angeforderte Aktionen
<p>Latenz bei Workload-Anfragen/ <i>CW Alarm ARN /</i> p90 Latenz > 100 ms für 5 Datenpunkte innerhalb von 5 Minuten, fehlende Daten als fehlend behandeln</p>	<p>Diese Metrik stellt die p90-Latenz für HTTP Anfragen dar, die durch den Workload erfüllt werden müssen.</p> <p>Dieser Alarm steht für die Latenz (ein wichtiges Maß für das Kundenerlebnis auf der Website).</p>	<p>Der Alarm ist in der letzten Woche 0 Mal in den Zustand „Alarm“ übergegangen.</p> <p>Probleme? Nein oder Ja (wenn Nein, leer lassen): Dieser Alarm wird während der Ausführung eines bestimmten Batch-Jobs häufig ausgelöst.</p> <p>Problemlöser: Zuverlässigkeitsingenieure vor Ort</p>	<p>Wenden Sie sich an das Site Reliability Engineering-Team, indem Sie eine E-Mail an senden <i>SRE@xyz.com</i></p> <p>Erstellen Sie eine AWS Premium-Supportanfrage für unsere und ECW RDS Services.</p> <p>Falls IMMEDIATE Maßnahmen erforderlich sind: Aktivieren Sie die Option EC2 Freier Arbeitsspeicher/Festplatten Speicher und informieren Sie die <i>XYZ</i>. Führen Sie ein Team per E-Mail durch, um die Instanz neu zu starten, oder führen Sie eine Protokollbereinigung durch. (wenn kein sofortiges Eingreifen erforderlich ist, lassen Sie das Feld leer)</p>

Name der MetrikARN //Schwellenwert	Beschreibung	Hinweise	Angeforderte Aktionen
<p>Verfügbarkeit der Workload-Anfrage/ <i>CW Alarm ARN /</i></p> <p>Verfügbarkeit < 95% für 5 Datenpunkte innerhalb von 5 Minuten, fehlende Daten werden als fehlend behandelt.</p>	<p>Diese Metrik gibt die Verfügbarkeit von HTTP Anfragen an, die vom Workload erfüllt werden müssen. (Anzahl von HTTP 200 /Anzahl der Anfragen) pro Zeitraum.</p> <p>Dieser Alarm steht für die Verfügbarkeit des Workloads.</p>	<p>Der Alarm ist in der letzten Woche 0 Mal in den Zustand „Alarm“ übergegangen.</p> <p>Probleme? Nein oder Ja (wenn Nein, leer lassen): Dieser Alarm wird während der Ausführung eines bestimmten Batch-Jobs häufig ausgelöst.</p> <p>Problemlöser: Zuverlässigkeitsingenieure vor Ort</p>	<p>Wenden Sie sich an das Site Reliability Engineering-Team, indem Sie eine E-Mail an senden SRE@xyz.com</p> <p>Erstellen Sie eine AWS Premium-Supportanfrage für unsere ELB und Route 53-Services.</p> <p>Falls IMMEDIATE Maßnahmen erforderlich sind: Aktivieren Sie die Option EC2 Freier Arbeitsspeicher/Festplatten Speicher und informieren Sie den <i>XYZ</i></p> <p>Führen Sie ein Team per E-Mail durch, um die Instanz neu zu starten, oder führen Sie eine Protokollbereinigung durch. (wenn kein sofortiges Eingreifen erforderlich ist, lassen Sie das Feld leer)</p>

Name der MetrikARN //Schwellenwert	Beschreibung	Hinweise	Angeforderte Aktionen
---------------------------------------	--------------	----------	-----------------------

Beispiel für New Relic Alarm

<p>Durchgängiger Integrationstest/ <i>CW Alarm ARN /</i></p> <p>Fehlerrate von 3% bei Messwerten von einer Minute über einen Zeitraum von 3 Minuten. Fehlende Daten werden als fehlend behandelt</p> <p>Workload-ID: End-to-End-Test-Workflow, AWS Region: EAST US-1, AWS Konto-ID: 012345678910</p>	<p>Diese Metrik testet, ob eine Anfrage jede Ebene des Workloads durchlaufen kann. Schlägt dieser Test fehl, stellt dies einen kritischen Fehler bei der Verarbeitung von Geschäftstransaktionen dar.</p> <p>Dieser Alarm steht für die Fähigkeit, Geschäftstransaktionen für den Workload zu verarbeiten.</p>	<p>Der Alarm ist in der letzten Woche 0 Mal in den Zustand „Alarm“ übergegangen.</p> <p>Probleme? Nein oder Ja (wenn Nein, leer lassen): Dieser Alarm wird während der Ausführung eines bestimmten Batch-Jobs häufig ausgelöst.</p> <p>Problemlöser: Zuverlässigkeitssingenieure vor Ort</p>	<p>Wenden Sie sich an das Site Reliability Engineering-Team, indem Sie eine E-Mail an senden <i>SRE@xyz.com</i></p> <p>Erstellen Sie eine AWS Premium-Supportanfrage für unsere ECS Dienste und DynamoDB.</p> <p>Falls IMMEDIATE Maßnahmen erforderlich sind: Aktivieren Sie die Option EC2 Freier Arbeitsspeicher/Festplatten Speicher und informieren Sie den <i>XYZ</i></p> <p>Führen Sie ein Team per E-Mail durch, um die Instanz neu zu starten, oder führen Sie eine Protokollbereinigung durch. (wenn kein sofortiges Eingreifen erforderlich ist, lassen Sie das Feld leer)</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Erkennung von Arbeitslasten bei der Erkennung und Reaktion auf Vorfälle

AWS arbeitet mit Ihnen zusammen, um so viel Kontext wie möglich über Ihren Workload zu erfahren. AWS Incident Detection and Response verwendet diese Informationen, um Runbooks zu erstellen, die Sie bei Vorfällen und AWS Serviceereignissen unterstützen. Die erforderlichen Informationen werden in der [Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen in Incident Detection and Response](#) erfasst. Es hat sich bewährt, Ihre Workloads auf AppRegistry zu registrieren. Weitere Informationen finden Sie im [AppRegistry Benutzerhandbuch](#).

Die wichtigsten Ausgaben:

- Workload-Informationen, wie z. B. die Beschreibung des Workloads, Architekturdiagramme, Kontakt- und Eskalationsdetails.
- Einzelheiten darüber, wie der Workload AWS Dienste in den einzelnen AWS Regionen nutzt.
- Spezifische Informationen darüber, wie wir Sie während einer Serviceveranstaltung AWS unterstützen.
- Von Ihrem Team verwendete Alarme zur Erkennung kritischer Auswirkungen auf die Arbeitslast.

Abonnieren Sie einen Workload für Incident Detection and Response

Um einen Workload für AWS Incident Detection and Response zu abonnieren, erstellen Sie für jeden Workload einen neuen Support-Fall. Beachten Sie bei der Erstellung des Support-Falls Folgendes:

- Um einen Workload zu integrieren, der sich in einem einzigen AWS Konto befindet, erstellen Sie den Support-Fall entweder über das Konto des Workloads oder über Ihr Zahlerkonto.
- Um einen Workload zu erstellen, der sich über mehrere AWS Konten erstreckt, erstellen Sie den Support-Fall von Ihrem Kostenträgerkonto aus. Führen Sie im Hauptteil des Support-Falls alle Konten auf, die Sie aufnehmen IDs möchten.

Important

Wenn Sie einen Support-Fall erstellen, um einen Workload vom falschen Konto aus für Incident Detection and Response zu abonnieren, kann es zu Verzögerungen kommen und

Sie müssen zusätzliche Informationen anfordern, bevor Ihre Workloads abonniert werden können.

Um einen Workload zu abonnieren

1. Gehen Sie zum [AWS Support Center](#) und wählen Sie dann Kundenvorgang erstellen aus, wie im folgenden Beispiel gezeigt. Sie können Workloads nur von Konten abonnieren, die für Enterprise Support registriert sind.
2. Füllen Sie das Support-Fallformular aus:
 - Wählen Sie Technischer Support aus.
 - Wählen Sie für Service die Option Incident Detection and Response aus.
 - Wählen Sie als Kategorie die Option Onboard New Workload aus.
 - Wählen Sie unter Schweregrad die Option Allgemeine Hinweise aus.
3. Geben Sie einen Betreff für diese Änderung ein. Beispielsweise:

[Onboard] Erkennung und Reaktion auf AWS Vorfälle - *workload_name*
4. Geben Sie eine Beschreibung für diese Änderung ein. Geben Sie beispielsweise „Diese Anfrage dient dazu, einen Workload für AWS Incident Detection and Response zu integrieren“ ein. Stellen Sie sicher, dass Ihre Anfrage die folgenden Informationen enthält:
 - Workload-Name: Ihr Workload-Name.
 - Konto-ID (s): ID1 ID2ID3,, usw. Dies sind die Konten, die Sie in AWS Incident Detection and Response einbinden möchten.
 - Startdatum des Abonnements: Das Datum, an dem Sie das Abonnement für AWS Incident Detection and Response starten möchten.
5. Geben Sie im Abschnitt Zusätzliche Kontakte — optional eine beliebige E-Mail-Adresse einIDs, an die Sie Informationen zu dieser Anfrage erhalten möchten.

Im Folgenden finden Sie ein Beispiel für den Abschnitt Zusätzliche Kontakte — optional:

⚠ Important

Wenn Sie IDs im Abschnitt **Zusätzliche Kontakte — optional** keine E-Mail hinzufügen, kann sich der Onboarding-Prozess für AWS Incident Detection and Response verzögern.

6. Wählen Sie Absenden aus.

Nachdem Sie die Anfrage eingereicht haben, können Sie weitere E-Mails von Ihrer Organisation hinzufügen. Um E-Mails hinzuzufügen, antworten Sie auf den Fall und fügen Sie dann die E-Mail IDs im Abschnitt **Zusätzliche Kontakte — optional** hinzu.

Im Folgenden finden Sie ein Beispiel für den Abschnitt **Zusätzliche Kontakte — optional**:

Nachdem Sie einen Supportfall für die Abonnementanfrage erstellt haben, halten Sie die folgenden beiden Dokumente bereit, um mit dem Onboarding-Prozess für den Workload fortzufahren:

- AWS Diagramm der Workload-Architektur.
- [Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen in Incident Detection and Response](#): Füllen Sie alle Informationen im Fragebogen aus, die sich auf die Arbeitslast beziehen, die Sie einarbeiten. Wenn Sie mehrere Workloads integrieren müssen, erstellen Sie für jeden Workload einen neuen Onboarding-Fragebogen. Wenn Sie Fragen zum Ausfüllen des Onboarding-Fragebogens haben, wenden Sie sich an Ihren Technical Account Manager (TAM).

📘 Note

NOTHängen Sie diese beiden Dokumente mithilfe der Option **Dateien anhängen** dem Fall bei. AWSDas Incident Detection and Response Team beantwortet den Fall mit einem Amazon Simple Storage Service Uploader-Link, über den Sie die Dokumente hochladen können.

Informationen darüber, wie Sie mit AWS Incident Detection and Response einen Fall erstellen, um Änderungen an einem vorhandenen integrierten Workload zu beantragen, finden Sie unter [Fragen Sie in Incident Detection and Response nach Änderungen an einem integrierten Workload](#)

Informationen zum Offboarding eines Workloads finden Sie unter. [Einen Workload aus Incident Detection and Response auslagern](#)

Definieren und konfigurieren Sie Alarme in Incident Detection and Response

AWS arbeitet mit Ihnen zusammen, um Metriken und Alarme zu definieren, um einen Überblick über die Leistung Ihrer Anwendungen und der zugrunde liegenden AWS Infrastruktur zu erhalten. Wir bitten darum, dass Alarme bei der Definition und Konfiguration von Schwellenwerten die folgenden Kriterien erfüllen:

- Alarme gehen nur dann in den Status „Alarm“ über, wenn es kritische Auswirkungen auf die überwachte Arbeitslast gibt (Umsatzverlust oder vermindertes Kundenerlebnis, wodurch die Leistung erheblich beeinträchtigt wird), die sofortige Aufmerksamkeit des Bedieners erfordern.
- Bei Alarmen müssen außerdem die von Ihnen angegebenen Resolver für die Arbeitslast aktiviert werden, und zwar gleichzeitig oder zuvor, indem das Incident-Management-Team eingeschaltet wird. Die Techniker für das Incident-Management sollten bei der Schadensbegrenzung mit den von Ihnen angegebenen Lösungskräften zusammenarbeiten und nicht als Ersthelfer fungieren und dann an Sie weiterleiten.
- Die Alarmschwellenwerte müssen auf einen angemessenen Schwellenwert und eine angemessene Dauer festgelegt werden, sodass bei jedem Auslösen eines Alarms eine Untersuchung durchgeführt werden muss. Wenn ein Alarm zwischen „Alarm“ und „OK“ wechselt, ist die Wirkung so groß, dass die Reaktion und Aufmerksamkeit des Bedieners gewährleistet ist.

Arten von Alarmen:

- Alarme, die das Ausmaß der Auswirkungen auf das Unternehmen aufzeigen und relevante Informationen zur einfachen Fehlererkennung weitergeben.
- CloudWatch Amazonas-Kanaren. [Weitere Informationen finden Sie unter Canaries and X-Ray Tracing und X-Ray.](#)
- Generelle Alarmierung (Überwachung von Abhängigkeiten)

Die folgende Tabelle enthält Beispielalarme, die alle das CloudWatch Überwachungssystem verwenden.

Name der Metrik//Alarmschwellenwert	Alarm ARN - oder Ressourcen-ID	Wenn dieser Alarm ausgelöst wird	Wenn Sie in Anspruch genommen werden, stellen Sie einen Premium-Supportfall für diese Services
APIFehler/ Anzahl der Fehler >= 10 für 10 Datenpunkte	arn:aws:cloudwatch:us-west-2:000000000000:alarm:E2 -Fehler MPmimLambda	Das Ticket wurde an das Datenbank administrator-Team () weitergeleitet DBA	Lambda, Gateway API
ServiceUnavailable (HTTP-Statuscode 503) Anzahl der Fehler >=3 für 10 Datenpunkte (verschiedene Clients) in einem 5-Minuten-Fenster	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	Das Ticket wurde an das Serviceteam am weitergeleitet	Lambda, Gateway API
ThrottlingException (HTTP-Statuscode 400)	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	Das Ticket wurde	EC2, Amazon Aurora

Name der Metrik//Alarmschwellenwert	Alarm ARN - oder Ressourcen-ID	Wenn dieser Alarm ausgelöst wird	Wenn Sie in Anspruch genommen werden, stellen Sie einen Premium-Supportfall für diese Services
Anzahl der Fehler ≥ 3 für 10 Datenpunkte (verschiedene Clients) in einem 5-Minuten-Fenster		an das Serviceteam weitergeleitet	

Weitere Details finden Sie unter [AWSÜberwachung und Beobachtbarkeit von Vorfällen bei der Erkennung und Reaktion](#).

Die wichtigsten Ergebnisse:

- Definition und Konfiguration von Alarmen für Ihre Workloads.
- Ausfüllen der Alarmdetails im Onboarding-Fragebogen.

Themen

- [Erstellen Sie in Incident Detection and Response CloudWatch Alarme, die Ihren Geschäftsanforderungen entsprechen](#)
- [Erstellen Sie CloudWatch Alarme in Incident Detection and Response mithilfe von Vorlagen CloudFormation](#)
- [Anwendungsbeispiele für CloudWatch Alarme im Bereich Incident Detection and Response](#)

Erstellen Sie in Incident Detection and Response CloudWatch Alarme, die Ihren Geschäftsanforderungen entsprechen

Wenn Sie CloudWatch Amazon-Alarme erstellen, können Sie mehrere Schritte unternehmen, um sicherzustellen, dass Ihre Alarme Ihren Geschäftsanforderungen am besten entsprechen.

Überprüfen Sie Ihre vorgeschlagenen CloudWatch Alarme

Prüfen Sie Ihre vorgeschlagenen Alarme, um sicherzustellen, dass sie nur dann in den Status „Alarm“ übergehen, wenn es kritische Auswirkungen auf die überwachte Arbeitslast gibt (Umsatzverlust oder vermindertes Kundenerlebnis, wodurch die Leistung erheblich beeinträchtigt wird). Halten Sie diesen Alarm beispielsweise für so wichtig, dass Sie sofort reagieren müssen, wenn er in den Status „Alarm“ übergeht?

Im Folgenden werden Metriken vorgeschlagen, die wichtige Auswirkungen auf Ihr Unternehmen haben könnten, z. B. die Auswirkungen auf die Erfahrung Ihrer Endbenutzer mit einer Anwendung:

- CloudFront: Weitere Informationen finden Sie unter [Metriken zu Funktionen anzeigen CloudFront und bearbeiten](#).
- Application Load Balancers: Es hat sich bewährt, wenn möglich die folgenden Alarme für Application Load Balancers zu erstellen:
 - HTTPCode_5xx_Count ELB
 - HTTPCode_Ziel_5xx_Anzahl

Die oben genannten Alarme ermöglichen es Ihnen, Antworten von Zielen zu überwachen, die sich hinter dem Application Load Balancer oder hinter anderen Ressourcen befinden. Dadurch ist es einfacher, die Ursache von 5XX-Fehlern zu identifizieren. Weitere Informationen finden Sie unter [CloudWatch Metriken für Ihren Application Load Balancer](#).

- Amazon API Gateway: Wenn Sie Elastic Beanstalk verwenden, sollten Sie die Verwendung der folgenden Metriken WebSocket API in Betracht ziehen:
 - Fehlerraten bei der Integration (gefiltert auf 5XX Fehler)
 - Latenz bei der Integration
 - Ausführungsfehler

Weitere Informationen finden Sie unter [Überwachung der WebSocket API Ausführung anhand von CloudWatch Metriken](#).

- Amazon Route 53: Überwachen Sie die EndPointUnhealthyENICountMetrik. Diese Metrik gibt die Anzahl der Elastic Network-Schnittstellen mit dem Status Automatische Wiederherstellung an. Dieser Status weist auf Versuche des Resolvers hin, eine oder mehrere der Amazon Virtual Private Cloud Cloud-Netzwerkschnittstellen wiederherzustellen, die dem Endpunkt zugeordnet sind (angegeben durch EndpointId). Während des Wiederherstellungsprozesses funktioniert der Endpunkt mit begrenzter Kapazität. Der Endpunkt kann DNS Abfragen erst verarbeiten, wenn er vollständig wiederhergestellt ist. Weitere Informationen finden Sie unter [Überwachung von Route 53 53-Resolver-Endpunkten mit Amazon CloudWatch](#).

Überprüfen Sie Ihre Alarmkonfigurationen

Nachdem Sie sich vergewissert haben, dass Ihre vorgeschlagenen Alarme Ihren Geschäftsanforderungen entsprechen, überprüfen Sie die Konfiguration und den Verlauf der Alarme:

- Überprüfen Sie den Schwellenwert für die Metrik, um in den Status „Alarm“ überzugehen, anhand des Trenddiagramms der Metrik.
- Überprüfen Sie den Zeitraum, der für die Abfrage von Datenpunkten verwendet wurde. Das Abfragen von Datenpunkten nach 60 Sekunden hilft bei der Früherkennung von Vorfällen.
- Überprüfen Sie die DatapointToAlarmKonfiguration. In den meisten Fällen hat es sich bewährt, diesen Wert auf 3 von 3 oder 5 von 5 zu setzen. Bei einem Vorfall wird der Alarm nach 3 Minuten ausgelöst, wenn er auf [60-Sekunden-Metriken mit 3 von 3 DatapointToAlarm] eingestellt ist, oder nach 5 Minuten, wenn er auf [60-Sekunden-Metriken mit 5 von 5 DatapointToAlarm] eingestellt ist. Verwenden Sie diese Kombination, um laute Alarme zu vermeiden.

Note

Die obigen Empfehlungen können je nachdem, wie Sie einen Dienst nutzen, variieren. Jeder AWS Dienst arbeitet innerhalb einer Arbeitslast unterschiedlich. Und derselbe Dienst kann unterschiedlich funktionieren, wenn er an mehreren Orten verwendet wird. Sie müssen sicher sein, dass Sie verstehen, wie Ihr Workload die Ressourcen nutzt, die den Alarm auslösen, sowie die vor- und nachgelagerten Auswirkungen.

Überprüfen Sie, wie Ihre Alarme mit fehlenden Daten umgehen

Einige Metrikquellen senden Daten nicht CloudWatch in regelmäßigen Abständen an. Für diese Metriken hat es sich bewährt, fehlende Daten als zu behandeln notBreaching. Weitere Informationen finden Sie unter [Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarme](#) und [Vermeidung vorzeitiger Übergänge in den Alarmzustand](#).

Wenn eine Metrik beispielsweise eine Fehlerrate überwacht und es keine Fehler gibt, dann meldet die Metrik keine Datenpunkte (Null). Wenn Sie den Alarm so konfigurieren, dass er fehlende Daten als Fehlend behandelt, führt ein einziger Datenpunkt, bei dem eine Verletzung vorliegt, gefolgt von zwei Datenpunkten ohne Daten (Null) dazu, dass die Metrik in den Status „Alarm“ wechselt (für 3 von 3 Datenpunkten). Das liegt daran, dass die Konfiguration für fehlende Daten den letzten bekannten Datenpunkt im Bewertungszeitraum auswertet.

In Fällen, in denen Metriken die Fehlerrate messen, können Sie ohne Leistungseinbußen davon ausgehen, dass das Fehlen von Daten eine gute Sache ist. Es hat sich bewährt, fehlende Daten notBreachingso zu behandeln, dass fehlende Daten als „OK“ behandelt werden und die Metrik nicht an einem einzelnen Datenpunkt in den Status „Alarm“ übergeht.

Überprüfen Sie den Verlauf jedes Alarms

Wenn aus der Historie eines Alarms hervorgeht, dass er häufig in den Status „Alarm“ wechselt und sich dann schnell wieder erholt, kann der Alarm zu einem Problem für Sie werden. Stellen Sie sicher, dass Sie den Alarm so einstellen, dass Geräusche oder Fehlalarme vermieden werden.

Überprüfen Sie die Metriken für die zugrunde liegenden Ressourcen

Stellen Sie sicher, dass Ihre Metriken valide zugrunde liegende Ressourcen berücksichtigen und die richtigen Statistiken verwenden. Wenn ein Alarm so konfiguriert ist, dass er ungültige Ressourcennamen überprüft, kann der Alarm die zugrunde liegenden Daten möglicherweise nicht verfolgen. Dies kann dazu führen, dass der Alarm in den Status „Alarm“ übergeht.

Erstellen Sie zusammengesetzte Alarme

Wenn Sie den Abteilungen Incident Detection and Response eine große Anzahl von Alarmen für das Onboarding zur Verfügung stellen, werden Sie möglicherweise aufgefordert, zusammengesetzte Alarme zu erstellen. Kombinierte Alarme reduzieren die Gesamtzahl der Alarme, die integriert werden müssen.

Erstellen Sie CloudWatch Alarme in Incident Detection and Response mithilfe von Vorlagen CloudFormation

Um die Einführung in AWS Incident Detection and Response zu beschleunigen und den Aufwand für die Erstellung von Alarmen zu reduzieren, AWS stellt Ihnen dieses Tool AWS CloudFormation Vorlagen zur Verfügung. Diese Vorlagen enthalten optimierte Alarmeinstellungen für häufig integrierte Dienste wie Application Load Balancer, Network Load Balancer und Amazon. CloudFront


Erstellen Sie Alarme mit Vorlagen CloudWatch CloudFormation

1. Laden Sie über die bereitgestellten Links eine Vorlage herunter:

NameSpace	Metriken	ComparisonOperator (Schwellenwert)	Intervall	DatapointsToAlarm	TreatMissingData	Statistik	Link zur Vorlage
Anwendung Elastic Load Balancer	(m1+m2)/ (m1+m2+m4) *100 m1= _ZIEL_2XX _Anzahl m2= _ZIEL_3XX _Anzahl m3= _ZIEL_4XX _Anzahl m4= _ZIEL_5XX _Anzahl HTTPCode HTTPCode	LessThanThreshold(95)	60	3 von 3	fehlt	Summe	Vorlage

NameSpace	Metriken	ComparisonOperator (Schwellenwert)	Intervall	DatapointsToAlarm	TreatMissingData	Statistik	Link zur Vorlage
	HTTPCode HTTPCode						
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3 von 3	notBreaching	Durchschnitt	Vorlage
Anwendung Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 von 3	notBreaching	Maximum	Vorlage
Elastic Load Balancer für Netzwerke	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 von 3	notBreaching	Maximum	Vorlage

- Überprüfen Sie die heruntergeladene JSON Datei, um sicherzustellen, dass sie den Betriebs- und Sicherheitsprozessen Ihres Unternehmens entspricht.
- Erstellen Sie einen CloudFormation Stapel:

 Note

Die folgenden Schritte verwenden den Standardprozess zur Erstellung von CloudFormation Stacks. Ausführliche Schritte finden Sie unter [Einen Stack auf der AWS CloudFormation Konsole](#) erstellen.

- Öffnen Sie die AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation>.
- Wählen Sie Stack erstellen aus.

- c. Wählen Sie „Vorlage ist bereit“ und laden Sie dann die Vorlagendatei aus Ihrem lokalen Ordner hoch.

Im Folgenden finden Sie ein Beispiel für den Bildschirm „Stapel erstellen“.

- d. Wählen Sie Weiter.
 - e. Geben Sie die folgenden erforderlichen Informationen ein:
 - AlarmNameConfig und AlarmDescriptionConfig: Geben Sie einen Namen und eine Beschreibung für Ihren Alarm ein.
 - ThresholdConfig: Passen Sie den Schwellenwert an die Anforderungen Ihrer Anwendung an.
 - DistributionIDConfig: Stellen Sie sicher, dass die Verteilungs-ID auf die richtigen Ressourcen in dem Konto verweist, in dem Sie den AWS CloudFormation Stack erstellen.
 - f. Wählen Sie Weiter.
 - g. Überprüfen Sie die Standardwerte in den DatapointsToAlarmConfigFeldern PeriodConfigEvaluationPeriodConfig, und. Es hat sich bewährt, die Standardwerte für diese Felder zu verwenden. Sie können bei Bedarf Anpassungen vornehmen, um die Anforderungen Ihrer Anwendung zu erfüllen.
 - h. Geben Sie optional nach Bedarf Tags und SNS Benachrichtigungsinformationen ein. Es hat sich bewährt, den Kündigungsschutz zu aktivieren, um ein versehentliches Löschen des Alarms zu verhindern. Um den Kündigungsschutz zu aktivieren, wählen Sie das Optionsfeld Aktiviert aus, wie im folgenden Beispiel gezeigt:
 - i. Wählen Sie Weiter.
 - j. Überprüfen Sie Ihre Stack-Einstellungen und wählen Sie dann Stack erstellen aus.
 - k. Nachdem Sie den Stack erstellt haben, wird der Alarm in der CloudWatch Amazon-Alarm-Liste aufgeführt, wie im folgenden Beispiel gezeigt:
4. Nachdem Sie alle Ihre Alarme im richtigen Konto und in der richtigen AWS Region erstellt haben, benachrichtigen Sie Ihren Technical Account Manager (TAM). Das AWS Incident Detection and Response Team überprüft den Status Ihrer neuen Alarme und setzt dann Ihr Onboarding fort.

Anwendungsbeispiele für CloudWatch Alarme im Bereich Incident Detection and Response

Die folgenden Anwendungsfälle bieten Beispiele dafür, wie Sie CloudWatch Amazon-Alarme in Incident Detection and Response verwenden können. Diese Beispiele zeigen, wie CloudWatch Alarme so konfiguriert werden können, dass sie wichtige Kennzahlen und Schwellenwerte für verschiedene AWS Dienste überwachen, sodass Sie potenzielle Probleme identifizieren und darauf reagieren können, die sich auf die Verfügbarkeit und Leistung Ihrer Anwendungen und Workloads auswirken könnten.

Beispiel für Anwendungsfall A: Application Load Balancer

Sie können den folgenden CloudWatch Alarm erstellen, der auf mögliche Auswirkungen auf die Arbeitslast hinweist. Zu diesem Zweck erstellen Sie eine metrische Mathematik, die einen Alarm ausgibt, wenn erfolgreiche Verbindungen einen bestimmten Schwellenwert unterschreiten. Die verfügbaren CloudWatch Metriken finden Sie unter [CloudWatch Metriken für Ihren Application Load Balancer](#)

Metrik:

```
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/Anwendung ELB

ComparisonOperator(Schwellenwert): Weniger als x (x = Schwellenwert des Kunden).

Zeitraum: 60 Sekunden

DatapointsToAlarm: 3 von 3

Behandlung fehlender Daten: Behandeln Sie fehlende Daten als [Sicherheitsverletzung](#).

Statistik: Summe

Das folgende Diagramm zeigt den Ablauf für Anwendungsfall A:

Beispiel für einen Anwendungsfall B: Amazon API Gateway

Sie können den folgenden CloudWatch Alarm erstellen, der auf mögliche Auswirkungen auf die Arbeitslast hinweist. Zu diesem Zweck erstellen Sie eine zusammengesetzte Metrik, die bei hoher

Latenz oder einer hohen durchschnittlichen Anzahl von 4XX-Fehlern im Gateway einen Alarm ausgibt. API Die verfügbaren Metriken finden Sie unter [Amazon API Gateway-Dimensionen und -Metriken](#)

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

NameSpace: AWS/APIGateway

ComparisonOperator(Schwellenwert): Größer als (x- oder y-Schwellenwerte des Kunden)

Zeitraum: 60 Sekunden

DatapointsToAlarm: 1 von 1

Behandlung fehlender Daten: Behandeln Sie fehlende Daten als [nicht verletzend](#).

Statistik:

Das folgende Diagramm zeigt den Ablauf für Anwendungsfall B:

Beispiel für Anwendungsfall C: Amazon Route 53

Sie können Ihre Ressourcen überwachen, indem Sie Route 53-Zustandsprüfungen erstellen, bei denen Rohdaten gesammelt und CloudWatch zu lesbaren Metriken nahezu in Echtzeit verarbeitet werden. Sie können den folgenden CloudWatch Alarm erstellen, der auf mögliche Auswirkungen auf die Arbeitslast hinweist. Sie können die CloudWatch Metriken verwenden, um einen Alarm zu erstellen, der ausgelöst wird, wenn der festgelegte Schwellenwert überschritten wird. Die verfügbaren CloudWatch Metriken finden Sie unter [CloudWatch Metriken für Route 53-Zustandsprüfungen](#)

Metrik: R53-HC-Success

NameSpace: AWS/Route 53

Schwellenwert HealthCheckStatus: HealthCheckStatus < x für 3 Datenpunkte innerhalb von 3 Minuten (entspricht dem Schwellenwert von x beim Kunden)

Zeitraum: 1 Minute

DatapointsToAlarm: 3 von 3

Behandlung fehlender Daten: Behandeln Sie fehlende Daten als [Sicherheitsverletzung](#).

Statistik: Minimum

Das folgende Diagramm zeigt den Ablauf für Anwendungsfall C:

Beispiel für einen Anwendungsfall D: Überwachen Sie einen Workload mit einer benutzerdefinierten App

In diesem Szenario ist es wichtig, dass Sie sich die Zeit nehmen, einen geeigneten Gesundheitscheck zu definieren. Wenn Sie nur überprüfen, ob der Port einer Anwendung geöffnet ist, haben Sie nicht überprüft, ob die Anwendung funktioniert. Darüber hinaus ist ein Aufruf der Startseite einer Anwendung nicht unbedingt der richtige Weg, um festzustellen, ob die App funktioniert. Wenn eine Anwendung beispielsweise sowohl von einer Datenbank als auch von Amazon Simple Storage Service (Amazon S3) abhängt, muss der Health Check alle Elemente validieren. Eine Möglichkeit, dies zu tun, besteht darin, eine Monitoring-Webseite wie /monitor zu erstellen. Die Überwachungswebseite ruft die Datenbank auf, um sicherzustellen, dass sie eine Verbindung herstellen und Daten abrufen kann. Und die Monitoring-Webseite ruft Amazon S3 auf. Anschließend verweisen Sie bei der Integritätsprüfung auf dem Load Balancer auf die Seite /monitor.

Das folgende Diagramm zeigt den Ablauf für Anwendungsfall D:

Alarmer in AWS Incident Detection and Response aufnehmen

[AWS Incident Detection and Response unterstützt die Erfassung von Alarmen über Amazon EventBridge](#) In diesem Abschnitt wird beschrieben, wie AWS Incident Detection and Response mit verschiedenen Tools zur Überwachung der Anwendungsleistung (APM), einschließlich Amazon CloudWatch, APMs mit direkter Integration mit Amazon EventBridge (z. B. Datadog und New Relic) und APMs ohne direkte Integration mit Amazon integriert werden kann. EventBridge Eine vollständige Liste APMs mit direkter Integration in Amazon finden Sie unter EventBridge [EventBridgeAmazon-Integrationen](#).

Themen

- [Bereitstellen des Zugriffs für die Erfassung von Warnmeldungen auf Incident Detection and Response](#)
- [Integrieren Sie Incident Detection and Response mit Amazon CloudWatch](#)
- [Erfassen Sie Alarme von APMs denen, die direkt mit Amazon integriert sind EventBridge](#)
- [Beispiel: Integrieren Sie Benachrichtigungen von Datadog und Splunk](#)

- [Verwenden Sie Webhooks, um Alarme APMs ohne direkte Integration mit Amazon aufzunehmen EventBridge](#)

Bereitstellen des Zugriffs für die Erfassung von Warnmeldungen auf Incident Detection and Response

Damit AWS Incident Detection and Response Alarme aus Ihrem Konto aufnehmen kann, installieren Sie die `AWSServiceRoleForHealth_EventProcessor` dienstbezogene Rolle (). SLR AWS geht davon aus, dass eine von Amazon EventBridge verwaltete Regel erstellt wird. Die verwaltete Regel sendet Benachrichtigungen von Ihren Konten an AWS Incident Detection and Response. Informationen dazu, einschließlich der zugehörigen AWS verwalteten Richtlinie, finden Sie im AWS Health Benutzerhandbuch [unter Verwenden von dienstbezogenen Rollen](#).

Sie können diese dienstverknüpfte Rolle in Ihrem Konto installieren, indem Sie den Anweisungen im Benutzerhandbuch unter [Serviceverknüpfte Rolle erstellen](#) folgen. AWS Identity and Access Management Sie können auch den folgenden Befehl der AWS Befehlszeilenschnittstelle (AWSCLI) verwenden:

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

Wichtige Ausgaben

- Erfolgreiche Installation der serviceverknüpften Rolle in Ihrem Konto.

Ähnliche Informationen

Weitere Informationen finden Sie unter den folgenden Themen:

- [Verwenden von serviceverknüpften Rollen für Health AWS](#)
- [Eine dienstbezogene Rolle erstellen](#)
- [AWSverwaltete Richtlinie: AWSHealth_EventProcessorServiceRolePolicy](#)

Integrieren Sie Incident Detection and Response mit Amazon CloudWatch

AWS Incident Detection and Response verwendet die serviceverknüpfte Rolle (SLR), die Sie bei der Zugriffsbereitstellung aktiviert haben, um eine von Amazon EventBridge verwaltete Regel in Ihrem

AWS Konto mit dem Namen zu erstellen. `AWSHealthEventProcessor-D0-NOT-DELETE` Incident Detection and Response verwendet diese Regel, um CloudWatch Amazon-Alarme von Ihren Konten aufzunehmen. Zusätzliche Schritte sind nicht erforderlich, um Alarme von zu empfangen. CloudWatch

Erfassen Sie Alarme von APMs denen, die direkt mit Amazon integriert sind EventBridge

Die folgende Abbildung zeigt den Prozess für das Senden von Benachrichtigungen an AWS Incident Detection and Response von Tools zur Überwachung der Anwendungsleistung (APM), die direkt mit Amazon integriert sind EventBridge, wie Datadog und Splunk. Eine vollständige Liste mit denen, mit APMs denen eine direkte Integration möglich ist EventBridge, finden Sie unter [EventBridge Amazon-Integrationen](#).

Gehen Sie wie folgt vor, um die Integration mit AWS Incident Detection and Response einzurichten. Bevor Sie diese Schritte ausführen, stellen Sie sicher, dass die AWS dienstverknüpfte Rolle (SLR) `AWSServiceRoleForHealth_EventProcessor` in Ihren Konten [installiert](#) ist.

Richten Sie die Integration mit AWS Incident Detection and Response ein

Sie müssen die folgenden Schritte für jedes AWS Konto und jede AWS Region ausführen. Benachrichtigungen müssen von dem AWS Konto und der AWS Region stammen, in der sich die Anwendungsressourcen befinden.

1. Richten Sie jede Ihrer Eventquellen APMs als EventBridge Amazon-Partner ein (z. B. `aws.partner/my_apm/integrationName`). Richtlinien zur Einrichtung Ihrer APM als Eventquelle finden Sie unter [Empfangen von Ereignissen von einem SaaS-Partner mit Amazon EventBridge](#). Dadurch wird ein Partner-Event-Bus in Ihrem Konto erstellt.
2. Führen Sie eine der folgenden Aktionen aus:
 - (Empfohlene Methode) Erstellen Sie einen benutzerdefinierten EventBridge Event-Bus. AWS Incident Detection and Response installiert einen verwalteten Regelbus (`AWSHealthEventProcessorEventSource-D0-NOT-DELETE`) über den `AWSServiceRoleForHealth_EventProcessorSLR`. Die Regelquelle ist der benutzerdefinierte Ereignisbus. Das Regelziel ist AWS Incident Detection and Response. Die Regel entspricht dem Muster für die Erfassung von APM Ereignissen von Drittanbietern.
 - (Alternative Methode) Verwenden Sie den Standard-Event-Bus anstelle eines benutzerdefinierten Event-Busses. Der Standardereignisbus erfordert, dass die verwaltete Regel APM Warnmeldungen an AWS Incident Detection and Response sendet.

3. Erstellen Sie eine [AWS Lambda](#)Funktion (z. B. `My_APM-AWSIncidentDetectionResponse-LambdaFunction`), um Ihre Event-Bus-Events für Partner zu transformieren. Die transformierten Ereignisse entsprechen der verwalteten Regel `AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
 - a. Transformierte Ereignisse enthalten eine eindeutige Kennung für AWS Incident Detection and Response und legen die Quelle und den Detailtyp des Ereignisses auf die erforderlichen Werte fest. Das Muster entspricht der verwalteten Regel.
 - b. Setzen Sie das Ziel der Lambda-Funktion entweder auf den in Schritt 2 erstellten benutzerdefinierten Eventbus (empfohlene Methode) oder auf Ihren Standard-Eventbus.
4. Erstellen Sie eine EventBridge Regel und definieren Sie die Ereignismuster, die der Liste der Ereignisse entsprechen, die Sie an AWS Incident Detection and Response weiterleiten möchten. Die Quelle der Regel ist der Partner-Event-Bus, den Sie in Schritt 1 definieren (z. B. `integrationName aws.partner/my_apm/`). Das Ziel der Regel ist die Lambda-Funktion, die Sie in Schritt 3 definieren (z. B. `My_APM-AWSIncidentDetectionResponse-LambdaFunction`). Richtlinien zur Definition Ihrer EventBridge Regel finden Sie unter [EventBridge Amazon-Regeln](#).

Beispiele für die Einrichtung einer Partner-Event-Bus-Integration zur Verwendung mit AWS Incident Detection and Response finden Sie unter [Beispiel: Integrieren Sie Benachrichtigungen von Datadog und Splunk](#)

Beispiel: Integrieren Sie Benachrichtigungen von Datadog und Splunk

Dieses Beispiel enthält detaillierte Schritte zur Integration von Benachrichtigungen von Datadog und Splunk in Incident Detection and Response. AWS

Themen

- [Schritt 1: Richten Sie Ihre APM als Eventquelle in Amazon ein EventBridge](#)
- [Schritt 2: Erstellen Sie einen benutzerdefinierten Event-Bus](#)
- [Schritt 3: Erstellen Sie eine AWS Lambda Funktion für die Transformation](#)
- [Schritt 4: Erstellen Sie eine benutzerdefinierte EventBridge Amazon-Regel](#)

Schritt 1: Richten Sie Ihre APM als Eventquelle in Amazon ein EventBridge

Richten Sie jede von Ihnen APMs als Eventquelle bei Amazon EventBridge in Ihrem AWS Konto ein. Anweisungen zur Einrichtung Ihres Tools APM als Eventquelle finden Sie in den [Anweisungen zur Einrichtung der Eventquelle für Ihr Tool bei EventBridge Amazon-Partnern](#).

Wenn Sie Ihr Event APM als Quelle einrichten, können Sie Benachrichtigungen von Ihrem Bus APM zu einem Event in Ihr AWS Konto aufnehmen. Nach der Einrichtung kann AWS Incident Detection and Response den Incident-Management-Prozess starten, wenn der Event-Bus ein Ereignis empfängt. Dieser Vorgang fügt Amazon EventBridge als Ziel zu Ihrem hinzuAPM.

Schritt 2: Erstellen Sie einen benutzerdefinierten Event-Bus

Es hat sich bewährt, einen benutzerdefinierten Eventbus zu verwenden. AWSIncident Detection and Response verwendet den benutzerdefinierten Event-Bus, um transformierte Ereignisse aufzunehmen. Eine AWS Lambda Funktion transformiert das Eventbus-Ereignis des Partners und sendet es an den benutzerdefinierten Event-Bus. AWSIncident Detection and Response installiert eine verwaltete Regel, um Ereignisse aus dem benutzerdefinierten Eventbus aufzunehmen.

Sie können den Standard-Event-Bus anstelle eines benutzerdefinierten Event-Busses verwenden. AWSBei Incident Detection and Response wird die verwaltete Regel dahingehend geändert, dass sie aus dem standardmäßigen Ereignisbus statt aus einem benutzerdefinierten Ereignisbus aufgenommen wird.

Erstellen Sie in Ihrem AWS Konto einen benutzerdefinierten Event-Bus:

1. Öffnen Sie die EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/>
2. Wählen Sie Busse, Eventbus.
3. Wählen Sie unter Benutzerdefinierter Eventbus die Option Erstellen aus.
4. Geben Sie unter Name einen Namen für Ihren Event-Bus ein. Das empfohlene Format ist APMName- AWSIncidentDetectionResponse - EventBus.

Verwenden Sie beispielsweise eine der folgenden Optionen, wenn Sie Datadog oder Splunk verwenden:

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

Schritt 3: Erstellen Sie eine AWS Lambda Funktion für die Transformation

Die Lambda-Funktion transformiert Ereignisse zwischen dem Partner-Event-Bus in Schritt 1 und dem benutzerdefinierten (oder standardmäßigen) Event-Bus aus Schritt 2. Die Lambda-Funktionstransformation entspricht der verwalteten Regel für AWS Incident Detection and Response.

Erstellen Sie eine AWS Lambda Funktion in Ihrem Konto AWS

1. Öffnen Sie die [Seite Funktionen](#) auf der AWS Lambda Konsole.
2. Wählen Sie Funktion erstellen aus.
3. Wählen Sie die Registerkarte Autor von Grund auf neu.
4. Geben Sie unter Funktionsname einen Namen im folgenden Format einAPMName-AWSIncidentDetectionResponse-LambdaFunction.

Im Folgenden finden Sie Beispiele für Datadog und Splunk:

- Datadog: Datadog-AWSIncidentDetectionResponse-LambdaFunction
 - Splunk: Splunk-AWSIncidentDetectionResponse-LambdaFunction
5. Geben Sie für Runtime Python 3.10 ein.
 6. Behalten Sie die Standardwerte für die übrigen Felder bei. Wählen Sie Funktion erstellen aus.
 7. Ersetzen Sie auf der Codebearbeitungsseite den standardmäßigen Lambda-Funktionsinhalt durch die Funktion in den folgenden Codebeispielen.

Beachten Sie die Kommentare, die in den folgenden Codebeispielen mit # beginnen. Diese Kommentare geben an, welche Werte geändert werden müssen.

Vorlage für den Datadog-Transformationscode:

```
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'])
```

Code-Vorlage für die Splunk-Transformation:

```
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-identifler"] 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-identifler"] = 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. Wählen Sie Bereitstellen.
9. Fügen Sie der Lambda-Ausführungsrolle die PutEventsBerechtigung für den Event-Bus hinzu, an den Sie die transformierten Daten senden:
 - a. Öffnen Sie die [Seite „Funktionen“](#) in der AWS Lambda Konsole.
 - b. Wählen Sie die Funktion und dann auf der Registerkarte Konfiguration die Option Berechtigungen aus.
 - c. Wählen Sie unter Ausführungsrolle den Rollennamen aus, um die Ausführungsrolle in der AWS Identity and Access Management Konsole zu öffnen.
 - d. Wählen Sie unter Berechtigungsrichtlinien den Namen der vorhandenen Richtlinie aus, um die Richtlinie zu öffnen.
 - e. Wählen Sie unter In dieser Richtlinie definierte Berechtigungen die Option Bearbeiten aus.
 - f. Wählen Sie auf der Seite des Richtlinien-Editors die Option Neue Aussage hinzufügen aus:

- g. Der Policy-Editor fügt eine neue leere Anweisung hinzu, die der folgenden ähnelt
- h. Ersetzen Sie die neue automatisch generierte Anweisung durch Folgendes:

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

- i. Die Ressource ist die ARN des benutzerdefinierten Event-Busses, den Sie in Ihrem Lambda-Code erstellt haben, [Schritt 2: Erstellen Sie einen benutzerdefinierten Event-Bus](#) oder die ARN Ihres Standard-Event-Busses, wenn Sie den Standard-Event-Bus in Ihrem Lambda-Code verwenden.
10. Überprüfen und bestätigen Sie, dass der Rolle die erforderlichen Berechtigungen hinzugefügt wurden.
 11. Wählen Sie Diese neue Version als Standard festlegen und wählen Sie dann Änderungen speichern aus.

Was ist für eine Payload-Transformation erforderlich?

Die folgenden JSON Schlüssel/Wert-Paare sind für Event-Bus-Ereignisse erforderlich, die von AWS Incident Detection and Response erfasst werden.

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

Die folgenden Beispiele zeigen ein Ereignis aus einem Partner-Eventbus vor und nach seiner Transformation.

```
{
```

```
"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"
]
}
```

Beachten Sie, dass vor der Transformation des Ereignisses `detail-type` angegeben wird, APM dass die Warnung von einem Partner APM stammt und der `incident-detection-response-identifizier` Schlüssel nicht vorhanden ist.

Die Lambda-Funktion transformiert das obige Ereignis und platziert es in den benutzerdefinierten oder standardmäßigen Ziel-Event-Bus. Die transformierte Nutzlast enthält jetzt die erforderlichen Schlüssel:Wert-Paare.

```
{
  "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-identifizier": "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"
]
}
```

Beachten Sie, dass detail-type es jetzt ist `aws.monitoring/generic-apm`, Quelle ist jetzt `GenericAPMEvent`, und unter Detail gibt es ein neues Schlüssel/Wert-Paar: `incident-detection-response-identifier`

Im vorherigen Beispiel wird der `incident-detection-response-identifizier` Wert aus dem Namen der Warnung unter dem Pfad übernommen. `$.detail.meta.monitor.name` APM Die Pfade der Warnungsnamen unterscheiden APM sich voneinander. Die Lambda-Funktion muss so geändert werden, dass sie den Alarmnamen aus dem richtigen JSON Partnerereignispfad übernimmt und ihn für den `incident-detection-response-identifizier` Wert verwendet.

Jeder eindeutige Name, der auf der festgelegt ist, `incident-detection-response-identifizier` wird dem AWS Incident Detection and Response Team beim Onboarding zur Verfügung gestellt. Ereignisse, die einen unbekannt Namen für haben, werden `incident-detection-response-identifizier` nicht verarbeitet.

Schritt 4: Erstellen Sie eine benutzerdefinierte EventBridge Amazon-Regel

Für den in Schritt 1 erstellten Partner-Event-Bus ist eine EventBridge Regel erforderlich, die Sie erstellen. Die Regel sendet die gewünschten Ereignisse vom Partner-Event-Bus an die in Schritt 3 erstellte Lambda-Funktion.

Richtlinien zur Definition Ihrer EventBridge Regel finden Sie unter [EventBridge Amazon-Regeln](#).

1. Öffnen Sie die EventBridge Amazon-Konsole unter <https://console.aws.amazon.com/events/>
2. Wählen Sie Regeln und dann den Partner-Event-Bus aus, der Ihrem zugeordnet ist APM. Im Folgenden finden Sie Beispiele für Eventbusse von Partnern:
 - Datadog: `aws.partner/datadog.com/eventbus-name`
 - Splunk: `aws.partner/splunk.com/ RandomString`
3. Wählen Sie Regel erstellen, um eine neue Regel zu erstellen. EventBridge
4. Geben Sie als Regelname einen Namen im folgenden Format `APMName-AWS Incident Detection and Response-EventBridgeRule` ein und wählen Sie dann Weiter aus. Im Folgenden finden Sie Beispielnamen:
 - Datadog: `Datadog-AWSIncidentDetectionResponse-EventBridgeRule`
 - Splunk: `Splunk-AWSIncidentDetectionResponse-EventBridgeRule`
5. Wählen Sie als Ereignisquelle AWS Ereignisse oder EventBridge Partnerereignisse aus.
6. Behalten Sie die Standardwerte Beispielergebnis und Erstellungsmethode bei.
7. Wählen Sie für Event-Pattern Folgendes aus:
 - a. Quelle des Ereignisses: EventBridge Partner.
 - b. Partner: Wählen Sie Ihren APM Partner aus.

c. Ereignistyp: Alle Ereignisse.

Im Folgenden finden Sie Beispiele für Ereignismuster:

Beispiel für ein Datadog-Ereignismuster

Beispiel für ein Splunk-Ereignismuster

8. Wählen Sie für Ziele Folgendes aus:

a. Zieltypen: AWS Dienst

b. Wählen Sie ein Ziel aus: Wählen Sie die Lambda-Funktion.

c. Funktion: Der Name der Lambda-Funktion, die Sie in Schritt 2 erstellt haben.

9. Wählen Sie Weiter, Regel speichern.

Verwenden Sie Webhooks, um Alarme APMs ohne direkte Integration mit Amazon aufzunehmen EventBridge

AWSIncident Detection and Response unterstützt die Verwendung von Webhooks für die Erfassung von Alarmen von Drittanbieter-APMs, die nicht direkt mit Amazon integriert sind. EventBridge

Eine Liste APMs mit direkten Integrationen mit Amazon finden Sie unter EventBridge [EventBridge Amazon-Integrationen](#).

Gehen Sie wie folgt vor, um die Integration mit AWS Incident Detection and Response einzurichten. Bevor Sie diese Schritte ausführen, stellen Sie sicher, dass die AWS verwaltete Regel AWSHealthEventProcessorEventSource-DO DELETE - NOT - in Ihren Konten installiert ist

Erfassen Sie Ereignisse mithilfe von Webhooks

1. Definieren Sie ein Amazon API Gateway, das die Nutzlast von Ihrem APM akzeptiert.
2. Definieren Sie eine AWS Lambda Funktion für die Autorisierung mithilfe eines Authentifizierungstokens, wie in der vorherigen Abbildung dargestellt.
3. Definieren Sie eine zweite Lambda-Funktion, um die AWS Incident Detection and Response Identifier zu transformieren und an Ihre Payload anzuhängen. Sie können diese Funktion

auch verwenden, um nach den Ereignissen zu filtern, die Sie an AWS Incident Detection and Response senden möchten.

4. Richten Sie Ihr System so ein, dass Benachrichtigungen APM an die vom API Gateway URL generierten Nachrichten gesendet werden.

Workloads in Incident Detection and Response verwalten

Ein wichtiger Bestandteil eines effektiven Incident-Managements besteht darin, über die richtigen Prozesse und Verfahren zu verfügen, um Ihre überwachten Workloads zu integrieren, zu testen und zu warten. In diesem Abschnitt werden die wichtigsten Schritte behandelt, darunter die Entwicklung umfassender Runbooks und Reaktionspläne, um Ihre Teams durch Vorfälle zu führen, neue Workloads vor dem Onboarding gründlich zu testen und zu validieren, Änderungen zur Aktualisierung der Workload-Überwachung anzufordern und Workloads bei Bedarf ordnungsgemäß auszulagern.

Themen

- [Entwickeln Sie unter Incident Detection and Response Runbooks und Reaktionspläne für die Reaktion auf einen Vorfall](#)
- [Testen Sie die integrierten Workloads im Bereich Incident Detection and Response](#)
- [Fragen Sie in Incident Detection and Response nach Änderungen an einem integrierten Workload](#)
- [Einen Workload aus Incident Detection and Response auslagern](#)

Entwickeln Sie unter Incident Detection and Response Runbooks und Reaktionspläne für die Reaktion auf einen Vorfall

Incident Detection and Response verwendet Informationen aus Ihrem Onboarding-Fragebogen, um Runbooks und Reaktionspläne für das Management von Vorfällen zu entwickeln, die sich auf Ihre Workloads auswirken. Runbooks dokumentieren die Schritte, die Incident Manager ergreifen, um auf einen Vorfall zu reagieren. Ein Reaktionsplan ist mindestens einer Ihrer Workloads zugeordnet. Das Incident-Management-Team erstellt diese Vorlagen anhand der Informationen, die Sie bei der [Workload-Erkennung](#) bereitgestellt haben. Reaktionspläne sind AWS Systems Manager (SSM) Dokumentvorlagen, mit denen Vorfälle ausgelöst werden. Weitere Informationen zu SSM Dokumenten finden Sie unter [AWS Systems Manager Dokumente](#). Weitere Informationen zu Incident Manager finden Sie unter [Was ist AWS Systems Manager Incident Manager?](#)

Die wichtigsten Ergebnisse:

- Fertigstellung Ihrer Workload-Definition im Bereich AWS Incident Detection and Response.
- Fertigstellung von Alarmen, Runbooks und Definition des Reaktionsplans zur Erkennung und Reaktion auf AWS Vorfälle.

[Sie können auch ein Beispiel für ein Runbook für AWS Incident Detection and Response herunterladen: aws-idr-runbook-example .zip.](#)

Beispiel für ein 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.

Testen Sie die integrierten Workloads im Bereich Incident Detection and Response

Note

Der AWS Identity and Access Management Benutzer oder die Rolle, die Sie für Alarmtests verwenden, muss über eine `cloudwatch:SetAlarmState` entsprechende Berechtigung verfügen.

Der letzte Schritt im Onboarding-Prozess besteht darin, einen Spieltag für Ihren neuen Workload durchzuführen. Nachdem die Alarmaufnahme abgeschlossen ist, bestätigt AWS Incident Detection and Response ein Datum und eine Uhrzeit Ihrer Wahl, um Ihren Spieltag zu beginnen.

Ihr Spieltag dient zwei Hauptzwecken:

- Funktionsvalidierung: Bestätigt, dass AWS Incident Detection and Response Ihre Alarmereignisse korrekt empfangen kann. Und die Funktionsvalidierung bestätigt, dass Ihre Alarmereignisse die entsprechenden Runbooks und alle anderen gewünschten Aktionen auslösen, z. B. die auto Erstellung von Fällen, wenn Sie diese Option bei der Alarmeinnahme ausgewählt haben.
- Simulation: Der Spieltag ist eine umfassende Simulation dessen, was während eines realen Vorfalls passieren könnte. AWS Incident Detection and Response folgt Ihren vorgeschriebenen Schritten, um Ihnen einen Einblick zu geben, wie sich ein realer Vorfall entwickeln könnte. Der Spieltag bietet Ihnen die Gelegenheit, Fragen zu stellen oder Anweisungen zu verfeinern, um das Engagement zu verbessern.

Während des Alarmtests arbeitet AWS Incident Detection and Response mit Ihnen zusammen, um alle festgestellten Probleme zu beheben.

CloudWatch Alarme

AWS Incident Detection and Response testet Ihre CloudWatch Amazon-Alarme, indem die Statusänderung Ihres Alarms überwacht wird. Ändern Sie dazu den Alarm manuell in den Alarmstatus mit dem AWS Command Line Interface. Sie können auch auf das Formular AWS CLI zugreifen AWS CloudShell. AWS Incident Detection and Response bietet Ihnen eine Liste mit AWS CLI Befehlen, die Sie beim Testen verwenden können.

AWS CLI Beispielbefehl zum Einstellen eines Alarmstatus:

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

Weitere Informationen zum manuellen Ändern des Status von CloudWatch Alarmen finden Sie unter [SetAlarmState](#).

Weitere Informationen zu den für den CloudWatch API Betrieb erforderlichen Berechtigungen finden Sie in der [CloudWatch Amazon-Berechtigungsreferenz](#).

APM Alarme von Drittanbietern

Workloads, die ein Tool zur Überwachung der Anwendungsleistung (APM) eines Drittanbieters wie Datadog, Splunk, New Relic oder Dynatrace verwenden, benötigen unterschiedliche Anweisungen, um einen Alarm zu simulieren. Zu Beginn des Spieltages fordert AWS Incident Detection and Response Sie auf, vorübergehend Ihre Alarmschwellenwerte oder Vergleichsoperatoren zu ändern, um den Alarm in den entsprechenden Status zu versetzen. ALARM Dieser Status löst eine Payload für AWS Incident Detection and Response aus.

Die wichtigsten Ergebnisse

Die wichtigsten Ergebnisse:

- Die Alarmeinspeisung war erfolgreich und Ihre Alarmkonfiguration ist korrekt.
- Alarme wurden erfolgreich von AWS Incident Detection and Response erstellt und empfangen.
- Für Ihr Engagement wird ein Support-Fall erstellt, und Ihre angegebenen Ansprechpartner werden benachrichtigt.
- AWS Incident Detection and Response kann mit Ihnen über die von Ihnen vorgeschriebenen Kommunikationswege in Kontakt treten.

- Alle Alarme und Support-Anfragen, die im Rahmen des Spieltages generiert wurden, wurden behoben.
- Es wird eine Go-Live-E-Mail gesendet, in der bestätigt wird, dass Ihr Workload jetzt von AWS Incident Detection and Response überwacht wird.

Fragen Sie in Incident Detection and Response nach Änderungen an einem integrierten Workload

Um Änderungen an einem integrierten Workload anzufordern, führen Sie die folgenden Schritte aus, um einen Support-Fall mit AWS Incident Detection and Response zu erstellen.

1. Gehen Sie zum [AWS Support Center](#) und wählen Sie dann Kundenvorgang erstellen aus, wie im folgenden Beispiel gezeigt:
2. Wählen Sie Technisch.
3. Wählen Sie für Service die Option Incident Detection and Response aus.
4. Wählen Sie als Kategorie die Option Workload Change Request aus.
5. Wählen Sie unter Schweregrad die Option Allgemeine Hinweise aus.
6. Geben Sie einen Betreff für diese Änderung ein. Beispielsweise:

AWSErkennung und Reaktion auf Vorfälle - *workload_name*

7. Geben Sie eine Beschreibung für diese Änderung ein. Geben Sie beispielsweise „Diese Anfrage bezieht sich auf Änderungen an einem bestehenden Workload, der in AWS Incident Detection and Response integriert wurde“. Stellen Sie sicher, dass Ihre Anfrage die folgenden Informationen enthält:
 - Workload-Name: Ihr Workload-Name.
 - Konto-ID (s): ID1 ID2ID3,, usw.
 - Details ändern: Geben Sie die Details für die von Ihnen angeforderte Änderung ein.
8. Geben Sie im Abschnitt Zusätzliche Kontakte — optional eine beliebige E-Mail-Adresse einIDs, an die Sie über diese Änderung informiert werden möchten.

Im Folgenden finden Sie ein Beispiel für den Abschnitt Zusätzliche Kontakte — optional.

⚠ Important

Wenn Sie dem Abschnitt **Zusätzliche Kontakte** — optional keine E-Mail IDs hinzufügen, kann sich der Änderungsprozess verzögern.

9. Wählen Sie Absenden aus.

Nachdem Sie die Änderungsanfrage eingereicht haben, können Sie weitere E-Mails von Ihrer Organisation hinzufügen. Um E-Mails hinzuzufügen, wählen Sie **In Kundenvorgangsdetails** antworten aus, wie im folgenden Beispiel gezeigt:

Fügen Sie dann die E-Mail IDs im Abschnitt **Zusätzliche Kontakte** — optional hinzu.

Im Folgenden finden Sie ein Beispiel für die Antwortseite, auf der Sie zusätzliche E-Mails eingeben können.

Einen Workload aus Incident Detection and Response auslagern

Um einen Workload aus AWS Incident Detection and Response auszulagern, erstellen Sie für jeden Workload einen neuen Support-Fall. Beachten Sie bei der Erstellung des Support-Falls Folgendes:

- Um einen Workload auszulagern, der sich in einem einzigen AWS Konto befindet, erstellen Sie den Support-Fall entweder über das Konto des Workloads oder über Ihr Zahlerkonto.
- Wenn du einen Workload auslagern möchtest, der sich über mehrere AWS Konten erstreckt, erstellst du den Support-Fall dann von deinem Konto aus. Führen Sie im Hauptteil des Support-Falls alle Konten IDs auf, die extern bearbeitet werden sollen.

⚠ Important

Wenn Sie eine Support-Anfrage erstellen, um einen Workload vom falschen Account zu entfernen, kann es zu Verzögerungen und Anfragen nach zusätzlichen Informationen kommen, bevor Ihre Workloads ausgelagert werden können.

Anfrage zum Offboarding eines Workloads

1. Gehen Sie zum [AWS Support Center](#) und wählen Sie dann Fall erstellen aus.
2. Wählen Sie Technisch aus.
3. Wählen Sie für Service die Option Incident Detection and Response aus.
4. Wählen Sie als Kategorie die Option Workload Offboarding aus.
5. Wählen Sie als Schweregrad die Option General Guidance aus.
6. Geben Sie einen Betreff für diese Änderung ein. Beispielsweise:

[Offboard] Erkennung und Reaktion auf AWS Vorfälle - *workload_name*

7. Geben Sie eine Beschreibung für diese Änderung ein. Geben Sie beispielsweise „Diese Anfrage dient dem Offboarding eines vorhandenen Workloads, der in AWS Incident Detection and Response integriert wurde“ ein. Stellen Sie sicher, dass Ihre Anfrage die folgenden Informationen enthält:
 - Workload-Name: Ihr Workload-Name.
 - Konto-ID (s): ID1 ID2ID3,, usw.
 - Grund für das Offboarding: Geben Sie einen Grund für das Offboarding des Workloads an.
8. Geben Sie im Abschnitt Zusätzliche Kontakte — optional die E-Mail-Adresse ein, an IDs die Sie Informationen zu dieser Offboarding-Anfrage erhalten möchten.
9. Wählen Sie Absenden aus.

AWSÜberwachung und Beobachtbarkeit von Vorfällen bei der Erkennung und Reaktion

AWSIncident Detection and Response bietet Ihnen fachkundige Unterstützung bei der Definition der Observability für Ihre Workloads — von der Anwendungsebene bis hin zur zugrunde liegenden Infrastruktur. Die Überwachung zeigt Ihnen, dass etwas nicht stimmt. Observability nutzt die Datenerfassung, um Ihnen mitzuteilen, was falsch ist und warum es passiert ist.

Das Incident Detection and Response-System überwacht Ihre AWS Workloads auf Ausfälle und Leistungseinbußen, indem es native AWS Dienste wie Amazon CloudWatch und Amazon nutzt, um Ereignisse EventBridge zu erkennen, die sich auf Ihre Arbeitslast auswirken könnten. Die Überwachung informiert Sie über drohende, andauernde, sich zurückziehende oder potenzielle Ausfälle oder Leistungseinbußen. Wenn Sie Ihr Konto in Incident Detection and Response einbinden, wählen Sie aus, welche Alarme in Ihrem Konto vom Incident Detection and Response Monitoring System überwacht werden sollen, und verknüpfen diese Alarme mit einer Anwendung und einem Runbook, die beim Incident Management verwendet werden.

Incident Detection and Response nutzt Amazon CloudWatch und andere AWS-Services , um Ihre Observability-Lösung zu entwickeln. AWSIncident Detection and Response unterstützt Sie auf zweierlei Weise bei der Beobachtbarkeit:

- **Kennzahlen zu Geschäftsergebnissen:** Die Beobachtbarkeit bei der Erkennung und Reaktion auf AWS Vorfälle beginnt mit der Definition der wichtigsten Kennzahlen, mit denen die Ergebnisse Ihrer Workloads oder der Endbenutzererfahrung überwacht werden. AWS Experten arbeiten mit Ihnen zusammen, um die Ziele Ihres Workloads, die wichtigsten Ergebnisse oder Faktoren, die sich auf die Benutzererfahrung auswirken können, zu verstehen und die Metriken und Warnmeldungen zu definieren, mit denen jegliche Verschlechterung dieser wichtigen Kennzahlen erfasst wird. Eine wichtige Geschäftskennzahl für eine mobile Anruferanwendung ist beispielsweise die Erfolgsquote bei der Einrichtung von Anrufen (überwacht die Erfolgsrate von Benutzeranrufversuchen), und eine wichtige Kennzahl für eine Website ist die Seitengeschwindigkeit. Die Interaktion mit Vorfällen wird auf der Grundlage von Kennzahlen zu Geschäftsergebnissen ausgelöst.
- **Metriken auf Infrastrukturebene:** In dieser Phase identifizieren wir die Grundlage AWS-Services und die Infrastruktur, die Ihre Anwendung unterstützt, und definieren Metriken und Alarme, um die Leistung dieser Infrastrukturdienste zu verfolgen. Dazu können Metriken wie `ApplicationLoadBalancerErrorCount` für Application Load Balancer Balancer-Instances gehören. Dies beginnt, nachdem der Workload integriert und die Überwachung eingerichtet wurde.

Implementierung der Beobachtbarkeit bei der Erkennung und Reaktion auf AWS Vorfälle

Da es sich bei der Observability um einen kontinuierlichen Prozess handelt, der möglicherweise nicht innerhalb einer einzigen Übung oder eines Zeitrahmens abgeschlossen werden kann, implementiert AWS Incident Detection and Response die Beobachtbarkeit in zwei Phasen:

- **Onboarding-Phase:** Die Beobachtbarkeit beim Onboarding konzentriert sich darauf, zu erkennen, wann die Geschäftsergebnisse Ihrer Anwendung beeinträchtigt werden. Zu diesem Zweck konzentriert sich die Beobachtbarkeit während der Onboarding-Phase auf die Definition der wichtigsten Kennzahlen für Geschäftsergebnisse auf Anwendungsebene, um Sie bei Störungen Ihrer Workloads zu benachrichtigen AWS . Auf diese Weise AWS können Sie umgehend auf diese Störungen reagieren und Sie bei der Wiederherstellung unterstützen.
- **Phase nach dem Onboarding:** AWS Incident Detection and Response bietet eine Reihe proaktiver Services zur Überwachung der Daten, darunter die Definition von Metriken auf Infrastrukturebene, die Optimierung von Metriken und die Einrichtung von Traces und Protokollen je nach Reifegrad des Kunden. Die Implementierung dieser Services kann sich über mehrere Monate erstrecken und mehrere Teams einbeziehen. AWS Incident Detection and Response bietet Anleitungen zur Einrichtung der Observability. Kunden sind verpflichtet, die erforderlichen Änderungen in ihrer Workload-Umgebung vorzunehmen. Wenn Sie Hilfe bei der praktischen Implementierung von Observability-Funktionen benötigen, wenden Sie sich bitte an Ihre technischen Kundenbetreuer (TAMs).

Incident-Management mit Incident Detection and Response

AWS Incident Detection and Response bietet Ihnen rund um die Uhr proaktive Überwachung und Verwaltung von Vorfällen, die von einem eigens dafür vorgesehenen Team von Incident Managern bereitgestellt werden. Das folgende Diagramm zeigt den Standardprozess für das Incident-Management, wenn ein Anwendungsalarm einen Vorfall auslöst, einschließlich der Alarmerzeugung, der Einbindung des AWS Incident Managers, der Behebung von Vorfällen und der Überprüfung nach dem Vorfall.

1. Generierung von Alarmen: Bei Ihren Workloads ausgelöste Alarme werden über Amazon EventBridge an AWS Incident Detection and Response weitergeleitet. AWS Incident Detection and Response ruft automatisch das mit Ihrem Alarm verknüpfte Runbook auf und benachrichtigt einen Incident Manager. Wenn bei Ihrem Workload ein kritischer Vorfall auftritt, der nicht durch Alarme erkannt wird, die von AWS Incident Detection and Response überwacht werden, können Sie einen Support-Fall erstellen, um eine Reaktion auf einen Vorfall anzufordern. Weitere Informationen zum Anfordern einer Reaktion auf einen Vorfall finden Sie unter [Fordern Sie eine Antwort auf einen Vorfall an](#).
2. AWS Engagement des Incident Managers: Der Incident Manager reagiert auf den Alarm und lädt Sie zu einer Telefonkonferenz ein oder wie im Runbook anderweitig angegeben. Der Incident Manager überprüft den Zustand der, AWS-Services um festzustellen, ob der Alarm auf Probleme zurückzuführen ist, die vom Workload AWS-Services genutzt wurden, und berät Sie über den Status der zugrunde liegenden Dienste. Falls erforderlich, erstellt der Incident Manager dann in Ihrem Namen einen Fall und beauftragt die richtigen AWS Experten mit der Unterstützung.

Da AWS Incident Detection and Response AWS-Services speziell für Ihre Anwendungen überwacht wird, kann AWS Incident Detection and Response feststellen, dass der Vorfall mit einem AWS-Service Problem zusammenhängt, noch bevor ein AWS-Service Ereignis gemeldet wird. In diesem Szenario berät Sie der Incident Manager über den Status des AWS-Service, löst den AWS Service Event Incident Management Flow aus und setzt sich mit dem Serviceteam in Verbindung, um die Lösung zu finden. Die bereitgestellten Informationen geben Ihnen die Möglichkeit, Ihre Wiederherstellungspläne oder Behelfslösungen frühzeitig umzusetzen, um die Auswirkungen des AWS Serviceereignisses zu minimieren. Weitere Informationen finden Sie unter [Verwaltung von Vorfällen bei Serviceereignissen](#).

3. Behebung von Vorfällen: Der Incident Manager koordiniert den Vorfall zwischen den erforderlichen AWS Teams und stellt sicher, dass Sie mit den richtigen AWS Experten zusammenarbeiten, bis der Vorfall gemildert oder gelöst ist.
4. Überprüfung nach dem Vorfall (falls gewünscht): Nach einem Vorfall kann AWS Incident Detection and Response auf Anfrage eine Überprüfung nach dem Vorfall durchführen und einen Bericht nach dem Vorfall erstellen. Der Bericht nach dem Vorfall enthält eine Beschreibung des Problems, der Auswirkungen, der beteiligten Teams und der zur Minderung oder Lösung des Vorfalls ergriffenen Abhilfemaßnahmen oder Maßnahmen. Der Bericht nach dem Vorfall kann Informationen enthalten, die verwendet werden können, um die Wahrscheinlichkeit eines erneuten Auftretens eines Vorfalls zu verringern oder das Management eines future Auftretens eines ähnlichen Vorfalls zu verbessern. Der Bericht nach dem Vorfall ist keine Ursachenanalyse (RCA). Sie können eine RCA Ergänzung zum Bericht nach dem Vorfall anfordern. Ein Beispiel für einen Bericht nach einem Vorfall finden Sie im folgenden Abschnitt.

⚠ Important

Die folgende Berichtsvorlage ist nur ein Beispiel.

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 newly provisioned to handle an increase in workload traffic for an on-going promotional event.

At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The Incident Manager worked with the Cloud Support Engineer to raise an escalation a higher support level to quickly scale the ALB per the runbook.

At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The back-off/retry logic yields mild recovery but timeouts are still being seen for some clients.

By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to pre-incident levels. Connection timeouts subside.

At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

Mitigation:

Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis (RCA).

Back-off and retries yielded mild recovery. Full mitigation happened after escalation to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):

Action items to be reviewed with your Technical Account Manager (TAM), if required. Review alarm thresholds to engage AWS Incident Detection and Response closer to the time of impact.

Work with AWS Support and TAM team to ensure newly created ALBs are pre-scaled to accommodate expected spikes in workload traffic.

Themen

- [Bereitstellen des Zugriffs auf das AWS Support Center für Anwendungsteams](#)
- [Verwaltung von Vorfällen bei Serviceereignissen](#)
- [Fordern Sie eine Antwort auf einen Vorfall an](#)
- [Verwalten Sie Supportfälle bei der Erkennung und Reaktion auf Vorfälle mit dem AWS Support App in Slack](#)

Bereitstellen des Zugriffs auf das AWS Support Center für Anwendungsteams

AWSIncident Detection and Response informiert Sie über alle AWS Support Fälle während des gesamten Lebenszyklus eines Vorfalls. Um mit den Incident Managern kommunizieren zu können, müssen Ihre Teams Zugriff auf das AWS Support Center haben.

Weitere Informationen zur Bereitstellung des Zugriffs finden Sie im AWS Support Benutzerhandbuch unter [Zugriff auf das AWS Support Center verwalten](#).

Verwaltung von Vorfällen bei Serviceereignissen

AWSIncident Detection and Response informiert Sie über ein laufendes Serviceereignis in Ihren AWS Regionen, unabhängig davon, ob Ihre Arbeitslast beeinträchtigt wird oder nicht. Während einer AWS Serviceveranstaltung erstellt AWS Incident Detection and Response einen AWS Support-Fall, nimmt an Ihrer Telefonkonferenz teil, um Feedback zu den Auswirkungen und der Stimmung zu erhalten, und gibt Ihnen Tipps, wie Sie Ihre Wiederherstellungspläne während der Veranstaltung in Anspruch nehmen können. Sie erhalten außerdem eine Benachrichtigung AWS Health mit Einzelheiten zum Ereignis. Kunden, die von dem betreffenden AWS Serviceereignis nicht betroffen sind (z. B. weil sie in einer anderen AWS Region tätig sind, den beeinträchtigten AWS Service nicht nutzen usw.), werden weiterhin durch das Standardangebot unterstützt. Weitere Informationen zu AWS Health finden Sie unter [Was ist AWS Health?](#)

Das folgende Diagramm veranschaulicht den Ablauf oder Prozess, der beim Eintreten eines AWS Serviceereignisses befolgt wird, und beschreibt die Maßnahmen, die Teams, AWS Incident-Response-Teams und Kunden ergriffen haben, um die Serviceunterbrechung oder das Problem zu identifizieren, zu mindern und zu lösen.


Bericht nach dem Vorfall für Serviceereignisse (falls gewünscht): Wenn ein Serviceereignis einen Vorfall verursacht, können Sie Incident Detection and Response AWS beauftragen, eine Überprüfung

nach dem Vorfall durchzuführen und einen Bericht nach dem Vorfall zu erstellen. Der Bericht nach dem Vorfall für Serviceereignisse umfasst Folgendes:

- Eine Beschreibung des Problems
- Die Auswirkungen des Vorfalls
- Auf dem AWS Health Dashboard geteilte Informationen
- Die Teams, die während des Vorfalls im Einsatz waren
- Behelfslösungen und Maßnahmen zur Minderung oder Lösung des Vorfalls

Der Bericht nach dem Vorfall für Serviceereignisse kann Informationen enthalten, die verwendet werden können, um die Wahrscheinlichkeit eines erneuten Auftretens eines Vorfalls zu verringern oder das Management eines future Auftretens eines ähnlichen Vorfalls zu verbessern. Der Bericht nach dem Vorfall für Serviceereignisse ist keine Ursachenanalyse (RCA). Für Serviceereignisse können Sie RCA zusätzlich zum Bericht nach dem Vorfall einen Bericht anfordern.

Im Folgenden finden Sie ein Beispiel für einen Bericht nach dem Vorfall für ein Serviceereignis:

 Note

Die folgende Berichtsvorlage ist nur ein Beispiel.

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 0000000000 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 a 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 ...

Fordern Sie eine Antwort auf einen Vorfall an

Wenn bei Ihrem Workload ein kritischer Vorfall auftritt, der nicht durch Alarme erkannt wird, die von AWS Incident Detection and Response überwacht werden, können Sie einen Support-Fall erstellen, um eine Reaktion auf einen Vorfall anzufordern. Mithilfe von, oder können Sie für jeden Workload, der AWS Incident Detection and Response abonniert hat, eine Incident Response anfordern,

einschließlich Workloads, die sich im Onboarding-Prozess befinden AWS Support Center Console.
AWS Support API AWS Support App in Slack

Das folgende Diagramm veranschaulicht den end-to-end Arbeitsablauf für einen AWS Kunden, der Unterstützung bei einem Vorfall vom Incident Detection and Response Team anfordert. Dabei werden die Schritte von der ersten Anfrage bis hin zur Untersuchung, Minderung und Lösung detailliert beschrieben.

Um eine Reaktion auf einen Vorfall zu beantragen, der sich aktiv auf Ihre Arbeitslast auswirkt, erstellen Sie einen Fall. AWS Support Nachdem der Support-Fall angesprochen wurde, werden Sie im Rahmen von AWS Incident Detection and Response mit den AWS Experten zusammengeführt, die Sie benötigen, um die Wiederherstellung Ihrer Arbeitslast zu beschleunigen.

Fordern Sie eine Incident-Response an, indem Sie AWS Support Center Console

1. Öffnen Sie die [AWS Support Center Console](#) und wählen Sie dann Fall erstellen aus.
2. Wählen Sie Technisch.
3. Wählen Sie für Service die Option Incident Detection and Response aus.
4. Wählen Sie als Kategorie die Option Active Incident aus.
5. Wählen Sie für Schweregrad die Option Geschäftskritisches System ausgefallen aus.
6. Geben Sie einen Betreff für diesen Vorfall ein. Beispielsweise:

AWSErkennung und Reaktion auf Vorfälle — Aktiver Vorfall — workload_name

7. Geben Sie die Problembeschreibung für diesen Vorfall ein. Fügen Sie die folgenden Details hinzu:

- Technische Informationen:

Betroffene Dienste:

Betroffene Ressource (n):

Betroffene Region (en):

Name des Workloads:

- Informationen zum Unternehmen:

Beschreibung der Auswirkungen auf das Unternehmen:

[Optional] Einzelheiten zur Kundenbrücke:

8. Geben Sie im Abschnitt **Zusätzliche Kontakte** alle E-Mail-Adressen ein, an die Sie Mitteilungen zu diesem Vorfall erhalten möchten.

Die folgende Abbildung zeigt den Konsolenbildschirm, wobei das Feld **Zusätzliche Kontakte** hervorgehoben ist.

9. Wählen Sie **Absenden** aus.

Nachdem Sie eine Anfrage zur Reaktion auf Vorfälle eingereicht haben, können Sie weitere E-Mail-Adressen aus Ihrer Organisation hinzufügen. Um weitere Adressen hinzuzufügen, antworten Sie auf den Fall und fügen Sie dann die E-Mail-Adressen im Abschnitt **Zusätzliche Kontakte** hinzu.

Die folgende Abbildung zeigt den Bildschirm mit den Falldetails, wobei die Schaltfläche **Antworten** hervorgehoben ist.

Die folgende Abbildung zeigt den Fall „Antwort“, wobei das Feld **Zusätzliche Kontakte** und die Schaltfläche „**Senden**“ hervorgehoben sind.

10. Bei Incident Detection and Response wird Ihr Fall innerhalb von fünf Minuten bestätigt und Sie werden auf einer Konferenz mit den entsprechenden AWS Experten vernetzt.

Fordern Sie eine Reaktion auf einen Vorfall an, indem Sie AWS Support API

Sie können den verwenden AWS Support API, um programmgesteuert Supportfälle zu erstellen. Weitere Informationen finden Sie unter [About the AWS Support API](#) im AWS Support Benutzerhandbuch.

Fordern Sie eine Reaktion auf einen Vorfall an, indem Sie AWS Support App in Slack

Gehen Sie wie folgt vor AWS Support App in Slack , um mit dem eine Antwort auf einen Vorfall anzufordern:

1. Öffnen Sie den Slack-Channel, AWS Support App in Slack in dem Sie den konfiguriert haben.
2. Geben Sie den folgenden Befehl ein:

```
/awssupport create
```

3. Geben Sie einen Betreff für diesen Vorfall ein. Geben Sie beispielsweise AWSIncident Detection and Response — Active Incident — workload_name ein.
4. Geben Sie die Problembeschreibung für diesen Vorfall ein. Fügen Sie die folgenden Details hinzu:

Technische Informationen:

Betroffene Dienste:

Betroffene Ressource (n):

Betroffene Region (en):

Name des Workloads:

Informationen zum Unternehmen:

Beschreibung der Auswirkungen auf das Unternehmen:

[Optional] Einzelheiten zur Kundenbrücke:

5. Wählen Sie Weiter.
6. Wählen Sie als Problemtyp die Option Technischer Support aus.
7. Wählen Sie für Service die Option Incident Detection and Response aus.
8. Wählen Sie als Kategorie die Option Active Incident aus.
9. Wählen Sie für Schweregrad die Option Geschäftskritisches System ausgefallen aus.
10. Geben Sie optional bis zu 10 zusätzliche Kontakte in das Feld Zusätzliche zu benachrichtigende Kontakte ein, getrennt durch Kommas. Diese zusätzlichen Kontakte erhalten Kopien der E-Mail-Korrespondenz zu diesem Vorfall.
11. Wählen Sie Überprüfen aus.
12. Eine neue Nachricht, die nur für dich sichtbar ist, erscheint im Slack-Channel. Überprüfe die Falldetails und wähle dann Kundenvorgang erstellen aus.

- 13 Deine Fall-ID wird in einer neuen Nachricht von der AWS Support App in Slack angegeben.
- 14 Incident Detection and Response bestätigt Ihren Fall innerhalb von 5 Minuten und verbindet Sie mit den entsprechenden AWS Experten auf einer Konferenz.
- 15 Die Korrespondenz von Incident Detection and Response wird im Fall-Thread aktualisiert.

Verwalten Sie Supportfälle bei der Erkennung und Reaktion auf Vorfälle mit dem AWS Support App in Slack

Mit dem [AWS Support App in Slack](#) kannst du deine AWS Support Fälle in Slack verwalten, Benachrichtigungen über neue, durch [Alarme ausgelöste Vorfälle in deinem AWS Workload zur Erkennung und Reaktion auf Vorfälle](#) erhalten und [Anfragen zur Reaktion auf Vorfälle](#) erstellen.

Folgen Sie den Anweisungen im [AWS Support Benutzerhandbuch AWS Support App in Slack](#), um das zu konfigurieren.

Important

- Um in Slack Benachrichtigungen für alle durch Alarme ausgelösten Vorfälle auf deinem Workload zu erhalten, musst du das AWS Support App in Slack für alle Accounts deines Workloads konfigurieren, die in AWS Incident Detection and Response integriert sind. Supportfälle werden in dem Konto erstellt, von dem der Workload-Alarm ausgegangen ist.
- Während eines Vorfalls können in Ihrem Namen mehrere Supportfälle mit hohem Schweregrad eröffnet werden, um die Problemlöser zu kontaktieren AWS Support . Du erhältst in Slack Benachrichtigungen für alle Supportanfragen, die während eines Vorfalls geöffnet werden und die deiner [Benachrichtigungskonfiguration für den](#) Slack-Kanal entsprechen.
- Benachrichtigungen, die du über den erhältst, ersetzen AWS Support App in Slack nicht die Initial- und Eskalationskontakte deines Workloads, die während eines Vorfalls per E-Mail oder Telefonanruf von AWS Incident Detection and Response kontaktiert wurden.

Themen

- [Benachrichtigungen über einen durch einen Alarm ausgelösten Vorfall in Slack](#)

- [Erstelle eine Anfrage zur Reaktion auf einen Vorfall in Slack](#)

Benachrichtigungen über einen durch einen Alarm ausgelösten Vorfall in Slack

Nachdem du das AWS Support App in Slack in deinem Slack-Kanal konfiguriert hast, erhältst du Benachrichtigungen über durch Alarme ausgelöste Vorfälle auf deinem Workload, der von AWS Incident Detection and Response überwacht wird.

Das folgende Beispiel zeigt, wie Benachrichtigungen für durch Alarme ausgelöste Vorfälle in Slack angezeigt werden.

Beispiel für eine Benachrichtigung

Wenn dein durch einen Alarm ausgelöster AWS Vorfall von Incident Detection and Response bestätigt wird, wird in Slack eine Benachrichtigung ähnlich der folgenden generiert:

Wähle Details anzeigen, um die vollständige Korrespondenz einzusehen, die von AWS Incident Detection and Response hinzugefügt wurde.

Weitere Updates von AWS Incident Detection and Response erscheinen im Thread des Falls.

Wählen Sie „Details anzeigen“, um die vollständige Korrespondenz einzusehen, die von AWS Incident Detection and Response hinzugefügt wurde.

Erstelle eine Anfrage zur Reaktion auf einen Vorfall in Slack

Eine Anleitung dazu, wie du über den eine Anfrage zur Reaktion auf einen Vorfall erstellst AWS Support App in Slack, findest du unter [Fordern Sie eine Antwort auf einen Vorfall an](#).

Berichterstattung bei der Erkennung und Reaktion auf Vorfälle

AWSIncident Detection and Response liefert Betriebs- und Leistungsdaten, anhand derer Sie sich ein Bild davon machen können, wie der Service konfiguriert ist, welche Vorfälle in der Vergangenheit aufgetreten sind und wie die Leistung des Incident Detection and Response Services aussieht. Auf dieser Seite werden die verfügbaren Datentypen behandelt, darunter Konfigurationsdaten, Vorfalldaten und Leistungsdaten.

Konfigurationsdaten

- Alle Konten sind integriert
- Namen aller Anwendungen
- Die Alarme, Runbooks und Supportprofile, die jeder Anwendung zugeordnet sind

Daten zu Vorfällen

- Datum, Anzahl und Dauer der Vorfälle für jede Anwendung
- Datum, Anzahl und Dauer von Vorfällen im Zusammenhang mit einem bestimmten Alarm
- Bericht nach dem Vorfall

Leistungsdaten

- Leistung des Service Level-Ziels (SLO)

Falls Sie Betriebs- und Leistungsdaten benötigen, wenden Sie sich an Ihren technischen Kundenbetreuer.

Sicherheit und Resilienz bei der Erkennung und Reaktion auf Vorfälle

Das [Modell der AWS gemeinsamen Verantwortung](#) gilt für den Datenschutz in AWS Support. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt umfasst die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services das, was Sie verwenden.

Weitere Informationen zum Datenschutz finden Sie im [Abschnitt Datenschutz FAQ](#).

Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model](#) und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir Ihnen, Ihre AWS Kontoanmeldeinformationen zu schützen und individuelle Benutzerkonten mit AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie Secure Sockets Layer/Transport Layer Security (SSL/TLS) -Zertifikate für die Kommunikation mit Ressourcen. AWS Wir empfehlen TLS 1.2 oder höher. Weitere Informationen finden Sie unter [Was ist ein SSL TLS /-Zertifikat?](#) .
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Weitere Informationen finden Sie unter [AWS CloudTrail](#).
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste. Weitere Informationen finden Sie unter [AWS Kryptografiedienste und -tools](#).
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern. Informationen zu Amazon Macie finden Sie unter [Amazon Macie](#).
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine FIPS 140-2 validierte kryptografische Module benötigen, verwenden Sie einen API Endpunkt. FIPS Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter [Federal Information Processing Standard \(\) 140-2](#).
FIPS

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole arbeiten AWS Support oder sie anderweitig AWS-Services verwenden,API, AWS CLI oder. AWS SDKs Alle Daten, die Sie in Tags (Markierungen) oder Freiformfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen in den angebenURL, um Ihre Anfrage an diesen Server zu überprüfen.

AWSZugriff auf Ihre Konten zur Erkennung und Reaktion auf Vorfälle

AWS Identity and Access Management (IAM) ist ein Webdienst, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können. Sie steuern IAM damit, wer authentifiziert (angemeldet) und autorisiert ist (über Berechtigungen verfügt), um Ressourcen zu verwenden.

AWSErkennung und Reaktion auf Vorfälle und Ihre Alarmdaten

Standardmäßig empfängt Incident Detection and Response den Amazon-Ressourcennamen (ARN) und den Status jedes CloudWatch Alarms in Ihrem Konto und startet dann den Prozess zur Erkennung und Reaktion auf Vorfälle, wenn Ihr integrierter Alarm in den ALARM Status wechselt. Wenn Sie anpassen möchten, welche Informationen Incident Detection and Response über Alarme von Ihrem Konto erhält, wenden Sie sich an Ihren Technical Account Manager.

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version des IDR Handbuchs beschrieben.

- Letzte Aktualisierung der Dokumentation: 1. November 2024

Änderung	Beschreibung	Datum
Zusätzlich AWS-Regionen hinzugefügt	Weitere AWS-Regionen wurden dem Abschnitt Verfügbarkeit von Incident Detection and Response hinzugefügt. Der Abschnitt wurde aktualisiert: Regionale Verfügbarkeit für Incident Detection and Response	1. November 2024
Aktualisierungen zur Verwaltung von Support-Fällen zur Erkennung und Reaktion auf Vorfälle auf AWS Support App in Slack dieser Seite	Die Seite wurde in den Bereich Incident Management verschoben, der Text überarbeitet und die Screenshots ersetzt. Abschnitt aktualisiert: Verwalten Sie Supportfälle bei der Erkennung und Reaktion auf Vorfälle mit dem AWS Support App in Slack	10. Oktober 2024
Eine neue Seite wurde hinzugefügt AWS Support App in Slack Aktualisiertes Incident-Management mit AWS Incident Detection and Response	Es wurde eine neue Seite hinzugefügt für AWS Support App in Slack Das Incident-Management wurde mit AWS Incident Detection and Response aktualisiert und um den neuen Abschnitt „Anfrage einer Reaktion auf Vorfälle mit dem AWS Support App in Slack“ erweitert.	10. September 2024
Kontoabonnement aktualisiert	Der Abschnitt „Kontoabonnement“ wurde aktualisiert und enthält nun Informationen darüber, wo Sie eine Support-Anfrage eröffnen	12. Juni 2024

Änderung	Beschreibung	Datum
	<p>können, wenn Sie ein Abonnement für ein Konto beantragen.</p> <p>Der Abschnitt wurde aktualisiert: Abonnieren Sie einen Workload für Incident Detection and Response</p>	
<p>Bericht nach dem Vorfall für Serviceveranstaltungen jetzt verfügbar</p>	<p>Der Abschnitt zur Verwaltung von Vorfällen für Serviceereignisse wurde aktualisiert und enthält nun Informationen zum Bericht nach dem Vorfall für Serviceereignisse.</p> <p>Der Abschnitt wurde aktualisiert: Verwaltung von Vorfällen bei Serviceereignissen</p>	<p>8. Mai 2024</p>
<p>Ein neuer Abschnitt wurde hinzugefügt: Offboard eines Workloads</p>	<p>Unter Erste Schritte wurde der Abschnitt Einen Workload auslagern hinzugefügt, der Informationen über das Offboarding von Workloads enthält</p> <p>Weitere Informationen finden Sie unter Einen Workload aus Incident Detection and Response auslagern.</p>	<p>28. März 2024</p>
<p>Kontoabonnement aktualisiert</p>	<p>Der Abschnitt „Kontoabonnement“ wurde aktualisiert und enthält nun Informationen zu Offboarding-Workloads</p> <p>Weitere Informationen finden Sie unter Kontoabonnement</p>	<p>28. März 2024</p>

Änderung	Beschreibung	Datum
Der Test wurde aktualisiert	<p>Der Abschnitt „Testen“ wurde aktualisiert und enthält nun Informationen zum Testen am Spieltag als letzten Schritt im Onboarding-Prozess.</p> <p>Der Abschnitt wurde aktualisiert: Testen Sie die integrierten Workloads im Bereich Incident Detection and Response</p>	29. Februar 2024
Aktualisiert Was ist Erkennung und Reaktion auf AWS Vorfälle	<p>Der Abschnitt „Was ist Erkennung und Reaktion auf AWS Vorfälle“ wurde aktualisiert.</p> <p>Abschnitt aktualisiert: Was ist AWS Incident Detection and Response?</p>	19. Februar 2024
Der Abschnitt zum Fragebogen wurde aktualisiert	<p>Der Fragebogen zum Onboarding von Workloads wurde aktualisiert und ein Fragebogen zur Erfassung von Alarmen hinzugefügt. Der Abschnitt wurde von Onboarding-Fragebogen in Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen umbenannt.</p> <p>Abschnitt aktualisiert: Fragebögen zum Onboarding von Workloads und zur Erfassung von Alarmen in Incident Detection and Response</p>	2. Februar 2024

Änderung	Beschreibung	Datum
<p>Aktualisierte Informationen zu AWS Servicetereignissen und Onboarding-Informationen</p>	<p>Mehrere Abschnitte wurden mit neuen Informationen für das Onboarding aktualisiert.</p> <p>Aktualisierte Abschnitte:</p> <ul style="list-style-type: none"> • Verwaltung von Vorfällen bei Serviceereignissen • Erkennung von Arbeitslasten bei der Erkennung und Reaktion auf Vorfälle • Einführung in die Erkennung und Reaktion auf Vorfälle • Abonnieren Sie einen Workload für Incident Detection and Response <p>Neue Abschnitte</p> <ul style="list-style-type: none"> • Bereitstellen des Zugriffs auf das AWS Support Center für Anwendungsteams 	<p>31. Januar 2024</p>
<p>Ein Abschnitt mit verwandten Informationen wurde hinzugefügt</p>	<p>In Access Provisioning wurde ein Abschnitt mit verwandten Informationen hinzugefügt.</p> <p>Abschnitt aktualisiert: Bereitstellen des Zugriffs für die Erfassung von Warnmeldungen auf Incident Detection and Response</p>	<p>17. Januar 2024</p>
<p>Die Beispielschritte wurden aktualisiert</p>	<p>Das Verfahren für die Schritte 2, 3 und 4 in Beispiel: Integration von Benachrichtigungen von Datadog und Splunk wurde aktualisiert.</p> <p>Abschnitt aktualisiert: Beispiel: Integrieren Sie Benachrichtigungen von Datadog und Splunk</p>	<p>21. Dezember 2023</p>

Änderung	Beschreibung	Datum
Grafik und Text der Einführung wurden aktualisiert	<p>Die Grafik in Ingest-Alarmen vonAPMs, die direkt mit Amazon EventBridge integriert sind, wurde aktualisiert.</p> <p>Abschnitt aktualisiert: Entwickeln Sie unter Incident Detection and Response Runbooks und Reaktionspläne für die Reaktion auf einen Vorfall</p>	21. Dezember 2023
Die Runbook-Vorlage wurde aktualisiert	<p>Die Runbook-Vorlage unter Entwickeln von Runbooks für die Erkennung und Reaktion auf AWS Vorfälle wurde aktualisiert.</p> <p>Der Abschnitt wurde aktualisiert: Entwickeln Sie unter Incident Detection and Response Runbooks und Reaktionspläne für die Reaktion auf einen Vorfall</p>	4. Dezember 2023
Aktualisierte Alarmkonfigurationen	<p>Aktualisierte Alarmkonfigurationen mit detaillierten Informationen zur CloudWatch Alarmkonfiguration.</p> <p>Neuer Abschnitt: Erstellen Sie in Incident Detection and Response CloudWatch Alarme, die Ihren Geschäftsanforderungen entsprechen</p> <p>Neuer Abschnitt: Erstellen Sie CloudWatch Alarme in Incident Detection and Response mithilfe von Vorlagen CloudFormation</p> <p>Neuer Abschnitt: Anwendungsbeispiele für CloudWatch Alarme im Bereich Incident Detection and Response</p>	28. September 2023

Änderung	Beschreibung	Datum
Die ersten Schritte wurden aktualisiert	<p>Die ersten Schritte wurden mit Informationen zu Workload-Änderungsanforderungen aktualisiert.</p> <p>Neuer Abschnitt: Fragen Sie in Incident Detection and Response nach Änderungen an einem integrierten Workload</p> <p>Aktualisierter Abschnitt: Abonnieren Sie einen Workload für Incident Detection and Response</p>	05. September 2023
Neuer Abschnitt in Getting Started	Die Erfassung Alarme in AWS Incident Detection and Response aufnehmen von Warnmeldungen wurde zur Erkennung und Reaktion auf AWS Vorfälle hinzugefügt.	30. Juni 2023
Originaldokument	AWSErkennung und Reaktion auf Vorfälle erstmals veröffentlicht	15. März 2023

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.