aws

User Guide

AWS Health



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Health: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die 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 Health? 1
Konzepte für AWS Health 3
AWS Health event 3
Account-specific Ereignis 4
Öffentliche Veranstaltung 4
AWS Health Dashboard 5
AWS Health Dashboard — Zustand des Dienstes 5
Code für den Veranstaltungstyp 5
Kategorien des Veranstaltungstyps 6
Status des Ereignisses 7
Umsetzbarkeit 8
Personas 8
Betroffene Entitäten 9
AWS Health Veranstaltungen auf Amazon EventBridge 9
AWS Health API 9
Organisationsansicht 10
AWS-Benutzerbenachrichtigungen 10
Erste Schritte 11
Registriere dich für einen AWS-Konto 12
Kontoereignisse im AWS Health Dashboard anzeigen 12
Offene und aktuelle Ausgaben 12
Geplante Änderungen 14
Andere Benachrichtigungen 15
Ereignisprotokoll 15
Ereignisdetails 16
Ereignistypen 18
Kalender-Ansicht 18
Ansicht „Betroffene Ressourcen“ 19
Einstellungen für die Zeitzone 21
Der Zustand Ihres Unternehmens 21
Warnmeldungen für AWS Health Veranstaltungen 22
Amazon konfigurieren EventBridge 22
Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen 23

Konfigurieren Sie Ihre AWS Abonnement für verwaltete Benachrichtigungen für AWS Health Veranstaltungen ... 24
AWS Häufig gestellte Fragen zu verwalteten Benachrichtigungen ... 25
AWS Health Dashboard ... 27
Geplante Lebenszyklusereignisse für AWS Health ... 30
Was sind geplante Lebenszyklusereignisse? ... 30
Was kann ich erwarten, wenn ich eine Benachrichtigung über ein geplantes Lebenszyklusereignis erhalte? ... 31
Modell der geteilten Verantwortung für Resilienz ... 33
Zugriff auf geplante Lebenszyklusereignisse ... 34
Integration mit anderen Systemen über die AWS Health API ... 35
Signieren AWS Health API-Anforderungen ... 36
Auswahl von Endpunkten für AWS Health API-Anforderungen ... 36
Demos: Programmgesteuertes Abrufen der Ereignisdaten der letzten sieben Tage ... 38
Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Java ... 38
Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Python ... 41
Tutorial: Verwenden des AWS Health API mit Java-Beispielen ... 44
Schritt 1: Initialisieren der Anmeldeinformationen ... 45
Schritt 2: Initialisieren Sie eine AWS Health API-Client ... 45
Schritt 3: Verwenden AWS Health API-Operationen zum Abrufen von Ereignisinformationen ... 45
Sicherheit ... 49
Datenschutz ... 50
Datenverschlüsselung ... 51
Identity and Access Management ... 51
Zielgruppe ... 52
Authentifizierung mit Identitäten ... 52
Verwalten des Zugriffs mit Richtlinien ... 53
Wie AWS Health funktioniert mit IAM ... 56
Identity-based Beispiele für politische Maßnahmen ... 61
Fehlerbehebung ... 75
Verwenden von servicegebundenen Rollen ... 79
AWS verwaltete Richtlinien für AWS Health ... 80
Einloggen und Überwachen AWS Health ... 86
Compliance-Validierung ... 87
Ausfallsicherheit ... 88

Sicherheit der Infrastruktur ... 88
Konfigurations- und Schwachstellenanalyse ... 89
Bewährte Methoden für die Gewährleistung der Sicherheit ... 89
Gewährung AWS Health mögliche Mindestberechtigungen für Benutzer ... 89
Sehen Sie sich das an Health Dashboard ... 89
Integrieren AWS Health mit Amazon Chime oder Slack ... 89
Überwachen Sie für AWS Health Veranstaltungen ... 89
Zusammenfassen von Ereignissen AWS Health ... 91
Voraussetzungen ... 91
Aktivieren der Organisationsansicht ... 92
Organisationsansicht anzeigen ... 96
Deaktivieren der Organisationsansicht ... 101
Delegierte Administratoransichten für eine Organisation verwalten ... 103
Registrierung eines delegierten Administratorkontos ... 103
Ein delegiertes Administratorkonto entfernen ... 104
Überwachung von Gesundheitsereignissen mit EventBridge ... 105
EventBridge Regeln erstellen für AWS-Region Abdeckung ... 106
Einrichtung für hohe Verfügbarkeit (optional) ... 107
Vereinfachte Integration ... 107
Weltweite Ereignisse ... 108
Überwachung kontospezifischer und öffentlicher Ereignisse für AWS Health ... 108
Backup-Regeln für AWS Health Veranstaltungen ... 109
Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge ... 109
Aggregieren AWS Health Ereignisse mithilfe der Unternehmensansicht und des delegierten Administratorzugriffs ... 110
Integration AWS Health Ereignisüberwachung und Benachrichtigungen mit JIRA und ServiceNow ... 110
Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse . 111
Mithilfe der API oder AWS Command Line Interface ... 112
Konfiguration von Amazon Q Developer in Chat-Anwendungen zum Senden von Benachrichtigungen über Ereignisse ... 114
Voraussetzungen ... 114
Automatisches Ausführen von Vorgängen auf EC2-Instances als Reaktion auf Ereignisse ... 116
Voraussetzungen ... 117
Erstellen Sie eine Regel für EventBridge ... 121
Referenz: AWS Health Veranstaltungen Amazon EventBridge schema ... 124

AWS Health Ereignisschema 124
Veranstaltung im Bereich der öffentlichen Gesundheit — Betriebsproblem bei Amazon EC2 139
Account-specific AWS Health Ereignis — Problem mit der Elastic Load Balancing API 140
Account-specific AWS Health Ereignis — Das Backup-Ereignis für das Amazon EC2 Instance Store-Laufwerk hat sich verschlechtert 141
Account-specific AWS Health Ereignis — Außerbetriebnahme der Amazon EC2-Instance ... 142
Account-specific AWS Health Ereignis — Lambda Planned Lifecycle-Ereignis 143
Überwachen AWS Health 146
Protokollierung AWS Health API-Aufrufe mit AWS CloudTrail 146
AWS Health Informationen in CloudTrail 147
Beispiel: AWS Health Protokolldateieinträge 148
Dokumentverlauf 150
Frühere Aktualisierungen 165
..... clxvii

Was ist AWS Health?

AWS Health bietet fortlaufenden Einblick in die Leistung Ihrer Ressourcen und die Verfügbarkeit Ihrer AWS-Services Konten. Anhand von AWS Health Ereignissen können Sie herausfinden, wie sich Änderungen an Diensten und Ressourcen auf Ihre Anwendungen auswirken können, auf denen Sie ausgeführt AWS werden. AWS Health stellt relevante und aktuelle Informationen bereit, die Sie bei der Verwaltung laufender Ereignisse unterstützen. AWS Health hilft Ihnen auch dabei, sich über geplante Aktivitäten im Klaren zu sein und sich darauf vorzubereiten. Der Service bietet Warnmeldungen und Benachrichtigungen, die bei Änderungen im Zustand der AWS Ressourcen ausgelöst werden, sodass Sie nahezu sofort über Ereignisse informiert und Anleitungen erhalten, um die Problembehebung zu beschleunigen.

Alle Kunden können das AWS Health Dashboard verwenden, das von der AWS Health API unterstützt wird. Das Dashboard erfordert keine Einrichtung und ist für authentifizierte AWS Benutzer sofort einsatzbereit. Weitere Service-Highlights finden Sie auf der AWS Health Dashboard-Detailseite auf der

AWS Health stellt allen Kunden eine Konsole, das sogenannte AWS Health Dashboard, zur Verfügung. Für die Einrichtung des Dashboards müssen Sie weder Code schreiben noch andere Aktionen ausführen.

Um sich mit den Grundlagen AWS Health und Begriffen vertraut zu machen, denen Sie bei der Nutzung des Dienstes begegnen werden, um die Grundlagen von AWS Health see zu verstehenKonzepte für AWS Health.

Hinweise

- Das AWS Health Dashboard steht allen AWS Kunden ohne zusätzliche Kosten zur Verfügung.
- Alle AWS Kunden können ohne zusätzliche Kosten AWS Health Veranstaltungen über Amazon EventBridge erhalten.
- Wenn Sie einen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan haben, können Sie die AWS Health API für die Integration mit internen Systemen und Systemen von Drittanbietern verwenden. Wenn Sie in einem Unternehmen sind AWS-Region , das keinen dieser AWS Support Pläne anbietet, oder wenn Sie noch nicht auf einen dieser Pläne umgestiegen sind, können Sie die AWS Health API mit einem

Business- On-Ramp, Enterprise- oder Enterprise Support-Plan verwenden. Weitere Informationen finden Sie in der AWS Health -API-Referenz.

- Weitere Informationen zu verfügbaren AWS Support Plänen finden Sie unter AWS Support.

Konzepte für AWS Health

Erfahren Sie mehr über AWS Health Konzepte und erfahren Sie, wie Sie den Dienst verwenden können, um den Zustand Ihrer Anwendungen, Dienste und Ressourcen in Ihrem zu gewährleisten AWS-Konto.

Topics

- AWS Health event
- AWS Health Dashboard
- Code für den Veranstaltungstyp
- Kategorien des Veranstaltungstyps
- Status des Ereignisses
- Umsetzbarkeit
- Personas
- Betroffene Entitäten
- AWS Health Veranstaltungen auf Amazon EventBridge
- AWS Health API
- Organisationsansicht
- AWS-Benutzerbenachrichtigungen

AWS Health event

AWS Health Ereignisse, auch bekannt als Integritätsereignisse, sind Benachrichtigungen, die im Namen anderer AWS Dienste AWS Health gesendet werden. Du kannst diese Ereignisse nutzen, um dich über bevorstehende oder geplante Änderungen zu informieren, die sich auf dein Konto auswirken könnten. Sie AWS Health können beispielsweise ein Ereignis senden, wenn AWS Identity and Access Management (IAM) plant, eine verwaltete Richtlinie als veraltet zu betrachten, oder AWS Config plant, eine verwaltete Regel abzuschaffen. AWS Health sendet auch Ereignisse, wenn es in einem zu Problemen mit der Serviceverfügbarkeit kommt. AWS-Region Sie können die Beschreibung des Ereignisses überprüfen, um das Problem zu verstehen, alle betroffenen Ressourcen zu identifizieren und die empfohlenen Maßnahmen zu ergreifen.

Es gibt zwei Arten von Gesundheitsereignissen:

Inhalt

- Account-specific Ereignis
- Öffentliche Veranstaltung

Account-specific Ereignis

Account-specific Ereignisse sind entweder für Sie AWS-Konto oder für ein Konto in Ihrer AWS Organisation lokal. Wenn beispielsweise in einer Region, die Sie verwenden, ein Problem mit einem Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Typ auftritt, AWS Health werden Informationen zum Ereignis und der Name der betroffenen Ressourcen bereitgestellt.

Sie können kontospezifische Ereignisse in Ihrem AWS Health Dashboard oder in der AWS Health API finden oder Amazon- EventBridge oder AWS Benutzerbenachrichtigungen verwenden, um Benachrichtigungen zu erhalten.

Öffentliche Veranstaltung

Öffentliche Ereignisse sind gemeldete Serviceereignisse, die nicht spezifisch für ein Konto sind. Wenn es beispielsweise ein Serviceproblem für Amazon Simple Storage Service (Amazon S3) in der Region USA Ost (Ohio) gibt, AWS Health stellt Informationen zu dem Ereignis bereit, auch wenn Sie diesen Service nicht nutzen oder S3-Buckets in dieser Region haben. Wir empfehlen Ihnen, öffentliche Benachrichtigungen zu überprüfen, bevor Sie entsprechende Maßnahmen ergreifen.

Öffentliche Veranstaltungen findest du in deinem AWS Health Dashboard und im AWS Health Dashboard — Service Health.

> **Important**
>
> Öffentliche Veranstaltungen sind über AWS verwaltete Benachrichtigungen unter nicht verfügbar AWS-Benutzerbenachrichtigungen. Um öffentliche Veranstaltungen zu erhalten, müssen Sie eine EventBridge Amazon-Regel oder eine User-configured Benachrichtigung (UCN) darin AWS-Benutzerbenachrichtigungen erstellen. Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge und Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.

Wenn Sie ein Konto haben, finden Sie weitere Informationen unterErste Schritte mit Ihrem AWS Health Dashboard.

Falls Sie kein Konto haben, finden Sie weitere Informationen unter AWS Health Dashboard.

AWS Health Dashboard

Wenn Sie ein Konto haben AWS-Konto, werden in Ihrem AWS Health Dashboard sowohl öffentliche als auch kontospezifische Ereignisse angezeigt.

Wir empfehlen Ihnen, Ihr AWS Health Dashboard zu verwenden, um sich über Ereignisse zu informieren, die für allgemeine Aufmerksamkeit sorgen, z. B. ein bevorstehendes Wartungsproblem für einen Dienst in einer Region. Sie können das AWS Health Dashboard auch verwenden, um sich über Ereignisse zu informieren, die Sie direkt betreffen könnten, z. B. eine veraltete Ressource in Ihrem Konto.

Sie können sich bei dem AWS-Managementkonsole anmelden, um Ihr AWS Health Dashboard unter einzusehen. https://health.aws.amazon.com/health/home

Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard.

AWS Health Dashboard — Zustand des Dienstes

Wenn Sie kein Konto haben, können Sie das AWS Health Dashboard — Service Health at verwenden https://health.aws.amazon.com/health/status, um öffentliche Veranstaltungen einzusehen. Bei öffentlichen Veranstaltungen handelt es sich um gemeldete Serviceprobleme, bei AWS denen Informationen zur Verfügbarkeit der Dienste bereitgestellt werden. Auf dieser Website werden nur öffentliche Veranstaltungen angezeigt, die für kein Konto spezifisch sind. Du musst dich nicht anmelden oder ein Konto haben, um diese Seite zu sehen.

Weitere Informationen finden Sie unter AWS Health Dashboard.

Code für den Veranstaltungstyp

Die in einem Health-Ereignis angezeigten Ereignistypcodes beinhalten den betroffenen Dienst und die Art des Ereignisses. Wenn Sie beispielsweise ein Health-Ereignis mit dem `AWS_EC2_SYSTEM_MAINTENANCE_EVENT` Ereignistypcode erhalten, bedeutet dies, dass der Dienst ein Wartungsereignis plant, das Sie betreffen könnte. Verwenden Sie diese Informationen, um im Voraus zu planen oder Maßnahmen für Ihr Konto zu ergreifen.

Kategorien des Veranstaltungstyps

Allen Gesundheitsereignissen ist eine Kategorie vom Ereignistyp zugeordnet. Bei einigen Ereignissen erscheint die Kategorie des Ereignistyps möglicherweise im Ereignistypcode, z. B. im `AWS_RDS_MAINTENANCE_SCHEDULED` Code. In diesem Beispiel ist die Kategorie geplant. Sie können diese Informationen verwenden, um die Veranstaltungskategorien auf einer allgemeinen Ebene zu verstehen.

Es hat sich bewährt, alle Kategorien von Ereignistypen zu überwachen. Beachten Sie, dass jede Kategorie für verschiedene Arten von Ereignissen angezeigt wird. Sie können auch die DescribeEventTypes API-Operation verwenden, um die Kategorie des Ereignistyps zu finden.

Benachrichtigung über das Konto

Diese Ereignisse enthalten Informationen über die Verwaltung oder Sicherheit Ihrer Konten und Dienste. Diese Ereignisse können informativ sein oder erfordern möglicherweise dringende Maßnahmen Ihrerseits. Wir empfehlen Ihnen, auf diese Art von Ereignissen zu achten und alle empfohlenen Maßnahmen zu überprüfen.

Im Folgenden finden Sie Beispiele für Ereignistypcodes für Kontobenachrichtigungen:

- `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`— Sie haben einen Amazon S3-Bucket, der möglicherweise öffentlichen Zugriff ermöglicht.
- `AWS_BILLING_SUSPENSION_NOTICE`— Ihr Konto hat ausstehende Gebühren und wurde gesperrt, oder Sie haben Ihr Konto deaktiviert.
- `AWS_WORKSPACES_OPERATIONAL_NOTIFICATION`— Es gibt ein Serviceproblem für Amazon WorkSpaces.

Problem

Bei diesen Ereignissen handelt es sich um unerwartete Ereignisse, die sich auf AWS Dienste oder Ressourcen auswirken. Zu den häufigsten Ereignissen in dieser Kategorie gehören Mitteilungen über Betriebsprobleme, die zu einer Beeinträchtigung der Dienste führen, oder lokalisierte Probleme, die zu Ihrer Information auf Ressourcenebene führen.

Im Folgenden finden Sie Beispiele für Ereignistypcodes für Probleme:

- `AWS_EC2_OPERATIONAL_ISSUE`— Ein Betriebsproblem für einen Dienst, z. B. Verzögerungen bei der Nutzung eines Dienstes.
- `AWS_EC2_API_ISSUE`— Ein Betriebsproblem mit der API eines Dienstes, z. B. eine erhöhte Latenz bei einem API-Vorgang.

- `AWS_EBS_VOLUME_ATTACHMENT_ISSUE`— Ein lokalisiertes Problem auf Ressourcenebene, das sich auf Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen auswirken könnte.
- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT`— Dieses Ereignis bedeutet, dass Ihr Konto möglicherweise gesperrt wird, wenn Sie keine Maßnahmen ergreifen.

Geplante Änderung

Diese Ereignisse informieren über bevorstehende Änderungen an Ihren Diensten und Ressourcen. Zu diesen Ereignissen gehören geplante Lebenszyklusereignisse wie Benachrichtigungen zum Ende des Supports und automatische Upgrades für verschiedene Versionen. Bei einigen Ereignissen wird möglicherweise empfohlen, Maßnahmen zur Vermeidung von Serviceunterbrechungen zu ergreifen, während andere automatisch eintreten, ohne dass Sie etwas unternehmen müssen. Ihre Ressource ist während der geplanten Änderungsaktivität möglicherweise vorübergehend nicht verfügbar. Alle Ereignisse in dieser Kategorie sind kontospezifische Ereignisse.

Im Folgenden finden Sie Beispiele für Ereignistypcodes für geplante Änderungen:

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`— Eine Amazon EC2-Instance erfordert einen Neustart.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker KI erfordert eine Wartung, z. B. die Behebung eines Serviceproblems.
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS plant ein geplantes Lifecycle-Ereignis, z. B. ein Ereignis zum Ende des Supports für eine seiner Versionen, für das ein Eingreifen des Kunden erforderlich ist.

> **Tip**
>
> Wenn Sie die AWS Health API oder AWS Command Line Interface (AWS CLI) verwenden, um Ereignisdetails zurückzugeben, enthält das `Event` Objekt das `eventScopeCode` Feld mit dem `ACCOUNT_SPECIFIC` Wert. Weitere Informationen finden Sie in der AWS Health -API-Referenz.

Status des Ereignisses

Der Eventstatus gibt an, ob das Health-Event geöffnet, geschlossen oder bevorsteht. Du kannst Health-Ereignisse bis zu 90 Tage lang im AWS Health Dashboard oder in der AWS Health API einsehen.

Umsetzbarkeit

Die Handlungsfähigkeit ist ein Feld, das Ihnen hilft, Gesundheitsereignisse danach zu priorisieren, ob eine Aktion von Ihnen erforderlich ist. Zu Gesundheitsereignissen gehört ein Aktionsstatus, der angibt, ob Sie Maßnahmen ergreifen müssen, um die Risiken für Ihre AWS Ressourcen zu minimieren, oder ob das Ereignis informativer Natur ist.

Das Feld „Aktionsfähigkeit“ kann einen der folgenden Werte enthalten:

- `ACTION_REQUIRED`: Bei Ereignissen mit diesem Status müssen Sie Maßnahmen ergreifen, um mögliche Auswirkungen auf die Verfügbarkeit, Abrechnung oder Sicherheit Ihrer AWS Ressourcen zu minimieren.
- `ACTION_MAY_BE_REQUIRED`: Ereignisse mit diesem Status weisen auf Änderungen hin, die je nach Ihrer spezifischen Implementierung, Ihren Abhängigkeiten und Arbeitsabläufen Maßnahmen erfordern. Diese Ereignisse müssen von Ihnen überprüft werden, um festzustellen, ob Maßnahmen erforderlich sind.
- `INFORMATIONAL`: Ereignisse mit diesem Status bieten einen kontinuierlichen Überblick über Betriebsinformationen zu den von Ihnen genutzten AWS Diensten. Es werden keine sofortigen Maßnahmen erwartet.

> **Note**
>
> Integritätsereignisse im Zusammenhang mit Serviceproblemen sind nicht mit einer Kennzeichnung versehen, da die Notwendigkeit von Wiederherstellungsmaßnahmen von Ihrer spezifischen Anwendungsarchitektur abhängt.

Personas

Das Feld Personas enthält eine Liste von Kontakten, anhand derer Sie relevante Informationen an die entsprechenden Teams innerhalb Ihrer Organisation weiterleiten können. Jedes Health-Event kann eine oder mehrere der folgenden Personas umfassen:

- `OPERATIONS`: Für Ereignisse im Zusammenhang mit betrieblichen Aktivitäten und der Verfügbarkeit von Diensten.
- `SECURITY`: Für Ereignisse im Zusammenhang mit Sicherheitsaspekten.

- `BILLING`: Für Ereignisse mit potenziellen Auswirkungen auf die Kosten.

Wenn beispielsweise ein Ereignis zum Ende des Standardsupports AWS gesendet wird, das in einen erweiterten Support umgewandelt wird, wird das Ereignis zusätzlich zu `OPERATIONS` den Personen `BILLING` in der Persona-Liste aufgeführt, um sicherzustellen, dass die Informationen die Teams erreichen, die für das Kostenmanagement verantwortlich sind.

Betroffene Entitäten

Bei den betroffenen Entitäten handelt es sich AWS um Ressourcen, die von dem Ereignis betroffen sein könnten. Wenn Sie beispielsweise ein geplantes Ereignis für die Amazon EC2-Wartung für einen bestimmten Instance-Typ erhalten, den Sie in Ihrem Konto verwenden, können Sie das Health-Ereignis verwenden, um die ID der betroffenen Instances zu ermitteln. Verwenden Sie diese Informationen, um potenzielle Serviceprobleme zu lösen, z. B. beim Erstellen oder Deaktivieren von Ressourcen.

AWS Health Veranstaltungen auf Amazon EventBridge

Sie können EventBridge Amazon-Regeln für Ihre Konten einrichten, um Aktionen zu automatisieren, nachdem das entsprechende AWS Health Ereignis bei einem Konto eingegangen ist. Dabei kann es sich um allgemeine Aktionen handeln, z. B. das Senden aller Nachrichten über geplante Ereignisse im Lebenszyklus an eine Chat-Oberfläche. Es kann sich auch um spezifische Aktionen handeln, z. B. das Auslösen eines Workflows in einem IT-Servicemanagement-Tool.

Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.

AWS Health API

Sie können die AWS Health API verwenden, um programmgesteuert auf die Informationen zuzugreifen, die im AWS Health Dashboard angezeigt werden, z. B. die folgenden:

- Informieren Sie sich über Ereignisse, die sich auf Ihre AWS Dienste und Ressourcen auswirken könnten
- Aktivieren oder deaktivieren Sie die Funktion „Organisationsansicht“ für Ihre AWS Organisation
- Filtern Sie Ihre Veranstaltungen nach bestimmten Diensten, Veranstaltungstypkategorien und Veranstaltungstypcodes

Weitere Informationen finden Sie in der AWS Health -API-Referenz.

> **Note**
>
> Sie müssen über einen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan von verfügen, AWS Support um die AWS Health API verwenden zu können. Wenn Sie die AWS Health API von einem Konto aus aufrufen, für das es keinen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan gibt, erhalten Sie eine `SubscriptionRequiredException` Fehlermeldung.

Organisationsansicht

Mit dieser Funktion können Sie alle Gesundheitsereignisse für AWS Konten in Ihrem Konto AWS Organizations in einer einzigen Ansicht im AWS Health Dashboard zusammenfassen. Sie können sich dann beim Verwaltungskonto Ihrer Organisation anmelden oder die AWS Health API verwenden, um alle Ereignisse anzuzeigen, die sich auf die verschiedenen Konten und Ressourcen auswirken könnten. Sie können diese Funktion über die AWS Health Konsole oder die API aktivieren. Weitere Informationen finden Sie unter Aggregieren AWS Health Ereignisse über Konten hinweg.

AWS-Benutzerbenachrichtigungen

AWS Health lässt sich in integrieren, AWS-Benutzerbenachrichtigungen sodass Sie auf einfache Weise Benachrichtigungen über Ereignisse erhalten und steuern können, die sich auf Ihre AWS-Konten Dienste auswirken. Benutzerbenachrichtigungen bietet standardmäßig verwaltete Benachrichtigungen für AWS Health Ereignisse. Sie können diese Abonnements so konfigurieren, dass Sie steuern, wie oft Sie Nachrichten durch zeitbasierte Aggregation erhalten, über welche Arten von AWS Health Ereignissen Sie benachrichtigt werden und wo Benachrichtigungen zugestellt werden. Um loszulegen, öffnen Sie Benutzerbenachrichtigungen im. AWS-Managementkonsole Weitere Informationen finden Sie unter Verwalten AWS Health Benachrichtigungen in AWS-Benutzerbenachrichtigungen.

Erste Schritte mit Ihrem AWS Health Dashboard

Sie können Ihr AWS Health Dashboard verwenden, um sich über AWS Health Ereignisse zu informieren. Diese Ereignisse können sich auf Ihr AWS-Services oder auswirken AWS-Konto. Nachdem Sie sich bei Ihrem Konto angemeldet haben, zeigt das AWS Health Dashboard Informationen auf folgende Weise an:

- Ihre Kontoereignisse — Auf dieser Seite werden Ereignisse angezeigt, die für Ihr Konto spezifisch sind. Du kannst offene, aktuelle und geplante Änderungen einsehen. Sie können auch Benachrichtigungen und ein Ereignisprotokoll anzeigen, in dem alle Ereignisse der letzten 90 Tage aufgeführt sind.
- Ereignisse in Ihrer Organisation — Auf dieser Seite werden Ereignisse angezeigt, die für Ihre Organisation spezifisch sind AWS Organizations. Sie können offene, aktuelle und geplante Änderungen für Ihre Organisation einsehen. Sie können auch Benachrichtigungen sowie ein Ereignisprotokoll einsehen, in dem alle Organisationsereignisse der letzten 90 Tage aufgeführt sind.

> **Note**
>
> Wenn Sie noch keinen haben, können Sie AWS-Konto ihn verwenden, AWS Health Dashboard um sich über die allgemeine Verfügbarkeit von Diensten zu informieren. Wenn Sie ein Konto haben, empfehlen wir Ihnen, sich in Ihrem AWS Health Dashboard anzumelden, um tiefere Einblicke in Ereignisse und bevorstehende Änderungen zu erhalten, die sich auf Ihre Dienste und Ressourcen auswirken könnten.

Themen

- Registriere dich für einen AWS-Konto
- Anzeigen Ihrer Kontoereignisse in der AWS Health Dashboard
- Amazon konfigurieren EventBridge
- Verwalten AWS Health Benachrichtigungen in AWS-Benutzerbenachrichtigungen

Registriere dich für einen AWS-Konto

Um damit zu beginnen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen einer AWS-Konto finden Sie AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch unter Erste Schritte mit einer.

Anzeigen Ihrer Kontoereignisse in der AWS Health Dashboard

Sie können sich in Ihrem Konto anmelden, um personalisierte Veranstaltungen und Empfehlungen zu erhalten.

Um Kontoereignisse in Ihrem Konto anzuzeigen AWS Health Dashboard

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Im Navigationsbereich können Sie für den Status Ihres Kontos die folgenden Optionen auswählen:

   a. Offene und aktuelle Ausgaben — Zeigt kürzlich geöffnete und geschlossene Veranstaltungen an.

   b. Geplante Änderungen — Sehen Sie sich bevorstehende Ereignisse an, die sich auf Ihre Dienste und Ressourcen auswirken könnten.

   c. Weitere Benachrichtigungen — Sieh dir alle anderen Benachrichtigungen und laufenden Ereignisse der letzten sieben Tage an, die sich auf dein Konto auswirken könnten.

   d. Ereignisprotokoll — Zeigt alle Ereignisse der letzten 90 Tage an.

Offene und aktuelle Ausgaben

Auf dem Tab Offene und aktuelle Probleme kannst du dir alle aktuellen Ereignisse der letzten sieben Tage ansehen, die sich auf dein Konto auswirken könnten.

Wenn Sie im Dashboard ein Ereignis auswählen, wird der Detailbereich mit Informationen zum Ereignis und einer Liste der betroffenen Ressourcen angezeigt. Weitere Informationen finden Sie unter Ereignisdetails.

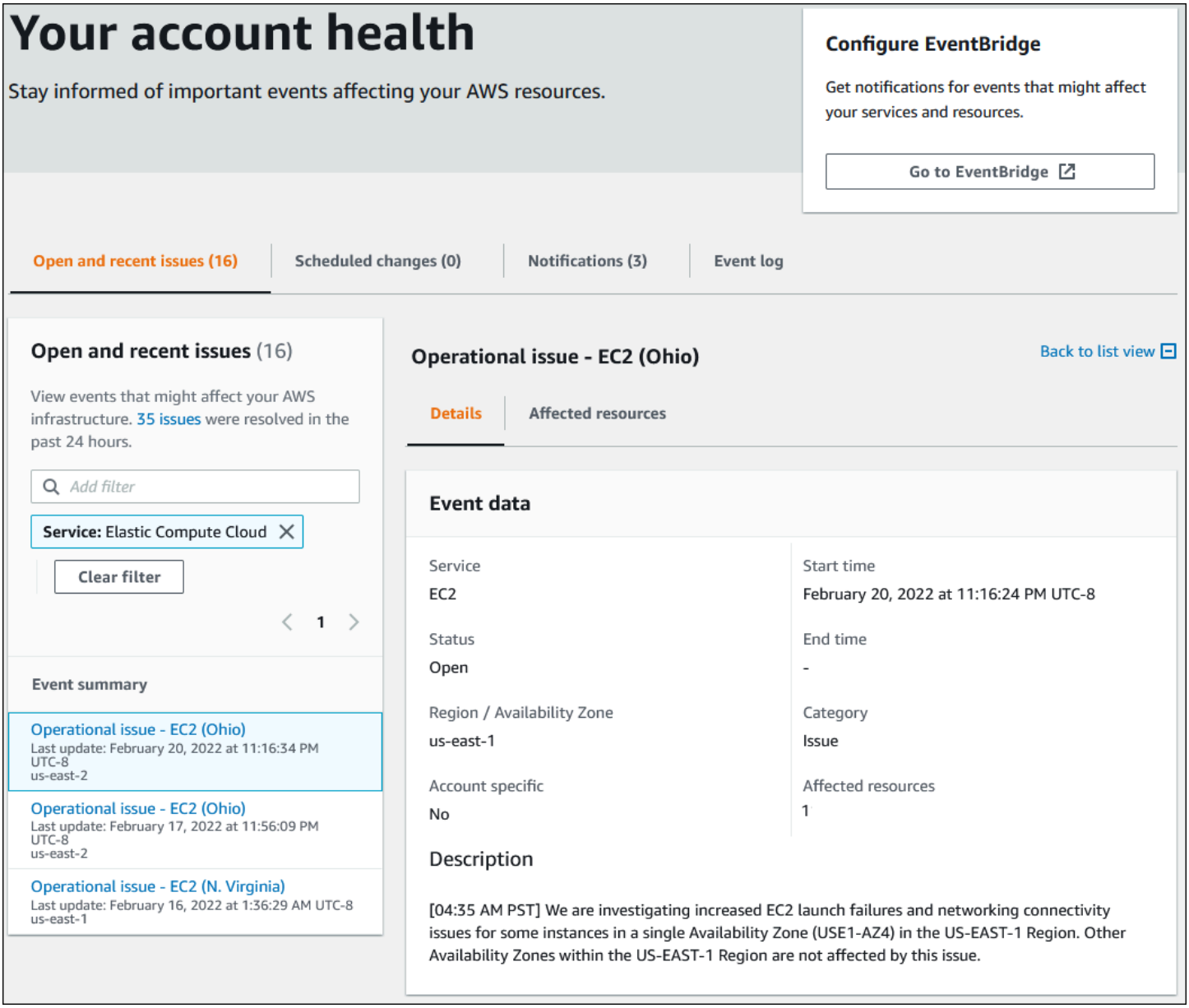
Sie können die Ereignisse, die auf einer beliebigen Registerkarte angezeigt werden, filtern, indem Sie Optionen aus der Filterliste auswählen. Sie können die Ergebnisse beispielsweise nach Availability Zone, Region, Endzeit der Veranstaltung oder Uhrzeit der letzten Aktualisierung AWS-Service usw. eingrenzen.

Um alle Ereignisse und nicht die letzten, die im Dashboard angezeigt werden, zu sehen, wählen Sie den Ereignisprotokoll Tab.

> **Note**
>
> Derzeit können Sie keine Benachrichtigungen für Ereignisse löschen, die in Ihrem AWS Health Dashboard angezeigt werden. Nachdem ein Ereignis AWS-Service behoben wurde, wird die Benachrichtigung aus Ihrer Dashboard-Ansicht entfernt.

Example: Ereignis mit Betriebsproblemen bei Amazon Elastic Compute Cloud (Amazon EC2)

Die folgende Abbildung zeigt ein Ereignis mit Startfehlern und Verbindungsproblemen für Amazon EC2-Instances.



Geplante Änderungen

Verwenden Sie den Tab Geplante Änderungen, um bevorstehende Ereignisse anzuzeigen, die sich auf Ihr Konto auswirken könnten. Zu diesen Ereignissen können geplante Wartungsaktivitäten für Dienste und geplante Lebenszyklusereignisse gehören, für deren Behebung Maßnahmen erforderlich sind. Um Ihnen bei der Planung dieser Aktivitäten zu helfen, steht eine Kalenderansicht zur Verfügung, sodass Sie diese geplanten Änderungen in einem Monatskalender zusammenfassen können. Filter sind verfügbar. Weitere Informationen zu geplanten Lebenszyklusereignissen finden Sie unterGeplante Lebenszyklusereignisse für AWS Health.

Andere Benachrichtigungen

Verwende den Tab Benachrichtigungen, um alle anderen Benachrichtigungen und laufenden Ereignisse der letzten sieben Tage anzuzeigen, die sich auf dein Konto auswirken könnten. Dazu können Ereignisse wie Zertifikatsrotationen, Abrechnungsbenachrichtigungen und Sicherheitslücken gehören.

Ereignisprotokoll

Verwenden Sie die Registerkarte „Ereignisprotokoll“, um alle AWS Health Ereignisse anzuzeigen. Die Protokolltabelle enthält zusätzliche Spalten, sodass Sie nach Status und Startzeit filtern können.

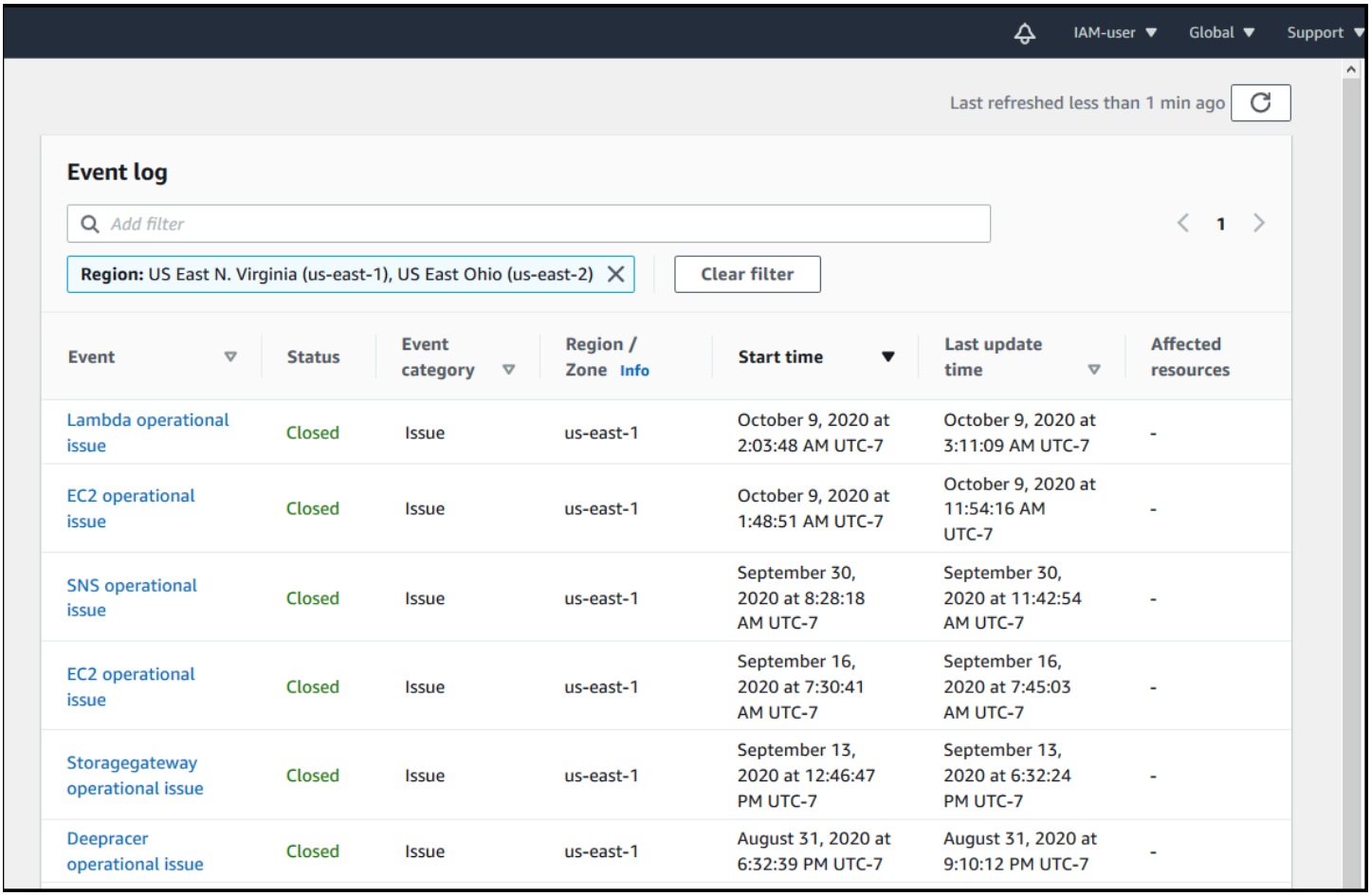
Wenn Sie ein Ereignis in der Tabelle mit den Ereignisprotokollen auswählen, wird der Detailbereich mit Informationen zum Ereignis und der Liste der betroffenen Ressourcen angezeigt. Weitere Informationen finden Sie unter Ereignisdetails.

Sie können die folgenden Filteroptionen wählen, um Ihre Ergebnisse einzugrenzen:

- Availability Zone
- Endzeit
- Veranstaltung
- Ereignis ARN
- Ereigniskategorie
- Uhrzeit der letzten Aktualisierung
- Region
- Ressourcen-ID//ARN
- Service
- Startzeit
- Status

Example: Ereignisprotokoll

Die folgende Abbildung zeigt die jüngsten Ereignisse für die Regionen USA Ost (Nord-Virginia) und USA Ost (Ohio).



Ereignisdetails

Wenn Sie ein Ereignis auswählen, werden zwei Tabs zu dem Ereignis angezeigt. Auf der Registerkarte „Details“ werden die folgenden Informationen angezeigt:

- Service
- Status
- Region/Verfügbarkeitszone
- Ob das Ereignis kontospezifisch ist oder nicht
- Start- und Endzeit
- Kategorie
- Anzahl der betroffenen Ressourcen
- Beschreibung und Zeitplan mit aktuellen Informationen zur Veranstaltung

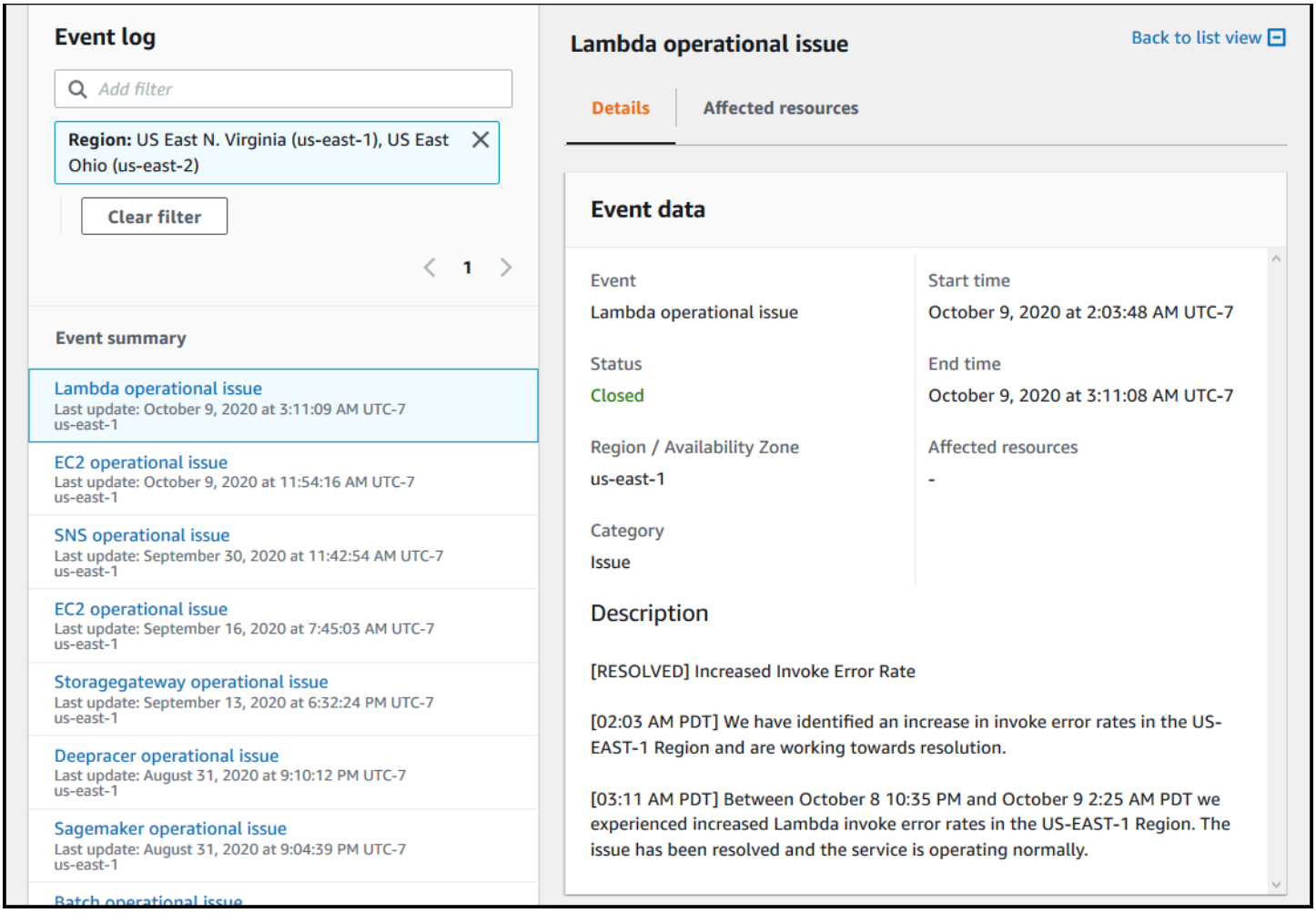
Auf der Registerkarte Betroffene Ressourcen werden die folgenden Informationen zu allen AWS Ressourcen angezeigt, die von dem Ereignis betroffen sind:

- Die Ressourcen-ID (z. B. eine Amazon EBS-Volume-ID wie`vol-a1b2c34f`) oder der Amazon-Ressourcenname (ARN), falls verfügbar oder relevant.
- Bei geplanten Lebenszyklusereignissen enthält diese Liste der betroffenen Ressourcen auch den aktuellen Status der Ressourcen (Ausstehend , Unbekannt oder Gelöst). Diese Liste wird in der Regel alle 24 Stunden aktualisiert, es kann jedoch bis zu 72 Stunden dauern, bis sie den aktuellen Status wiedergibt.

Sie können die Elemente filtern, die in den Ressourcen angezeigt werden. Sie können Ihre Ergebnisse nach Ressourcen-ID oder ARN eingrenzen.

Example: AWS Health Veranstaltung für AWS Lambda

Der folgende Screenshot zeigt ein Beispielereignis für Lambda.



Ereignistypen

Es gibt zwei Arten von AWS Health Ereignissen:

- Öffentliche Ereignisse sind Serviceereignisse, die nicht spezifisch für ein Konto sind. Wenn beispielsweise in einem ein Problem mit Amazon EC2 auftritt AWS-Region, AWS Health werden Informationen zu dem Ereignis bereitgestellt, auch wenn Sie in dieser Region keine Dienste oder Ressourcen nutzen.
- Account-specificEreignisse sind spezifisch für Ihr Konto oder ein Konto in Ihrer Organisation. Wenn beispielsweise ein Problem mit einer Amazon EC2-Instance in einer, AWS-Region die Sie verwenden, auftritt, werden Informationen über das Ereignis und die Liste der betroffenen Amazon EC2-Instances AWS Health bereitgestellt.

Sie können die folgenden Optionen verwenden, um festzustellen, ob ein Ereignis öffentlich oder kontospezifisch ist:

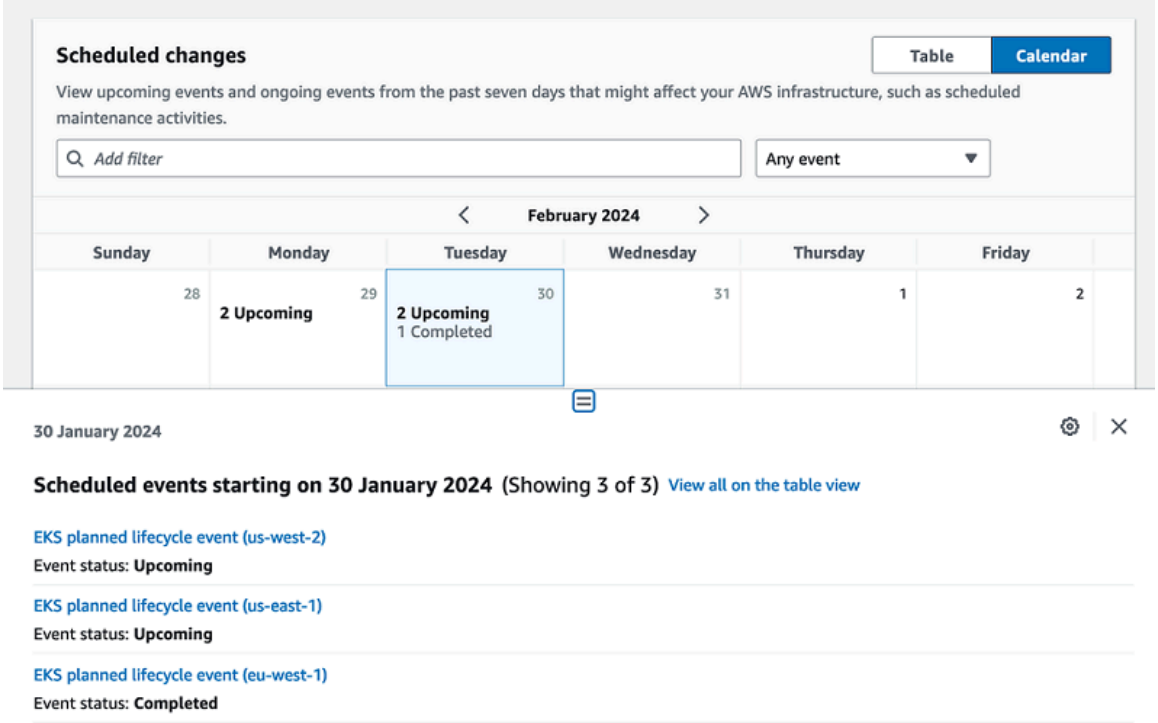
- Wählen Sie im AWS Health Dashboard den Tab Betroffene Ressourcen für ein Ereignis aus. Ereignisse mit Ressourcen sind spezifisch für Ihr Konto. Ereignisse ohne Ressourcen sind öffentlich und sind nicht spezifisch für Ihr Konto. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard.
- Verwenden Sie die AWS Health API, um den `eventScopeCode` Parameter zurückzugeben. Ereignisse können den Wert `PUBLIC`, `ACCOUNT_SPECIFIC`, oder `NONE` haben. Weitere Informationen finden Sie unter dem DescribeEventDetails Vorgang in der AWS Health API-Referenz.

Kalender-Ansicht

Die Kalenderansicht ist auf der Registerkarte „Geplante Änderungen“ verfügbar, um AWS Health Ereignisse in einen Monatskalender zu projizieren. In dieser Ansicht können Sie geplante Änderungen sehen, die bis zu 3 Monate in der Vergangenheit und ein Jahr in der Zukunft zurückliegen.

AWS Health Ereignisse werden nach Datum sortiert angezeigt. Wählen Sie ein Datum aus, um ein Seitenfenster mit weiteren Informationen zum AWS Health Ereignis anzuzeigen. Kommende und laufende Ereignisse werden schwarz angezeigt. Abgeschlossene Ereignisse werden grau angezeigt. Wenn ein Datum mehr als zwei Ereignisse enthält, wird nur die Anzahl der schwarzen und grauen Ereignisse angezeigt. Wählen Sie ein Datum aus, um eine Liste der AWS Health Ereignisse

im Seitenbereich anzuzeigen. Sie können im Seitenbereich ein Ereignis auswählen, um Informationen zu dem Ereignis anzuzeigen. Im Seitenbereich befinden sich Breadcrumbs, mit denen Sie zu einer früheren Ansicht navigieren können.



Ansicht „Betroffene Ressourcen“

AWS Health Ereignisse können die genauen Ressourcen angeben, die betroffen sind. Sie können die betroffenen Ressourcen auf der Registerkarte „Betroffene Ressourcen“ des AWS Health Ereignisses einsehen. Um den Status anzuzeigen, wählen Sie das AWS Health Ereignis aus. Der Status wird auf der Registerkarte „Betroffene Ressourcen“ im Seitenbereich angezeigt. Bei geplanten AWS Health Lebenszyklusereignissen bieten Ereignisse tägliche Aktualisierungen des Status der betroffenen Ressourcen.

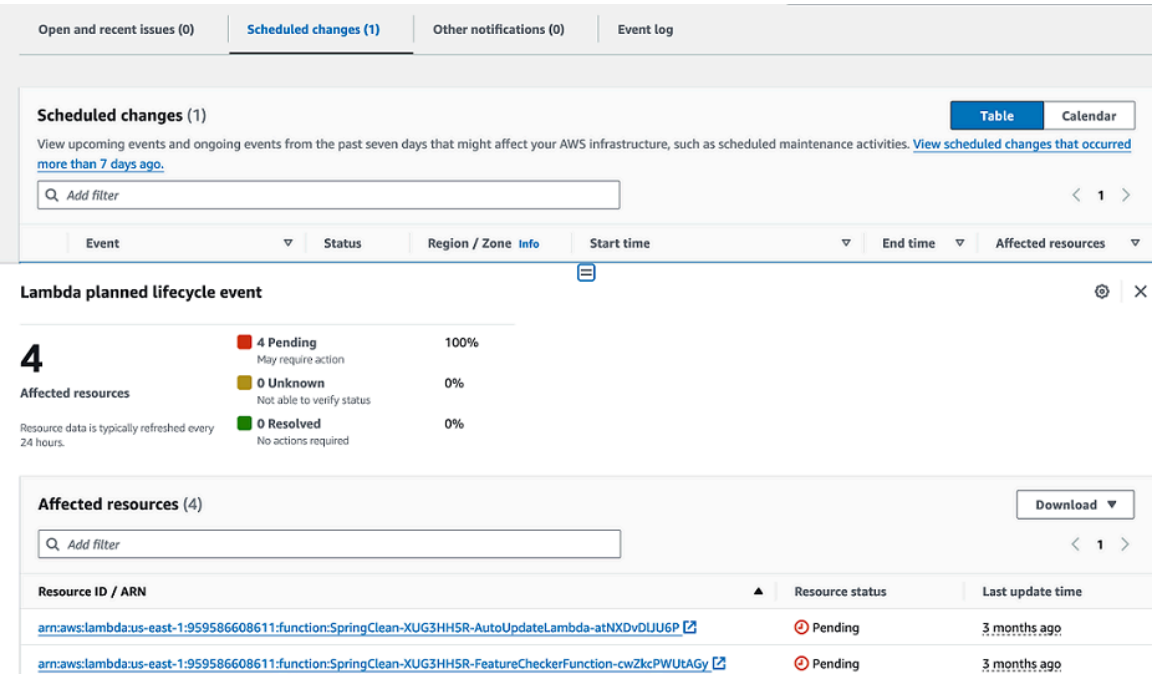
Account-level AWS Health Ereignisse zeigen oben auf der Registerkarte „Betroffene Ressourcen“ eine Zusammenfassung des Status der betroffenen Ressourcen an. Eine Liste der betroffenen Ressourcen wird zusammen mit dem entsprechenden Status in einer Tabelle angezeigt. Geplante Lebenszyklusereignisse sind ein Beispiel für Ereignistypen, die das Feld Ressourcenstatus verwenden. Weitere Informationen zu geplanten Lebenszyklusereignissen finden Sie unterGeplante Lebenszyklusereignisse für AWS Health.

Wenn Sie auf die Organisationsansicht zugreifen, wird im Rahmen von AWS Health Ereignissen eine Zusammenfassung des Status aller betroffenen Ressourcen für alle enthaltenen Konten angezeigt.

Nach der Zusammenfassung finden Sie eine Liste der betroffenen Konten und die Anzahl der ausstehenden Ressourcen für dieses Konto. Wählen Sie die Kontonummer oder die Anzahl der ausstehenden Ressourcen aus, um die Kontoübersicht anzuzeigen. Die Zusammenfassung der Kontoansicht enthält Breadcrumbs, mit denen Sie zur Organisationsliste der betroffenen Konten zurückkehren können. Eine Zusammenfassung des Status der betroffenen Ressourcen wird oben im geteilten Bereich angezeigt.

Sie können die Liste der betroffenen Ressourcen auf der Registerkarte „Betroffene Ressourcen“ im CSV- oder JSON-Format herunterladen. In der Unternehmensansicht enthält die heruntergeladene Datei alle Ressourcen in den aufgelisteten Konten. Navigieren Sie in der Organisationsansicht zur Kontoebene, um nur Ressourcen für dieses Konto in die heruntergeladene Datei aufzunehmen. Jede betroffene Ressource in der heruntergeladenen Datei enthält die AWS-Konto ID, die EventArn, den Entitätsnamen, die EntityARN, den Status und die Uhrzeit der letzten Aktualisierung der Ressource. Wenn Filter aktiviert sind, enthält die heruntergeladene Datei nur die gefilterten Ergebnisse.

Sie können jeweils nur eine Datei herunterladen. Die Dateien werden automatisch in den Standard-Download-Ordner Ihres Browsers heruntergeladen und haben einen voreingestellten Dateinamen AWS-Region, der auf dem Veranstaltungstitel, dem Startdatum der Veranstaltung und dem Download-Datum basiert.



Einstellungen für die Zeitzone

Sie können die Ereignisse im AWS Health Dashboard in Ihrer lokalen Zeitzone oder in UTC anzeigen. Wenn Sie die Zeitzone in Ihrem AWS Health Dashboard ändern, werden alle Zeitstempel im Dashboard und öffentliche Ereignisse auf die von Ihnen angegebene Zeitzone aktualisiert.

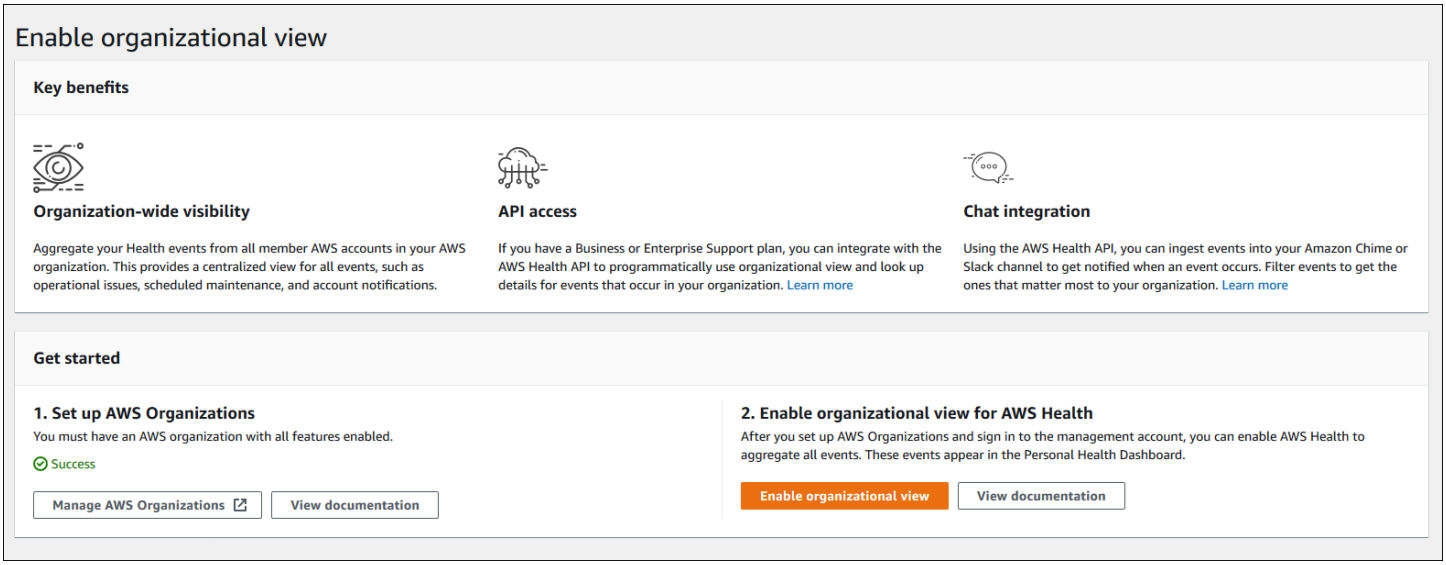
Um deine Zeitzoneneinstellungen zu aktualisieren

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie unten auf der Seite die Option Cookie-Einstellungen aus.
3. Wählen Sie für funktionale Cookies die Option Zulässig aus. Wählen Sie dann Einstellungen speichern.
4. Wählen Sie im Navigationsbereich Ihres AWS Health Dashboards Zeitzoneneinstellungen aus.
5. Wählen Sie eine Zeitzone für Ihre AWS Health Dashboard-Sitzungen aus. Wählen Sie dann Save changes (Änderungen speichern).

Der Zustand Ihres Unternehmens

AWS Health integriert mit, AWS Organizations sodass Sie Ereignisse für alle Konten anzeigen können, die Teil Ihrer Organisation sind. Auf diese Weise erhalten Sie eine zentrale Ansicht für Ereignisse, die in Ihrer Organisation angezeigt werden. Sie können diese Ereignisse verwenden, um Änderungen in Ihren Ressourcen, Services und Anwendungen zu überwachen.

Weitere Informationen finden Sie unter Aggregieren AWS Health Ereignisse über Konten hinweg.



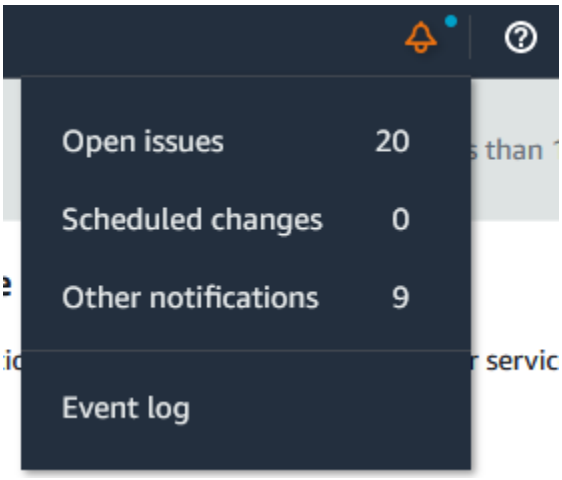
Warnmeldungen für AWS Health Veranstaltungen

Ihr AWS Health Dashboard hat ein Glockensymbol in der Navigationsleiste der Konsole mit einem Warnmenü. Diese Funktion zeigt die Anzahl der letzten AWS Health Ereignisse an, die im Dashboard in jeder Kategorie angezeigt werden. Dieses Glockensymbol erscheint auf mehreren AWS Konsolen, z. B. auf den Konsolen für Amazon EC2, Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM) und. AWS Trusted Advisor

Wählen Sie das Glockensymbol, um zu sehen, ob sich aktuelle Ereignisse auf Ihr Konto auswirken. Sie können dann ein Ereignis auswählen, um zu Ihrem AWS Health Dashboard zu gelangen, um weitere Informationen zu erhalten.

Example: Ereignisse öffnen

Die folgende Abbildung zeigt Öffnungs- und Benachrichtigungsereignisse für ein Konto.



Amazon konfigurieren EventBridge

Wird verwendet EventBridge , um Änderungen bei AWS Health Ereignissen zu erkennen und darauf zu reagieren. Sie können bestimmte AWS Health Ereignisse in Ihrem Konto überwachen und dann Regeln einrichten, sodass Sie AWS Health benachrichtigt werden oder Maßnahmen ergreifen, wenn sich Ereignisse ändern.

Verwenden Sie mit EventBridge AWS Health

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Gehen Sie wie folgt vor, um zur EventBridge Konsole zu navigieren und eine Regel zu erstellen:

- Wählen Sie im Navigationsbereich unter Health Integrations die Option Amazon EventBridge aus.
- Wählen Sie unter Konfigurieren EventBridge die Option Gehe zu EventBridge aus.

3. Gehen Sie wie folgt vor, um Regeln zu erstellen und Ereignisse zu überwachen. Siehe Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.

Verwalten AWS Health Benachrichtigungen in AWS-Benutzerbenachrichtigungen

> **Important**
>
> Öffentliche Veranstaltungen sind über AWS verwaltete Benachrichtigungen in nicht verfügbar AWS-Benutzerbenachrichtigungen. Um öffentliche Veranstaltungen zu erhalten, müssen Sie eine EventBridge Amazon-Regel oder eine User-configured Benachrichtigung (UCN) darin AWS-Benutzerbenachrichtigungen erstellen. Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge und Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.

AWS Mit verwalteten Benachrichtigungen in AWS-Benutzerbenachrichtigungen können Sie Benachrichtigungen über Ereignisse, die sich auf Ihre AWS-Konten und Ihre Dienste auswirken, empfangen und verwalten. Wenn Sie AWS verwaltete Benachrichtigungen in verwenden AWS-Benutzerbenachrichtigungen, können Sie angeben, welche AWS Health Ereigniskategorien Sie erhalten möchten, eine organisatorische Ansicht für E-Mails einrichten und konsolidierte Benachrichtigungen anstelle mehrerer ähnlicher E-Mails erhalten.

Sie können die folgenden zusätzlichen Kanäle auswählen, über die Sie Ihre AWS Health Ereignisse erhalten möchten AWS-Benutzerbenachrichtigungen:

- Email
- Chat
- Push-Benachrichtigungen an AWS Console Mobile Application

Diese Benachrichtigungen sind zwar nicht so detailliert wie direkte AWS Health Tools, bieten aber eine effektive Möglichkeit, Stakeholder über Probleme und Änderungen zu informieren.

> **Note**
>
> Für einen umfassenden Überblick über die AWS Health Veranstaltungsdetails, einschließlich der betroffenen Ressourcen-IDs, des aktuellen Status (offen oder geschlossen) und des Ressourcenstatus, empfiehlt es sich, eines der folgenden AWS Health Tools zu verwenden:
>
> - Die AWS Health API
> - Die aws.health-Quelle bei Amazon EventBridge
> - Die Health Dashboard
>
> Diese Tools bieten die detailliertesten Echtzeitinformationen zu laufenden Ereignissen und Änderungen, die sich auf Ihre Workloads auswirken könnten.

Konfigurieren Sie Ihre AWS Abonnement für verwaltete Benachrichtigungen für AWS Health Veranstaltungen

Gehen Sie wie folgt vor, um Ihr Abonnement für AWS verwaltete Benachrichtigungen zu konfigurieren:

1. Öffnen Sie Benutzerbenachrichtigungen in der AWS-Managementkonsole.
2. Wählen Sie im Navigationsbereich Abonnements für AWS verwaltete Benachrichtigungen aus.
3. Sie können Ihre AWS Health Event-Benachrichtigungen nach Kategorien verwalten. Weitere Informationen findest du unter Hinzufügen und Entfernen von Kontokontakten für AWS verwaltete Benachrichtigungen in AWS-Benutzerbenachrichtigungen.

> **Note**
>
> AWS Health hat die E-Mail-Zustellung zu AWS verwalteten Benachrichtigungen in AWS-Benutzerbenachrichtigungen migriert. Seit dem 15. Dezember 2025 erhalten Sie E-Mails von AWS verwalteten Benachrichtigungen. Weitere Informationen findest du unter Was hat sich bei der Migration zu AWS verwalteten Benachrichtigungen geändert? in derAWS verwaltete Benachrichtigungen in AWS Häufig gestellte Fragen zu Benutzerbenachrichtigungen.

AWS verwaltete Benachrichtigungen in AWS Häufig gestellte Fragen zu Benutzerbenachrichtigungen

Was hat sich bei der Migration zu geändert AWS verwaltete Benachrichtigungen?

Standardmäßig werden E-Mails zu verwalteten Benachrichtigungen an Ihre bestehenden Kontokontakte (Root-, Betriebs-, Rechnungs- und Sicherheits-E-Mail-Adressen) gesendet. Die E-Mails, die Sie über AWS verwaltete Benachrichtigungen erhaltenno-reply-aws@amazon.com, stammen von health@aws.com statt und das Format der E-Mail ändert sich. Wenn Sie zuvor E-Mail-Regeln für AWS Health Benachrichtigungen eingerichtet haben, z. B. das Weiterleiten einer E-Mail nach Absender-ID oder das Löschen des E-Mail-Inhalts, müssen Sie diese Konfiguration aktualisieren, damit sie dem neuen E-Mail-Format entspricht. Wenn Sie eine Automatisierung durch Push-Benachrichtigungen benötigen, empfehlen wir Ihnen, AWS Health Ereignisse, die über Amazon gesendet werden, EventBridge als Alternative zu verwalteten Benachrichtigungen zu evaluieren.

Wie funktioniert die Aggregation für E-Mails und wie aktiviere ich diese Funktion?

AWS Eine verwaltete Benachrichtigung fasst AWS Health Ereignisse, die sich auf mehrere Konten innerhalb derselben AWS Organizations Organisation auswirken, in einer einzigen aggregierten Benachrichtigung zusammen. Sie können die aggregierte Organisation im Benachrichtigungscenter des Verwaltungskontos einsehen. Verwaltete Benachrichtigungen senden die aggregierten Benachrichtigungen per E-Mail an die Kontakte des Verwaltungskontos. Um doppelte E-Mails zu vermeiden, sendet AWS verwaltete Benachrichtigungen eine Benachrichtigung, wenn Kontokontakte zwischen Verwaltungs- und Mitgliedskonten gemeinsam genutzt werden.

Um die Aggregation zu aktivieren, müssen Sie den vertrauenswürdigen Zugriff zwischen Ihrem Verwaltungskonto und dem AWS-Benutzerbenachrichtigungen Dienst AWS Organizations konfiguriert und gewährt haben.

Weitere Informationen finden Sie unter Aggregation AWS verwalteter Benachrichtigungen unter. AWS-Benutzerbenachrichtigungen

Muss ich aktivieren AWS Organizations vertrauenswürdiger Zugriff mit AWS-Benutzerbenachrichtigungen um aggregierte E-Mails zu erhalten von AWS verwaltete Benachrichtigungen?

Ja, vertrauenswürdiger Zugriff mit AWS-Benutzerbenachrichtigungen von AWS Organizations ist erforderlich.

Was ist der Unterschied zwischen der Aktivierung von vertrauenswürdigem Zugriff durch AWS Organizations mit AWS Health und mit AWS-Benutzerbenachrichtigungen?

Das Vertrauen der Organisation und die damit verbundenen delegierten Administratorrechte werden vom Dienst vergeben und dienen als Schutzmaßnahmen gegen überzogene Berechtigungen. Der vertrauenswürdige Zugriff für AWS Health ermöglicht den organisatorischen Überblick über die AWS Health APIs Health Dashboard, die über Amazon gesendeten AWS Health Ereignisse und die EventBridge Benachrichtigungskonfigurationen in. Benutzerbenachrichtigungen Der vertrauenswürdige Zugriff auf AWS-Benutzerbenachrichtigungen ermöglicht die Zusammenfassung von Benachrichtigungen innerhalb AWS verwalteter Benachrichtigungen. Da vertrauenswürdiger Zugriff nicht gemeinsam genutzt wird, muss die Einrichtung delegierter Administratoren für jeden Dienst separat hinzugefügt werden.

Gibt es eine Möglichkeit, Klartext-E-Mails für meinen speziellen Anwendungsfall aufzubewahren?

Nein. Die aktuellen AWS Health Klartext-E-Mails werden nach Abschluss der Migration deaktiviert. Wenn Sie E-Mail-Regeln verwenden, um verschiedene Workflows zu steuern, empfehlen wir Ihnen, die über Amazon gesendeten AWS Health Ereignisse EventBridge als Alternative zu evaluieren.

Was tun AWS Die Kategorien für verwaltete Benachrichtigungen entsprechen den AWS Health Schema?

Statusmeldungen, Sicherheitsinformationen und Abrechnungsbenachrichtigungen entsprechen AWS Health Kontobenachrichtigungen und geplanten Änderungen, an denen jeweils die Personen für Betrieb, Sicherheit und Abrechnung beteiligt sind. AWS Health Ereignisse mit mehr als einem Persona-Tag werden über die Kategorien Sicherheit und Abrechnung versendet. Account-specific Zu den Problemen gehören Gesundheitsereignisse der Problemkategorie, die spezifisch für einen AWS-Konto sind.

Öffentliche Veranstaltungen sind nicht über AWS verwaltete Benachrichtigungen verfügbar.

AWS Health Dashboard

Sie können das AWS Health Dashboard — Dienststatus verwenden, um den Status aller Benutzer einzusehen AWS-Services. Auf dieser Seite werden gemeldete Serviceereignisse für alle Dienste angezeigt AWS-Regionen. Sie müssen sich nicht anmelden oder eine haben, AWS-Konto um auf die Seite AWS Health Dashboard — Servicestatus zuzugreifen.

> **Tip**
>
> Auf dieser Website werden nur öffentliche Ereignisse angezeigt, die nicht spezifisch für eine sind AWS-Konto. Wenn Sie bereits ein Konto haben, empfehlen wir Ihnen, sich anzumelden, um Ihr AWS Health Dashboard aufzurufen und über Ereignisse informiert zu werden, die sich auf Ihr Konto und Ihre Dienste auswirken können. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard.

Um das anzusehen AWS Health Dashboard — Zustand des Dienstes

1. Navigieren Sie zur Seite https://health.aws.amazon.com/health/status.

   > **Note**
   >
   > Wenn Sie bereits auf Ihrer AWS-Konto Seite angemeldet sind, werden Sie zur Seite AWS Health Dashboard — Ihr Kontostatus weitergeleitet.

2. Wählen Sie unter Dienststatus die Option Offene und aktuelle Probleme aus, um sich die kürzlich gemeldeten Ereignisse anzusehen. Sie können die folgenden Informationen zu dem Ereignis einsehen:

   - Der Name des Ereignisses und die betroffene Region. Zum Beispiel Betriebsproblem — Amazon Elastic Compute Cloud (Nord-Virginia)
   - Der Name des Services
   - Der Schweregrad des Ereignisses, z. B. Beeinträchtigt oder Beeinträchtigt
   - Eine Zeitleiste der letzten Aktualisierungen für das Ereignis
   - Eine Liste von Personen AWS-Services , die ebenfalls von diesem Ereignis betroffen sind

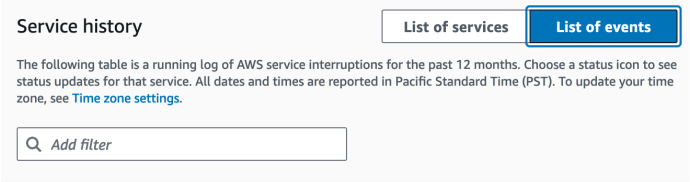
> **Note**
>
> Sie können die Ereignisse in Ihrer lokalen Zeitzone oder in UTC anzeigen. Weitere Informationen finden Sie unter Zeitzoneneinstellungen.

3. Wählen Sie Serviceverlauf, um die Tabelle mit dem Serviceverlauf anzuzeigen. In dieser Tabelle sind alle AWS-Service Unterbrechungen der letzten 12 Monate aufgeführt.

> **Tip**
>
> Sie können nach Service AWS-Region, und Datum filtern.

4. Wählen Sie neben einem laufenden Serviceereignis das Statussymbol ( ) aus, um weitere Informationen zu dem Ereignis anzuzeigen.

5. (Optional) Um diese Liste als Liste historischer Ereignisse anzuzeigen, klicken Sie auf die Schaltfläche „Liste der Ereignisse“. Wählen Sie ein Ereignis in der Ereignisspalte aus, um weitere Informationen zu diesem bestimmten Ereignis im Popup-Seitenbereich anzuzeigen.



> **Note**
>
> Wenn Sie eine öffentliche Veranstaltung nach September 2023 auswählen, wird die URL im Browser mit einem Link zu dieser öffentlichen AWS Health Veranstaltung gefüllt. Nachdem Sie diesen Link ausgewählt haben, navigieren Sie zur Ansicht mit der Liste der Ereignisse mit diesem Event-Popup.

6. (Optional) Sie können die Ereignisse in Ihrer lokalen Zeitzone oder in UTC anzeigen. Weitere Informationen finden Sie unter Einstellungen für die Zeitzone.

7. (Optional) Wenn Sie ein Konto haben, wählen Sie Öffnen Sie Ihren Kontostatus, um sich anzumelden. Nachdem Sie sich angemeldet haben, können Sie sich Ereignisse ansehen, die für

Ihr Konto spezifisch sind. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard.

> **Note**
>
> Für Gesundheitsereignisse ist zwar ein RSS-Feed verfügbar, das Format kann sich jedoch ändern. Das Scrapen des RSS-Feeds liefert also möglicherweise nicht alle relevanten Daten. Um Daten zu Gesundheitsereignissen programmatisch aufzunehmen, empfehlen wir die Integration mit Amazon. EventBridge Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.

Geplante Lebenszyklusereignisse für AWS Health

Erfahren Sie mehr über geplante Lebenszyklusereignisse für AWS Health.

Topics

- Was sind geplante Lebenszyklusereignisse?
- Was kann ich erwarten, wenn ich eine Benachrichtigung über ein geplantes Lebenszyklusereignis erhalte?
- Modell der geteilten Verantwortung für Resilienz
- Zugriff auf geplante Lebenszyklusereignisse

Was sind geplante Lebenszyklusereignisse?

AWS Health kommuniziert wichtige Änderungen, die sich auf die Verfügbarkeit Ihrer Anwendungen auswirken können. AWS Ergreift im AWS Rahmen des Modells der gemeinsamen Verantwortung Maßnahmen, um die zugrunde liegende Hardware und Infrastruktur, die Ihre Ressourcen unterstützen, auf dem neuesten Stand und sicher zu halten. Einige Änderungen erfordern jedoch Maßnahmen oder eine Abstimmung durch den Kunden, um Auswirkungen auf Ihre Anwendungen zu vermeiden. AWS Health informiert Sie im Voraus über wichtige Änderungen wie:

- Ende des Supports für Open-Source-Software — In einigen AWS-Services Fällen werden Open-Source-Versionen von Software ausgeführt. Wenn die Open-Source-Community den Support für Softwareversionen einstellt, werden Sie AWS darüber informiert, wann Sie Maßnahmen ergreifen müssen, um ein Upgrade durchzuführen und Auswirkungen auf Ihre Anwendungen zu vermeiden.
  - Ende der Unterstützung für die Version der Amazon RDS-Engine für MySQL
  - Ende der Unterstützung für die Amazon EKS Kubernetes-Version
- Änderungen, die sich auf AWS eigene Ressourcen auswirken und möglicherweise Ihr Eingreifen erfordern.
  - Ablauf der Zertifikate der Amazon RDS Certificate Authority.

> **Note**
>
> Alle Benachrichtigungen, die diese Kriterien erfüllen, werden AWS Health als geplante Lebenszyklusereignisse gemeldet.

- Dynamischer Ressourcenverbrauch und verbesserte Metadaten: Ab dem Zeitpunkt, an dem Sie die Benachrichtigung erhalten, bis zum Ablauf des AWS Health Ereignisses werden Ihre betroffenen Ressourcen dem AWS Health Ereignis als betroffene Entitäten mit einem bestimmten Entitätsstatus zugeordnet. Betroffene Ressourcen werden gegebenenfalls ARN ARN-Format angegeben. Wenn für Ihre betroffenen Ressourcen ein Eingreifen des Kunden erforderlich ist, werden sie mit dem Status „AUSSTEHEND“ aufgeführt. Wenn für Ihre betroffenen Ressourcen die erforderlichen Maßnahmen ausgeführt wurden oder die Ressourcen gelöscht wurden, wird der Status auf „BEHOBEN“ aktualisiert.

> **Note**
>
> - Aktualisierungen des Ressourcenstatus werden asynchron und regelmäßig durchgeführt und können in seltenen Fällen eine Verzögerung von bis zu 72 Stunden haben.
> - In den Ausnahmen, in denen keine dynamischen Aktualisierungen bereitgestellt werden, wird Ressourcen nicht der Status „AUSSTEHEND“ oder „BEHOBEN“ zugewiesen.
> - Aktualisierungen des Ressourcenstatus werden in den Regionen AWS GovCloud (US) und China nicht unterstützt.

Was kann ich erwarten, wenn ich eine Benachrichtigung über ein geplantes Lebenszyklusereignis erhalte?

Die AWS Health Erfahrung mit geplanten Lebenszyklusereignissen hilft Ihren Teams, sich über bevorstehende Änderungen im Lebenszyklus zu informieren und den Abschluss von Maßnahmen zu verfolgen.

Typkategorie: Geplante Änderung

Code für den Ereignistyp: AWS_ {SERVICE} _PLANNED_LIFECYCLE_EVENT

Startzeit des Ereignisses: Die Startzeit des Ereignisses ist das früheste Datum, an dem Ihre Ressourcen von der Änderung betroffen sind.

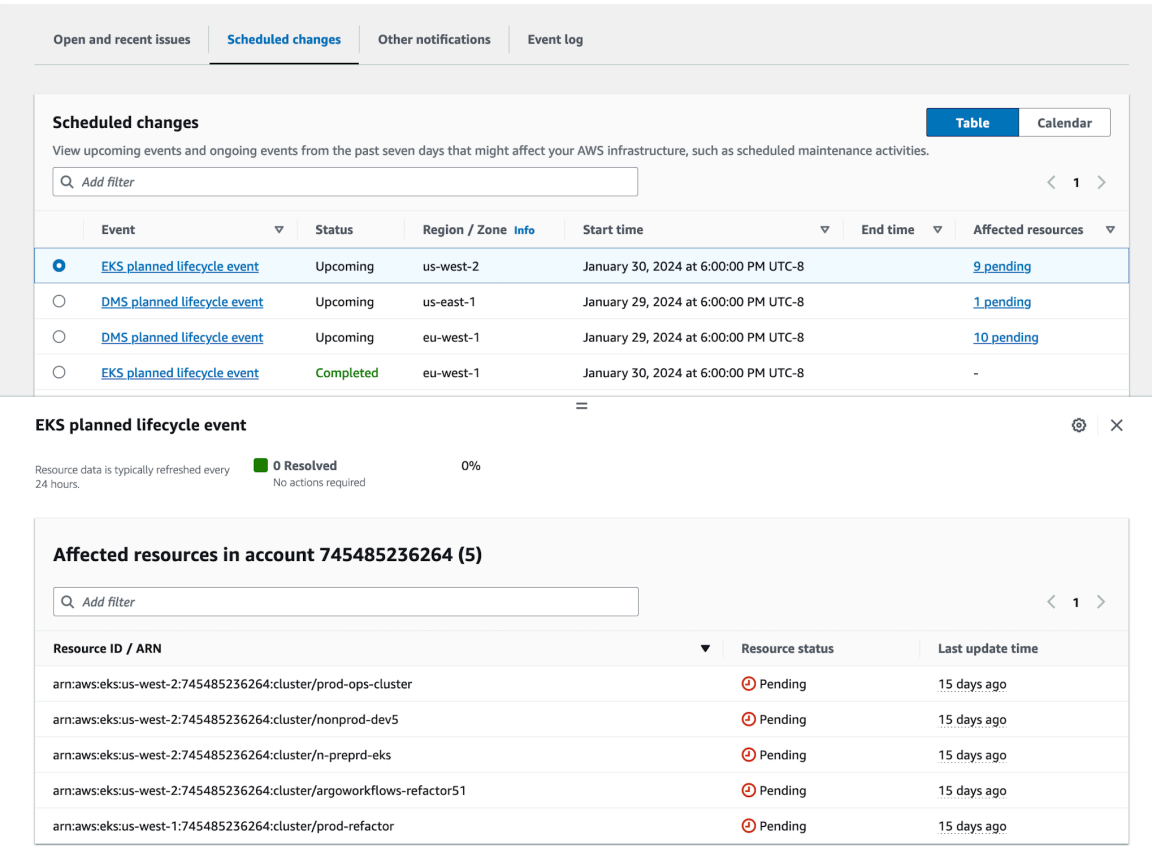
Endzeit des Ereignisses: Die Endzeit des Ereignisses ist das Datum, an dem die Änderung für alle AWS Ressourcen abgeschlossen ist. Beachten Sie, dass die Endzeit nicht immer angegeben ist. Es ist wichtig, die Startzeit als Änderungsdatum zu behandeln.

> **Note**
>
> Organizations können damit rechnen, für jedes geplante Lebenszyklusereignis, gruppiert nach Regionen, in denen Ressourcen betroffen sind, einen einzigen Event-ARN zu erhalten. Sie erhalten jedoch möglicherweise mehrere, ARNs wenn die Organisation über eine große Anzahl von betroffenen AWS-Konten oder Ressourcen verfügt.

Frühzeitiger Einblick in geplante Lebenszyklusereignisse: Geplante Lebenszyklusereignisse sind so konzipiert, dass sie für wichtige Ereignisseversions/changes and 90 days for minor versions/changes, soweit möglich, eine Mindestvorlaufzeit von 180 Tagen haben.

Dynamischer Ressourcenverbrauch und verbesserte Metadaten: Ab dem Zeitpunkt, an dem Sie die Benachrichtigung erhalten, bis zur Laufzeit des AWS Health Ereignisses werden Ihre betroffenen Ressourcen dem AWS Health Ereignis als betroffene Entitäten mit einem bestimmten Entitätsstatus zugeordnet. Betroffene Ressourcen werden gegebenenfalls ARN ARN-Format angegeben. Wenn für Ihre betroffenen Ressourcen ein Eingreifen des Kunden erforderlich ist, werden sie mit dem Status „AUSSTEHEND“ aufgeführt. Wenn für Ihre betroffenen Ressourcen die erforderlichen Maßnahmen ausgeführt wurden oder die Ressourcen gelöscht wurden, wird der Status auf „BEHOBEN“ aktualisiert.

> **Note**
>
> - AWS Health Benachrichtigungen bieten nach Möglichkeit Statusaktualisierungen im Laufe der Zeit, außer für die Regionen AWS GovCloud (US) und China.
> - Aktualisierungen des Ressourcenstatus werden asynchron und regelmäßig durchgeführt und können in seltenen Fällen eine Verzögerung von bis zu 72 Stunden haben.



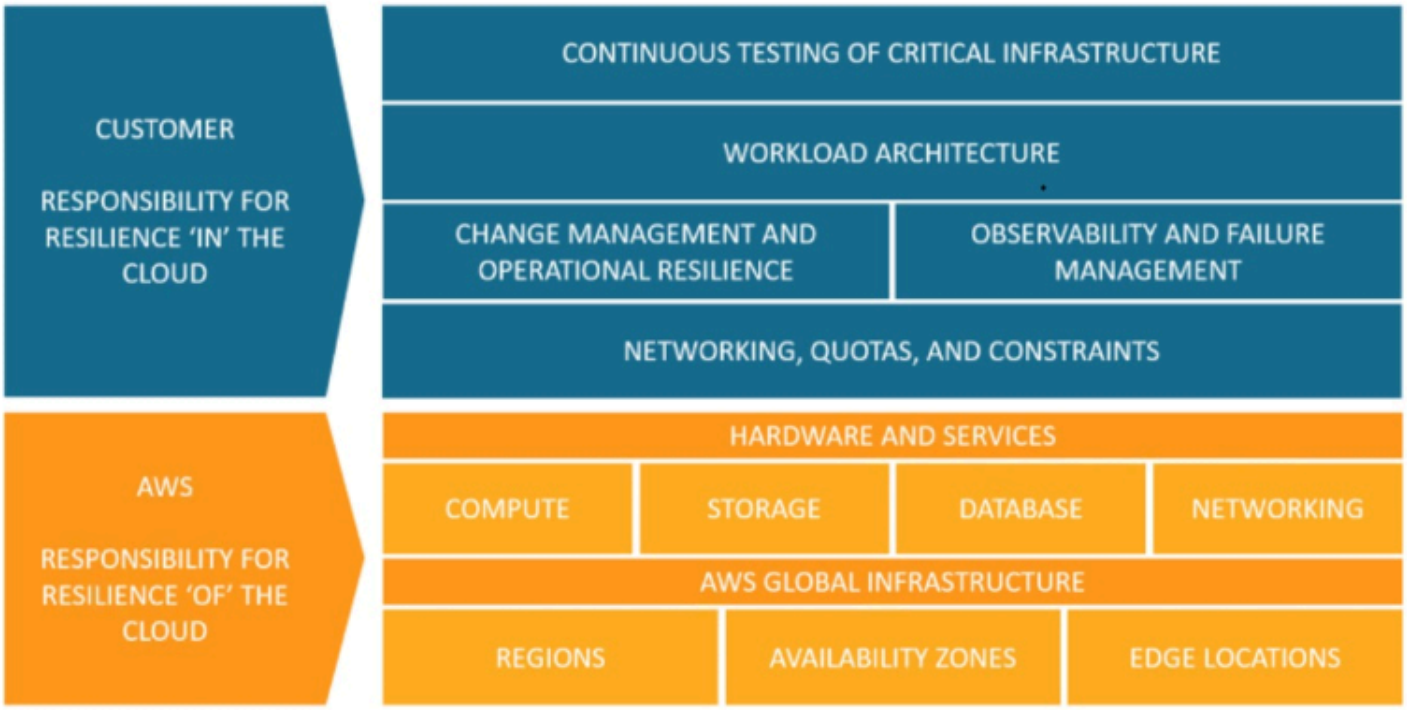
Nach Ablauf des geplanten Veranstaltungstermins:

1. Falls zutreffend, kann der Service die beschriebene Änderung jederzeit nach dem Startdatum der Veranstaltung an Ihrer Ressource vornehmen.
2. Wenn Sie alle Ressourcen vor Ablauf des Supportzeitraums lösen, ändert sich der Status Ihrer AWS Health Veranstaltung`Closed`.
3. Wenn Sie nach dem Änderungsdatum noch ausstehende Ressourcen haben, die aber nicht gelöst sind, bleibt die AWS Health Veranstaltung nach dem Start- oder Enddatum der Veranstaltung noch 4 Jahre lang geöffnet (je nachdem, welcher Zeitpunkt später ist). Nach Ablauf dieser Zeit wird die AWS Health Veranstaltung gelöscht.

Modell der geteilten Verantwortung für Resilienz

Sicherheit und Compliance liegen in der gemeinsamen AWS Verantwortung des Kunden. Je nach den bereitgestellten Diensten kann dieses gemeinsame Modell dazu beitragen, die betriebliche Belastung des Kunden zu verringern. Dies liegt daran AWS , dass die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis hin zur physischen Sicherheit der Einrichtungen,

in denen der Service betrieben wird, betrieben, verwaltet und kontrolliert werden. Der Kunde übernimmt die Verantwortung und Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches) und anderer zugehöriger Anwendungssoftware sowie der Konfiguration der Sicherheitsgruppen-Firewall, die von bereitgestellt wird AWS. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.



Zugriff auf geplante Lebenszyklusereignisse

Geplante Lebenszyklusereignisse können über mehrere Kanäle abgerufen und überwacht werden:

- Verwenden Sie Amazon EventBridge
- Verwenden Sie das AWS Health Dashboard
  - Kalenderansicht
  - Ansicht der betroffenen Ressourcen
- Verwenden Sie die AWS Health API

Integration AWS Health mit anderen Systemen, die AWS Health API

AWS Health ist ein RESTful-Webdienst, der HTTPS als Transport und JSON als Nachrichtenserialisierungsformat verwendet. Ihr Anwendungscode kann Anfragen direkt an die AWS Health -API stellen. Wenn Sie die REST-API direkt verwenden, müssen Sie den erforderlichen Code schreiben, um Ihre Anfragen zu signieren und zu authentifizieren. Weitere Informationen zu den AWS Health Vorgängen und Parametern finden Sie in der AWS Health API-Referenz.

> **Note**
>
> Sie müssen über einen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan von verfügen, AWS Supportum die AWS Health API verwenden zu können. Wenn Sie in einem Unternehmen sind AWS-Region , das keinen dieser AWS Support Pläne anbietet, oder wenn Sie noch nicht auf einen dieser Pläne umgestiegen sind, können Sie die AWS Health API mit einem Business- On-Ramp, Enterprise- oder Enterprise Support-Plan verwenden. Wenn Sie die AWS Health API von einem Gerät aus aufrufen AWS-Konto , das nicht in einem dieser Pläne registriert ist, erhalten Sie eine `SubscriptionRequiredException` Fehlermeldung.

Sie können die AWS SDKs verwenden, um die AWS Health REST-API-Aufrufe zu umschließen, was Ihre Anwendungsentwicklung vereinfachen kann. Sie geben Ihre AWS Anmeldeinformationen an, und diese Bibliotheken kümmern sich für Sie um die Authentifizierung und das Signieren von Anfragen.

AWS Health bietet auch ein AWS Health Dashboard AWS-Managementkonsole , mit dem Sie Ereignisse und betroffene Entitäten anzeigen und danach suchen können. Siehe Erste Schritte mit Ihrem AWS Health Dashboard.

Themen

- Signieren AWS Health API-Anforderungen
- Auswahl von Endpunkten für AWS Health API-Anforderungen
- Demos: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten programmgesteuert
- Tutorial: Verwenden des AWS Health API mit Java-Beispielen

Signieren AWS Health API-Anforderungen

Wenn Sie die AWS SDKs oder das AWS Command Line Interface (AWS CLI) verwenden, um Anfragen zu stellen AWS, signieren diese Tools die Anfragen automatisch für Sie mit dem Zugriffsschlüssel, den Sie bei der Konfiguration der Tools angeben. Wenn Sie beispielsweise die Demoversion AWS SDK für Java für den vorherigen Endpunkt mit hoher Verfügbarkeit verwenden, müssen Sie Anfragen nicht selbst signieren.

Java-Codebeispiele

Weitere Beispiele zur Verwendung der AWS Health API mit dem AWS SDK für Java finden Sie in diesem Beispielcode.

Wenn Sie Anfragen stellen, empfehlen wir Ihnen dringend, Ihre AWS Root-Kontoanmeldeinformationen nicht für den regulären Zugriff auf zu verwenden AWS Health. Sie können die Anmeldeinformationen eines IAM-Benutzers nutzen. Weitere Informationen finden Sie unter Sperren der Root-Benutzerzugriffsschlüssel für Ihr AWS Konto im IAM-Benutzerhandbuch.

Wenn Sie die AWS SDKs oder die nicht verwenden AWS CLI, müssen Sie Ihre Anfragen selbst signieren. Wir empfehlen, dass Sie AWS Signature Version 4 verwenden. Weitere Informationen finden Sie unter Signieren von AWS API-Anfragen im Allgemeine AWS-Referenz.

Auswahl von Endpunkten für AWS Health API-Anforderungen

Die AWS Health API folgt einer Anwendungsarchitektur mit mehreren Regionen und verfügt über zwei regionale Endpunkte in einer Konfiguration. Bietet einen einzigen, globalen Endpunkt zur Unterstützung von aktiv-passivem DNS-Failover. AWS Health Sie können eine DNS-Suche auf dem globalen Endpunkt durchführen, um den aktiven Endpunkt und die entsprechende Signaturregion zu ermitteln. AWS Auf diese Weise wissen Sie, welchen Endpunkt Sie in Ihrem Code verwenden müssen, sodass Sie die neuesten Informationen abrufen können AWS Health.

Wenn Sie eine Anfrage an den globalen Endpunkt stellen, müssen Sie Ihre AWS Zugangsdaten für den regionalen Endpunkt angeben, auf den Sie abzielen, und die Signatur für Ihre Region konfigurieren. Andernfalls schlägt Ihre Authentifizierung möglicherweise fehl. Weitere Informationen finden Sie unter Signieren AWS Health API-Anforderungen.

Bei IPv6-only Anfragen empfehlen wir, eine DNS-Suche auf dem globalen Endpunkt durchzuführen, um den aktiven Endpunkt zu ermitteln, AWS-Region und dann den IPv6-unterstützten Dual-Stack-Endpunkt für diese Region aufzurufen.

Die folgende Tabelle stellt die Standardkonfiguration dar.

Description	Region der Signatur	Endpoint	Protocol (Protokoll)
Aktiv	us-east-1	health.us-east-1.amazonaws.com (IPv4-only) health.us-east-1.api.aws (IPv4 und IPv6 werden unterstützt)	HTTPS
Passiv	us-east-2	health.us-east-2.amazonaws.com (IPv4-only) health.us-east-2.api.aws (IPv4 und IPv6 werden unterstützt)	HTTPS
Global	us-east-1 **Note** Dies ist die Signaturregion des aktuellen aktiven Endpunkts.	global.health.amazonaws.com	HTTPS

Um festzustellen, ob ein Endpunkt der aktive Endpunkt ist, führen Sie eine DNS-Suche auf dem globalen Endpunkt CNAME durch und extrahieren Sie dann die Region aus dem aufgelösten Namen. AWS

Example: DNS-Suche auf dem globalen Endpunkt

Der Befehl gibt dann den Endpunkt us-east-1 cn-northwest-1 zurück. In dieser Ausgabe erfahren Sie, für welchen Endpunkt Sie ihn verwenden sollten. AWS Health

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

> **Tip**
>
> Sowohl der aktive als auch der passive Endpunkt geben AWS Health Daten zurück. Die neuesten AWS Health Daten sind jedoch nur vom aktiven Endpunkt aus verfügbar. Die Daten vom passiven Endpunkt werden irgendwann mit denen des aktiven Endpunkts übereinstimmen. Wir empfehlen, dass Sie alle Workflows neu starten, wenn sich der aktive Endpunkt ändert.

Demos: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten programmgesteuert

In den folgenden Codebeispielen AWS Health verwendet eine DNS-Suche für den globalen Endpunkt, um den aktiven regionalen Endpunkt und die Signaturregion zu ermitteln. AWS Health verwendet diese Informationen, um einen Bericht über die Ereignisdaten der letzten sieben Tage abzurufen. Der Code startet den Workflow neu, wenn sich der aktive Endpunkt ändert.

Themen

- Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Java
- Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Python

Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Java

Voraussetzung

Sie müssen Gradle installieren.

Um das Java-Beispiel zu verwenden

1. Laden Sie die Demo für AWS Health Hochverfügbarkeitsendpunkte von herunter GitHub.
2. Navigieren Sie zum `high-availability-endpoint/java` Demo-Projektverzeichnis.
3. Geben Sie in einem Befehlszeilenfenster den folgenden Befehl ein.

```
gradle build
```

4. Geben Sie die folgenden Befehle ein, um Ihre AWS Anmeldeinformationen anzugeben.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Geben Sie den folgenden Befehl ein, um die Demo auszuführen.

```
gradle run
```

Example: AWS Health Ausgabe des Ereignisses

Das Codebeispiel gibt das jüngste AWS Health Ereignis der letzten sieben Tage in Ihrem AWS Konto zurück. Im folgenden Beispiel enthält die Ausgabe ein AWS Health Ereignis für den AWS Config Dienst.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
```

```
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
```

```
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'

If you have any questions regarding this deprecation plan, please contact AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Java-Ressourcen

- Weitere Informationen finden Sie unter Interface HealthClient in der AWS SDK für Java API-Referenz und im Quellcode.
- Weitere Informationen zu der Bibliothek, die in dieser Demo für DNS-Lookups verwendet wird, finden Sie im Abschnitt dnsjava unter. GitHub

Demo: Abrufen der letzten sieben Tage von AWS Health Ereignisdaten mit Python

Voraussetzung

Sie müssen Python 3 installieren.

Um das Python-Beispiel zu verwenden

1. Laden Sie die Demo für AWS Health Hochverfügbarkeitsendpunkte von herunter GitHub.
2. Navigieren Sie zum `high-availability-endpoint/python` Demo-Projektverzeichnis.
3. Geben Sie in einem Befehlszeilenfenster die folgenden Befehle ein.

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Für Python 3.3 und höher können Sie das integrierte `venv` Modul verwenden, um die virtuelle Umgebung zu erstellen, anstatt sie zu installieren`virtualenv`. Weitere Informationen finden Sie unter venv — Erstellung virtueller Umgebungen auf der Python-Website.
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. Geben Sie den folgenden Befehl ein, um die virtuelle Umgebung zu aktivieren.

```
source v-aws-health-env/bin/activate
```

5. Geben Sie den folgenden Befehl ein, um die Abhängigkeiten zu installieren.

```
pip install -r requirements.txt
```

6. Geben Sie die folgenden Befehle ein, um Ihre AWS Anmeldeinformationen anzugeben.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Geben Sie den folgenden Befehl ein, um die Demo auszuführen.

```
python3 main.py
```

Example: AWS Health Ausgabe des Ereignisses

Das Codebeispiel gibt das jüngste AWS Health Ereignis der letzten sieben Tage in Ihrem AWS Konto zurück. Die folgende Ausgabe gibt ein AWS Health Ereignis für eine AWS Sicherheitsbenachrichtigung zurück.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a ‘TLS’ tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
```

```
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. Wenn Sie fertig sind, geben Sie den folgenden Befehl ein, um die virtuelle Maschine zu deaktivieren.

```
deactivate
```

Python-Ressourcen

- Weitere Informationen zu finden Sie in der `Health. Client` API-Referenz zum AWS SDK for Python (Boto3).
- Weitere Informationen zu der Bibliothek, die in dieser Demo für DNS-Lookups verwendet wird, finden Sie im dnspython-Toolkit und im Quellcode unter. GitHub

Tutorial: Verwenden des AWS Health API mit Java-Beispielen

Die folgenden Java-Codebeispiele zeigen, wie Sie einen AWS Health Client initialisieren und Informationen über Ereignisse und Entitäten abrufen.

Schritt 1: Initialisieren der Anmeldeinformationen

Für die Kommunikation mit der AWS Health API sind gültige Anmeldeinformationen erforderlich. Sie können das key pair eines beliebigen IAM-Benutzers verwenden, der mit dem AWS Konto verknüpft ist.

Erstellen und initialisieren Sie eine AWSCredentials-Instance:

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Schritt 2: Initialisieren Sie eine AWS Health API-Client

Erstellen Sie mit den im vorigen Schritt generierten initialisierten Anmeldeinformationen einen AWS Health -Client:

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Schritt 3: Verwenden AWS Health API-Operationen zum Abrufen von Ereignisinformationen

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
```

```
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;


DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();
```

```
filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Sicherheit bei AWS Health

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die so konzipiert sind, dass sie die Anforderungen der sicherheitsrelevantesten Organisationen erfüllen.

Sicherheit ist eine gemeinsame Verantwortung zwischen AWS Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist für den Schutz der Infrastruktur verantwortlich, auf der AWS Dienste in der AWS Cloud ausgeführt werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-partyAuditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsvorkehrungen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Folgendes gelten AWS Health, finden Sie unter AWS Services im Umfang nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung wird durch den AWS Dienst bestimmt, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, darunter die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens sowie die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden AWS Health. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration so einrichten AWS Health , dass Ihre Sicherheits- und Compliance-Ziele erreicht werden. Außerdem erfahren Sie, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre AWS Health Ressourcen überwachen und sichern können.

Topics

- Datenschutz in AWS Health
- Identitäts- und Zugriffsmanagement für AWS Health
- Einloggen und Überwachen AWS Health
- Überprüfung der Konformität für AWS Health
- Widerstandsfähigkeit in AWS Health
- Sicherheit der Infrastruktur in AWS Health
- Konfiguration und Schwachstellenanalyse in AWS Health
- Bewährte Sicherheitsmethoden für AWS Health

Datenschutz in AWS Health

Das Modell der AWS gemeinsamen Verantwortung (Modell der gilt für den Datenschutz in. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der das gesamte System läuft AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie in den häufig gestellten Fragen zum Datenschutz in der Region . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, Ihre AWS-Konto Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten findest du unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, 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, der API oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen

externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

In den folgenden Informationen finden Sie Informationen zum AWS Health Verschlüsseln von Daten.

Datenverschlüsselung bezieht sich auf den Schutz von Daten während der Übertragung (auf dem Weg vom Dienst zu Ihrem AWS Konto) und im Ruhezustand (während sie in AWS Diensten gespeichert sind). Sie können Daten während der Übertragung mit TLS (Transport Layer Security) oder im Ruhezustand mit clientseitiger Verschlüsselung schützen.

AWS Health zeichnet bei Veranstaltungen keine personenbezogenen Daten (PII) wie E-Mail-Adressen oder Kundennamen auf.

Verschlüsselung im Ruhezustand

Alle von AWS Health gespeicherten Daten werden im Ruhezustand verschlüsselt.

Verschlüsselung während der Übertragung

Alle Daten, die an und von AWS Health dort gesendet werden, werden bei der Übertragung verschlüsselt.

Schlüsselverwaltung

AWS Health unterstützt keine vom Kunden verwalteten Verschlüsselungsschlüssel für in der AWS Cloud verschlüsselte Daten.

Identitäts- und Zugriffsmanagement für AWS Health

AWS Identity and Access Management (IAM) ist ein Programm AWS-Service , das einem Administrator hilft, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer zur Nutzung von Ressourcen authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt). AWS Health IAM ist ein Dienst AWS-Service , den Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS Health funktioniert mit IAM
- AWS Health Beispiele für identitätsbasierte Richtlinien
- Fehlerbehebung AWS Health Identität und Zugriff
- Verwenden Sie serviceverknüpfte Rollen für AWS Health
- AWS verwaltete Richtlinien für AWS Health

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung AWS Health Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie AWS Health funktioniert mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe AWS Health Beispiele für identitätsbasierte Richtlinien).

Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich AWS mit Ihren Identitätsdaten an. Sie müssen als IAM-Benutzer oder als IAM-Benutzer authentifiziert sein, indem Sie eine IAM-Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich mit Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen als Verbundidentität anmelden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Stellt für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen bereit. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS Stammbenutzer des Kontos

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle Ressourcen hat. AWS-Services Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer einen Verbund mit einem Identitätsanbieter verwenden, um AWS mithilfe temporärer Anmeldeinformationen auf den Zugriff zuzugreifen.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder eine AWS API-Operation aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie einer Identität oder Ressource zugeordnet sind. AWS wertet diese Richtlinien aus, wenn ein Principal eine Anfrage

stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können integrierte Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

AWS Health unterstützt ressourcenbasierte Bedingungen. Sie können festlegen, welche AWS Health -Ereignisse Benutzer anzeigen können. Sie können beispielsweise eine Richtlinie erstellen, die nur

einem IAM-Benutzer den Zugriff auf bestimmte Amazon EC2-Ereignisse im Dashboard gewährt. AWS Health

Weitere Informationen finden Sie unter Ressourcen.

Zugriffskontrolllisten

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste AWS WAF, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

AWS Health unterstützt keine ACLs.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximale Anzahl von Berechtigungen festgelegt werden kann, die für gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen komplizierter zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob

eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Logik zur Richtlinienauswertung.

Wie AWS Health funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden AWS Health, sollten Sie sich darüber im Klaren sein, mit welchen IAM-Funktionen Sie diese verwenden können. AWS Health Einen allgemeinen Überblick darüber, wie AWS Health und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren.

Themen

- AWS Health Identitätsbasierte Richtlinien
- AWS Health Ressourcenbasierte Richtlinien
- Die Autorisierung basiert auf AWS Health tags
- AWS Health IAM-Rollen

AWS Health Identitätsbasierte Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen erteilt oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. AWS Health unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu gewähren.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Health verwendet:`health:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, detaillierte Informationen zu bestimmten

Ereignissen im Rahmen des DescribeEventDetails API-Vorgangs einzusehen, nehmen Sie die `heath:DescribeEventDetails` Aktion in die Richtlinie auf.

Richtlinienerklärungen müssen ein `Action` `NotAction` OR-Element enthalten. AWS Health definiert seinen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere -Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen durch Kommas.

```
"Action": [
      "health:action1",
      "health:action2"
```

Sie können auch Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "health:Describe*"
```

Eine Liste der AWS Health Aktionen finden Sie AWS Health im IAM-Benutzerhandbuch unter Actions Defined by.

Ressourcen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Ein AWS Health Ereignis hat das folgende Amazon Resource Name (ARN) -Format.

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Wenn Sie beispielsweise das Ereignis `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` in Ihrer Anweisung angeben möchten, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Um alle AWS Health Ereignisse für Amazon EC2 anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) und Service Namespaces. AWS

Einige AWS Health Aktionen können für eine bestimmte Ressource nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

AWS Health API-Operationen können mehrere Ressourcen umfassen. Der DescribeEvents Vorgang gibt beispielsweise Informationen über Ereignisse zurück, die ein bestimmtes Filterkriterium erfüllen. Das bedeutet, dass ein IAM-Benutzer über Berechtigungen zum Anzeigen dieses Ereignisses verfügen muss.

Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health unterstützt nur Berechtigungen auf Ressourcenebene für Integritätsereignisse und nur für die DescribeAffectedEntities und API-Operationen. DescribeEventDetails Weitere Informationen finden Sie unter Ressourcen- und aktionsbasierte Bedingungen.

Eine Liste der AWS Health Ressourcentypen und ihrer ARNs finden Sie AWS Health im IAM-Benutzerhandbuch unter Resources Defined by. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Health definierte Aktionen.

Bedingungsschlüssel

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Alle AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

AWS Health definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Alle AWS globalen Bedingungsschlüssel finden Sie im IAM-Benutzerhandbuch unter AWS Globale Bedingungskontextschlüssel.

Die Operationen DescribeAffectedEntities und die DescribeEventDetails API unterstützen die `health:service` Bedingungsschlüssel `health:eventTypeCode` und.

Eine Liste der AWS Health Bedingungsschlüssel finden Sie AWS Health im IAM-Benutzerhandbuch unter Bedingungsschlüssel für. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS Health.

Beispiele

Beispiele für AWS Health identitätsbasierte Richtlinien finden Sie unter. AWS Health Beispiele für identitätsbasierte Richtlinien

AWS Health Ressourcenbasierte Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Principal unter welchen Bedingungen auf der AWS Health Ressource ausführen kann. AWS Health unterstützt ressourcenbasierte Berechtigungsrichtlinien für Gesundheitsereignisse. Resource-based Mithilfe von Richtlinien können Sie anderen Konten Nutzungsberechtigungen auf Ressourcenbasis gewähren. Sie können auch eine ressourcenbasierte Richtlinie verwenden, um einem AWS Dienst den Zugriff auf Ihre Ereignisse zu ermöglichen. AWS Health

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das

Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Principal und die Ressource in unterschiedlichen AWS Konten befinden, müssen Sie der Prinzipal-Entität auch die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der Entität eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter So unterscheiden sich IAM-Rollen von Resource-based Richtlinien.

AWS Health unterstützt nur ressourcenbasierte Richtlinien für die und API-Operationen. DescribeAffectedEntities DescribeEventDetails Sie können diese Aktionen in einer Richtlinie angeben, um zu definieren, welche Hauptentitäten (Konten, Benutzer, Rollen und Verbundbenutzer) Aktionen für das Ereignis ausführen können. AWS Health

Beispiele

Beispiele für AWS Health ressourcenbasierte Richtlinien finden Sie unter. Ressourcen- und aktionsbasierte Bedingungen

Die Autorisierung basiert auf AWS Health tags

AWS Health unterstützt nicht das Markieren von Ressourcen oder die Steuerung des Zugriffs auf der Grundlage von Stichwörtern.

AWS Health IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS Konto, die über bestimmte Berechtigungen verfügt.

Verwenden Sie temporäre Anmeldeinformationen mit AWS Health

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS API-Operationen wie AssumeRole oder aufrufen GetFederationToken.

AWS Health unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-linked Rollen

Service-linked Rollen ermöglichen es AWS Diensten, auf Ressourcen in anderen Diensten zuzugreifen, um eine Aktion in Ihrem Namen durchzuführen. Service-linked Rollen werden in Ihrem

IAM-Konto angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

AWS Health unterstützt serviceverknüpfte Rollen zur Integration mit. AWS Organizations Die Service-verknüpfte Rolle wird `AWSServiceRoleForHealth_Organizations` benannt. Der Rolle ist die Health_OrganizationsServiceRolePolicy AWS verwaltete Richtlinie zugeordnet. Die AWS verwaltete Richtlinie ermöglicht AWS Health den Zugriff auf Gesundheitsereignisse von anderen AWS Konten in der Organisation aus.

Sie können den EnableHealthServiceAccessForOrganization Vorgang verwenden, um die mit dem Dienst verknüpfte Rolle im Konto zu erstellen. Wenn Sie diese Funktion jedoch deaktivieren möchten, müssen Sie den DisableHealthServiceAccessForOrganization Vorgang zuerst aufrufen. Anschließend können Sie die Rolle über die IAM-Konsole, die IAM-API oder AWS Command Line Interface ()AWS CLI löschen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

Weitere Informationen finden Sie unter Aggregieren AWS Health Ereignisse über Konten hinweg.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

AWS Health unterstützt keine Servicerollen.

AWS Health Beispiele für identitätsbasierte Richtlinien

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von AWS Health -Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS-Managementkonsole, AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien
- Verwendung der AWS Health Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugreifen auf AWS Health Dashboard und das AWS Health API
- Ressourcen- und aktionsbasierte Bedingungen

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand AWS Health Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn du identitätsbasierte Richtlinien erstellst oder bearbeitest, befolge diese Richtlinien und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese im Rahmen einer bestimmten Aktion verwendet werden AWS-Service, z. CloudFormation

B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Mehrstufige Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, in dem IAM-Benutzer oder ein Root-Benutzer in Ihrem System erforderlich sind AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwendung der AWS Health Konsole

Um auf die AWS Health Konsole zugreifen zu können, müssen Sie über ein Mindestmaß an Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, die AWS Health Ressourcen in Ihrem AWS Konto aufzulisten und Details zu ihnen anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten die AWS Health Konsole weiterhin verwenden können, können Sie die folgende AWS verwaltete Richtlinie anhängen: AWSHealthFullAccess.

Die `AWSHealthFullAccess` Richtlinie gewährt einer Entität vollen Zugriff auf Folgendes:

- Aktivieren oder deaktivieren Sie die Funktion zur AWS Health Organisationsansicht für alle Konten in einer AWS Organisation
- Das AWS Health Dashboard in der AWS Health Konsole
- AWS Health API-Operationen und Benachrichtigungen
- Sehen Sie sich Informationen zu Konten an, die Teil Ihrer AWS Organisation sind

- Sehen Sie sich die Organisationseinheiten (OU) des Verwaltungskontos an

Example: AWSHealthFullAccess

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
```

```
        }
    ]
}
```

> **Note**
>
> Sie können auch die `Health_OrganizationsServiceRolePolicy` AWS verwaltete Richtlinie verwenden, AWS Health um Ereignisse für andere Konten in Ihrer Organisation anzuzeigen. Weitere Informationen finden Sie unter Verwenden Sie serviceverknüpfte Rollen für AWS Health.

Sie müssen Benutzern, die nur die AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Zugreifen auf AWS Health Dashboard und das AWS Health API

Das AWS Health Dashboard ist für alle AWS Konten verfügbar. Die AWS Health API ist nur für Konten mit einem AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan verfügbar. Weitere Informationen finden Sie unter Support.

Sie können IAM verwenden, um Entitäten (Benutzer, Gruppen oder Rollen) zu erstellen und diesen Entitäten dann Berechtigungen für den Zugriff auf das AWS Health Dashboard und die AWS Health API zu erteilen.

Standardmäßig haben IAM-Benutzer keinen Zugriff auf das AWS Health Dashboard oder die AWS Health API. Sie gewähren Benutzern Zugriff auf die AWS Health Informationen Ihres Kontos, indem Sie IAM-Richtlinien an einen einzelnen Benutzer, eine Benutzergruppe oder eine Rolle anhängen. Weitere Informationen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) und Übersicht über IAM-Richtlinien.

Nachdem Sie die IAM-Benutzer erstellt haben, können Sie diesen individuelle Passwörter zuordnen. Anschließend können sie sich über eine kontospezifische Anmeldeseite bei Ihrem Konto anmelden und AWS Health Informationen einsehen. Weitere Informationen finden Sie unter Wie sich Benutzer bei Ihrem Konto anmelden.

> **Note**
>
> Ein IAM-Benutzer mit Berechtigungen zum Anzeigen des AWS Health Dashboards hat Lesezugriff auf alle AWS Dienste des Kontos. Dazu können unter anderem AWS Ressourcen-IDs wie Amazon EC2-Instance-IDs, EC2-Instance-IP-Adressen und allgemeine Sicherheitsbenachrichtigungen gehören.
> Wenn eine IAM-Richtlinie beispielsweise nur Zugriff auf das AWS Health Dashboard und die AWS Health API gewährt, kann der Benutzer oder die Rolle, für die die Richtlinie gilt, auf alle Informationen zugreifen, die über AWS Dienste und zugehörige Ressourcen veröffentlicht wurden, auch wenn andere IAM-Richtlinien diesen Zugriff nicht zulassen.

Sie können zwei Gruppen von APIs für verwenden. AWS Health

- Individuelle Konten — Sie können die Funktionen wie DescribeEvents und verwenden DescribeEventDetails, um Informationen über AWS Health Ereignisse für Ihr Konto abzurufen.
- Organisationskonto — Mithilfe von Vorgängen wie DescribeEventsForOrganization und können DescribeEventDetailsForOrganization Sie Informationen über AWS Health Ereignisse für Konten abrufen, die Teil Ihrer Organisation sind.

Weitere Informationen zu den verfügbaren API-Vorgängen finden Sie in der AWS Health API-Referenz.

Individuelle Aktionen

Sie können das `Action` Element einer IAM-Richtlinie auf `health:Describe*` festlegen. Dies ermöglicht den Zugriff auf das AWS Health Dashboard und AWS Health. AWS Health unterstützt die Zugriffskontrolle auf Ereignisse auf der Grundlage des `eventTypeCode` AND-Dienstes.

Zugriffsbeschreibung

Diese Grundsatzerklärung gewährt Zugriff auf das AWS Health Dashboard und alle API-Operationen. `Describe*` AWS Health Beispielsweise kann ein IAM-Benutzer mit dieser Richtlinie im auf das AWS Health Dashboard zugreifen AWS-Managementkonsole und den AWS Health `DescribeEvents` API-Vorgang aufrufen.

Example: Zugriffsbeschreibung

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

Zugriffsverweigerung

Diese Richtlinienerklärung verweigert den Zugriff auf das AWS Health Dashboard und die AWS Health API. Ein IAM-Benutzer mit dieser Richtlinie kann das AWS Health Dashboard in der nicht sehen AWS-Managementkonsole und keine der AWS Health API-Operationen aufrufen.

Example: Zugriffsverweigerung

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

Organisationsansicht

Wenn Sie die Organisationsansicht für aktivieren möchten AWS Health, müssen Sie den Zugriff auf die AWS Organizations Aktionen AWS Health und zulassen.

Das `Action` Element einer IAM-Richtlinie muss die folgenden Berechtigungen enthalten:

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

Informationen zu den genauen Berechtigungen, die für die einzelnen APIs erforderlich sind, finden Sie im IAM-Benutzerhandbuch unter Von AWS Health APIs und Benachrichtigungen definierte Aktionen.

> **Note**
>
> Sie müssen die Anmeldeinformationen des Verwaltungskontos einer Organisation verwenden, für die auf die AWS Health APIs zugegriffen werden soll. AWS Organizations Weitere Informationen finden Sie unter Aggregieren AWS Health Ereignisse über Konten hinweg.

Erlauben Sie den Zugriff auf AWS Health Organisationsansicht

Diese Grundsatzerklärung gewährt Zugriff auf alle AWS Health AWS Organizations Aktionen, die Sie für die Funktion zur Unternehmensansicht benötigen.

Example: Erlauben AWS Health Zugriff auf organisatorische Ansicht

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
health.amazonaws.com/AWSServiceRoleForHealth*"
        }
    ]
}
```

Zugriff verweigern auf AWS Health Organisationsansicht

Diese Grundsatzerklärung verweigert den Zugriff auf die AWS Organizations Aktionen, ermöglicht aber den Zugriff auf die AWS Health Aktionen für ein einzelnes Konto.

Example: Ablehnen AWS Health Zugriff auf organisatorische Ansicht

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
health.amazonaws.com/AWSServiceRoleForHealth*"
        }
```

```
    ]
}
```

> **Note**
>
> Wenn der Benutzer oder die Gruppe, der Sie Berechtigungen erteilen möchten, bereits über eine IAM-Richtlinie verfügt, können Sie dieser Richtlinie die AWS Health-spezifische Richtlinienanweisung hinzufügen.

Ressourcen- und aktionsbasierte Bedingungen

AWS Health unterstützt IAM-Bedingungen für die DescribeAffectedEntities und DescribeEventDetails API-Operationen. Sie können ressourcen- und aktionsbasierte Bedingungen verwenden, um Ereignisse einzuschränken, die die AWS Health API an einen Benutzer, eine Gruppe oder eine Rolle sendet.

Aktualisieren Sie dazu den `Condition` Block der IAM-Richtlinie oder legen Sie das `Resource` Element fest. Sie können String-Bedingungen verwenden, um den Zugriff auf der Grundlage bestimmter AWS Health Ereignisfelder einzuschränken.

Sie können die folgenden Felder verwenden, wenn Sie ein AWS Health Ereignis in Ihrer Richtlinie angeben:

- `eventTypeCode`
- `service`

> **Hinweise**
>
> - Die Operationen DescribeAffectedEntities und DescribeEventDetails API unterstützen Berechtigungen auf Ressourcenebene. Sie können beispielsweise eine Richtlinie erstellen, um bestimmte Ereignisse zuzulassen oder abzulehnen. AWS Health
> - Die Operationen DescribeAffectedEntitiesForOrganization und DescribeEventDetailsForOrganization API unterstützen keine Berechtigungen auf Ressourcenebene.

- Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Health APIs und Benachrichtigungen in der Serviceautorisierungsreferenz.

Example: Action-based Zustand

Diese Grundsatzerklärung gewährt Zugriff auf das AWS Health Dashboard und die AWS Health `Describe*` API-Operationen, verweigert jedoch den Zugriff auf alle AWS Health Ereignisse, die Amazon EC2 betreffen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example: Zustand Resource-based

Die folgende Richtlinie hat den gleichen Effekt, verwendet aber stattdessen das Element `Resource`.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example: TypeCode Zustand des Ereignisses

Diese Grundsatzerklärung gewährt Zugriff auf das AWS Health Dashboard und die AWS Health `Describe*` API-Operationen, verweigert jedoch den Zugriff auf alle AWS Health Ereignisse`eventTypeCode`, denen das entsprichtAWS_EC2_*.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
```

```
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

> **Important**
>
> Wenn Sie die DescribeEventDetails Operationen DescribeAffectedEntities und aufrufen und nicht berechtigt sind, auf das AWS Health Ereignis zuzugreifen, wird der `AccessDeniedException` Fehler angezeigt. Weitere Informationen finden Sie unter Fehlerbehebung AWS Health Identität und Zugriff.

Fehlerbehebung AWS Health Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Health und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion auszuführen in AWS Health
- Ich bin nicht berechtigt, IAM durchzuführen: PassRole
- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen den Zugriff gewähren AWS Health
- Ich möchte Personen außerhalb meiner AWS Konto für den Zugriff auf mein AWS Health Ressourcen

Ich bin nicht berechtigt, eine Aktion auszuführen in AWS Health

Wenn Ihnen der AWS-Managementkonsole mitteilt, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie Ihren Administrator um Unterstützung bitten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort gegeben hat.

Der `AccessDeniedException` Fehler tritt auf, wenn ein Benutzer nicht berechtigt ist, das AWS Health Dashboard oder die AWS Health API-Operationen zu verwenden.

In diesem Fall muss der Administrator des Benutzers die Richtlinie aktualisieren, um dem Benutzer Zugriff zu ermöglichen.

Für die AWS Health API ist ein AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan von AWS Support erforderlich. Wenn Sie die AWS Health API von einem Konto aus aufrufen, das keinen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan hat, wird der folgende Fehlercode zurückgegeben:`SubscriptionRequiredException`.

Ich bin nicht berechtigt, IAM durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Healthübergeben zu können.

In einigen AWS-Services Fällen können Sie eine vorhandene Rolle an diesen Dienst übergeben, anstatt eine neue oder mit einem Dienst verknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Health auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anforderungen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Auf diese Weise können Sie jemandem dauerhaften Zugriff auf Ihre gewähren AWS-Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen den Zugriff gewähren AWS Health

Um anderen den Zugriff zu ermöglichen AWS Health, müssen Sie den Personen oder Anwendungen, die Zugriff benötigen, die Erlaubnis erteilen. Wenn Sie es AWS IAM Identity Center zur Verwaltung von Personen und Anwendungen verwenden, weisen Sie Benutzern oder Gruppen Berechtigungssätze zu, um deren Zugriffsebene zu definieren. Mit Berechtigungssätzen werden automatisch IAM-Richtlinien erstellt und den IAM-Rollen zugewiesen, die der Person oder Anwendung zugeordnet sind. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Berechtigungssätze.

Wenn Sie IAM Identity Center nicht verwenden, müssen Sie IAM-Entitäten (Benutzer oder Rollen) für die Personen oder Anwendungen erstellen, die Zugriff benötigen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in AWS Health gewährt. Nachdem die Berechtigungen erteilt wurden, stellen Sie dem Benutzer oder Anwendungsentwickler die Anmeldeinformationen zur Verfügung. Sie verwenden diese Anmeldeinformationen für den Zugriff AWS. Weitere Informationen zum Erstellen von IAM-Benutzern, -Gruppen, -Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch unter IAM-Identitäten und -Richtlinien und -Berechtigungen in IAM.

Ich möchte Personen außerhalb meiner AWS Konto für den Zugriff auf mein AWS Health Ressourcen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Health unterstützt werden, finden Sie unterWie AWS Health funktioniert mit IAM.
- Informationen zum Bereitstellen des Zugriffs auf Ihre Ressourcen in Ihrem eigenen AWS-Konten Bereich finden Sie im IAM-Benutzerhandbuch unter Bereitstellen des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dessen Eigentümer Sie sind.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf Ressourcen, die Dritten AWS-Konten gehören.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden Sie serviceverknüpfte Rollen für AWS Health

AWS Health verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger IAM-Rollentyp, mit dem direkt verknüpft ist. AWS Health Service-linked Rollen sind von vordefiniert AWS Health und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS-Services für Sie aufzurufen.

Sie können eine dienstbezogene Rolle zum Einrichten verwenden, um das manuelle Hinzufügen der erforderlichen Berechtigungen AWS Health zu vermeiden. AWS Health definiert die Berechtigungen ihrer dienstverknüpften Rollen und AWS Health kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Service-linked Rollenberechtigungen für AWS Health

AWS Health hat zwei dienstbezogene Rollen:

- AWSServiceRoleForHealth_Organizations— Diese Rolle vertraut darauf, dass AWS Health (`health.amazonaws.com`) die Rolle übernimmt, auf die Sie zugreifen können AWS-Services . Dieser Rolle ist die `Health_OrganizationsServiceRolePolicy` AWS verwaltete Richtlinie zugeordnet.
- AWSServiceRoleForHealth_EventProcessor— Diese Rolle vertraut darauf, dass der AWS Health Service Principal (`event-processor.health.amazonaws.com`) die Rolle für Sie übernimmt. Dieser Rolle ist die `AWSHealth_EventProcessorServiceRolePolicy` AWS verwaltete Richtlinie zugeordnet. Der Service Principal verwendet die Rolle, um eine von Amazon EventBridge verwaltete Regel für die Erkennung und Reaktion auf AWS Vorfälle zu erstellen. Diese Regel ist die Infrastruktur, die in Ihrem Konto erforderlich ist AWS-Konto , um Informationen über die Änderung des Alarmzustands von Ihrem Konto an zu senden AWS Health.

Weitere Informationen zu den AWS verwalteten Richtlinien finden Sie unterAWS verwaltete Richtlinien für AWS Health.

Erstellen einer serviceverknüpften Rolle für AWS Health

Sie müssen die AWSServiceRoleForHealth_Organizations serviceverknüpfte Rolle nicht erstellen. Wenn Sie den EnableHealthServiceAccessForOrganization Vorgang aufrufen, AWS Health erstellt diese dienstverknüpfte Rolle im Konto für Sie.

Sie müssen die AWSServiceRoleForHealth_EventProcessor serviceverknüpfte Rolle in Ihrem Konto manuell erstellen. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Bearbeiten einer serviceverknüpften Rolle für AWS Health

AWS Health ermöglicht es Ihnen nicht, die serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Health

Um die AWSServiceRoleForHealth_Organizations Rolle zu löschen, müssen Sie zuerst den DisableHealthServiceAccessForOrganization Vorgang aufrufen. Anschließend können Sie die Rolle über die IAM-Konsole, die IAM-API oder AWS Command Line Interface ()AWS CLI löschen.

Um die AWSServiceRoleForHealth_EventProcessor Rolle zu löschen, kontaktieren Sie sie AWS Support und bitten Sie sie, Ihre Workloads von AWS Incident Detection and Response zu trennen. Nach Abschluss dieses Vorgangs können Sie entweder die Rollen über die IAM-Konsole, die IAM-API oder löschen. AWS CLI

Ähnliche Informationen

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für AWS Health

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie von allen AWS Kunden

verwendet werden können. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Hauptidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie am ehesten, wenn eine neue eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Health hat die folgenden verwalteten Richtlinien.

Inhalt

- AWS verwaltete Richtlinie: AWS Health_EventProcessorServiceRolePolicy
- AWS verwaltete Richtlinie: Health_OrganizationsServiceRolePolicy
- AWS verwaltete Richtlinie: AWSHealthFullAccess
- AWS Health Aktualisierungen zu AWS Verwaltete Richtlinien

AWS verwaltete Richtlinie: AWS Health_EventProcessorServiceRolePolicy

AWS Health verwendet die AWSHealth_EventProcessorServiceRolePolicy AWS verwaltete Richtlinie. Diese verwaltete Richtlinie ist mit der `AWSServiceRoleForHealth_EventProcessor` dienstverknüpften Rolle verbunden. Die Richtlinie ermöglicht es der dienstverknüpften Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden Sie serviceverknüpfte Rollen für AWS Health.

Die verwaltete Richtlinie verfügt über die folgenden Berechtigungen, um den Zugriff auf die EventBridge Amazon-Regel für die Erkennung und Reaktion von AWS Vorfällen AWS Health zu ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `events`— Beschreibt und löscht EventBridge Regeln und beschreibt und aktualisiert die Ziele für diese Regeln.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Eine Liste der Änderungen an der Richtlinie finden Sie unterAWS Health Aktualisierungen zu AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: Health_OrganizationsServiceRolePolicy

AWS Health verwendet die Health_OrganizationsServiceRolePolicy AWS verwaltete Richtlinie. Diese verwaltete Richtlinie ist mit der `AWSServiceRoleForHealth_Organizations` dienstverknüpften

Rolle verbunden. Die Richtlinie ermöglicht es der dienstverknüpften Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden Sie serviceverknüpfte Rollen für AWS Health.

Diese Richtlinie gewährt Berechtigungen, die den AWS Health Zugriff auf die erforderlichen AWS Organizations Details für die Ansicht „Health Organizational“ ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Beschreibt die Konten in AWS Organizations und die Konten AWS-Services , die mit Organisationen verwendet werden können.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

Eine Liste der Änderungen an der Richtlinie finden Sie unterAWS Health Aktualisierungen zu AWS Verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSHealthFullAccess

AWS Health verwendet die AWSHealthFullAccess AWS verwaltete Richtlinie. Die Richtlinie gewährt Entitäten (IAM-Benutzer oder -Rollen) Zugriff auf die AWS Health Konsole. Weitere Informationen finden Sie unter Verwendung der AWS Health Konsole.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Aktivieren oder deaktivieren Sie die Funktion zur AWS Health Organisationsansicht für alle Konten in einer AWS Organisation und lassen Sie sich die Organisationseinheiten (OU) des Verwaltungskontos anzeigen
- `health`— Zugriff auf die AWS Health API-Operationen und Benachrichtigungen
- `iam`— Erstellt eine IAM-Rolle, die mit dem AWS Health Dienst verknüpft ist

JSON

```
{
    "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
```

```
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
                "Sid": "ServiceLinkAccess",
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

Eine Liste der Änderungen an der Richtlinie finden Sie unterAWS Health Aktualisierungen zu AWS Verwaltete Richtlinien.

AWS Health Aktualisierungen zu AWS Verwaltete Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Health seit Beginn der Erfassung dieser Änderungen durch diesen Dienst vorgenommen wurden. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumenthistorie für AWS Health-Seite.

In der folgenden Tabelle werden wichtige Aktualisierungen der AWS Health verwalteten Richtlinien seit dem 13. Januar 2022 beschrieben.

AWS Health

Änderungen	Beschreibung	Datum
AWS verwaltete Richtlinie: AWSHealthFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Health hat die AWSHealthFullAccess Richtlinie auf die Regionen China AWS GovCloud (US) Regions und China ausgeweitet.	16. Oktober 2023
AWS verwaltete Richtlinie: Health_OrganizationsServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS Health hat neue AWS Organizations Aktionen hinzugefügt, um es der dienstbezogenen Rolle zu ermöglichen, die Konten und AWS Dienste zu beschreiben, mit AWS Organizations denen verwendet werden kann.	19. Juli 2023
Änderungsprotokoll veröffentlicht	Änderungsprotokoll für die AWS Health verwalteten Richtlinien.	13. Januar 2023

Einloggen und Überwachen AWS Health

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Health anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AWS Health, melden, wenn etwas nicht stimmt, und gegebenenfalls Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Messwerte Ihrer Amazon Elastic Compute

Cloud (Amazon EC2) -Instances CloudWatch verfolgen lassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

- Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Rechnen. Sie können Regeln schreiben, die auf bestimmte Ereignisse überwachen und automatische Aktionen in anderen AWS -Services auslösen, wenn diese Ereignisse auftreten. Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt werden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Sie können ermitteln, welche Benutzer und Konten angerufen wurden AWS, die Quell-IP-Adresse, von der aus die Anrufe getätigt wurden, und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.

Weitere Informationen finden Sie unter Überwachen AWS Health.

Überprüfung der Konformität für AWS Health

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen für AWS Ihre Umgebung anmelden oder diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme, .

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen im Abschnitt Berichte AWS Artifact .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Widerstandsfähigkeit in AWS Health

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hochredundanten Netzwerken miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

AWS Health Ereignisse werden gespeichert und über mehrere Availability Zones hinweg repliziert. Dieser Ansatz stellt sicher, dass Sie über die Health Dashboard oder die AWS Health API-Operationen auf sie zugreifen können. Sie können AWS Health Ereignisse bis zu 90 Tage nach ihrem Eintreten anzeigen.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Health

Als verwalteter Service AWS Health ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Für den Zugriff AWS Health über das Netzwerk verwenden Sie AWS veröffentlichte API-Aufrufe. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder neuer. Clients müssen außerdem Verschlüsselungssammlungen mit Perfect Forward Secrecy (PFS) wie Ephemeral (DHE) oder Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) unterstützen. Diffie-Hellman Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS-Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfiguration und Schwachstellenanalyse in AWS Health

Konfiguration und IT-Kontrollen liegen in der gemeinsamen Verantwortung von Ihnen AWS und Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Bewährte Sicherheitsmethoden für AWS Health

Lesen Sie die folgenden bewährten Methoden für die Arbeit mit AWS Health.

Gewährung AWS Health mögliche Mindestberechtigungen für Benutzer

Befolgen Sie das Prinzip der geringsten Rechte, indem Sie die Mindestanzahl von Zugriffsrichtlinienberechtigungen für Ihre -Benutzer und -Gruppen verwenden. Beispielsweise könnten Sie einem AWS Identity and Access Management (IAM-) Benutzer den Zugriff auf die Health Dashboard gewähren. Aber Sie können es demselben Benutzer nicht gestatten, den Zugriff auf AWS Organizations zu aktivieren oder zu deaktivieren.

Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Sehen Sie sich das an Health Dashboard

Schauen Sie Health Dashboard regelmäßig vorbei, um Ereignisse zu identifizieren, die sich auf Ihr Konto oder Ihre Anwendungen auswirken könnten. Beispielsweise erhalten Sie möglicherweise eine Ereignisbenachrichtigung über Ihre Ressourcen, z. B. eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, die aktualisiert werden muss.

Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard.

Integrieren AWS Health mit Amazon Chime oder Slack

Sie können es in Ihre AWS Health Chat-Tools integrieren. Mit dieser Integration können Sie und Ihr Team in Echtzeit über AWS Health Ereignisse informiert werden. Weitere Informationen finden Sie in den AWS Health Tools unter GitHub.

Überwachen Sie für AWS Health Veranstaltungen

Sie können Amazon CloudWatch Events AWS Health integrieren, sodass Sie Regeln für bestimmte Ereignisse erstellen können. Wenn CloudWatch Events ein Ereignis erkennt, das Ihrer Regel

entspricht, werden Sie benachrichtigt und können dann Maßnahmen ergreifen. CloudWatch Ereignisse sind Ereignisse Region-specific, daher müssen Sie diesen Dienst in der Region konfigurieren, in der sich Ihre Anwendung oder Infrastruktur befindet.

In einigen Fällen kann die Region für das AWS Health Ereignis nicht bestimmt werden. Tritt diese Situation ein, wird das Ereignis standardmäßig in der Region USA Ost (Nord-Virginia) angezeigt. Sie können CloudWatch Ereignisse in dieser Region einrichten, um sicherzustellen, dass Sie diese Ereignisse überwachen.

Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.

Aggregieren AWS Health Ereignisse über Konten hinweg

Standardmäßig können Sie es verwenden, AWS Health um die AWS Health Ereignisse eines einzelnen AWS Kontos anzuzeigen. Wenn Sie diese AWS Organizations Option verwenden, können Sie AWS Health Ereignisse auch zentral in Ihrer Organisation anzeigen. Diese Funktion bietet Zugriff auf dieselben Informationen wie Operationen mit einzelnen Konten. Sie können Filter verwenden, um Ereignisse in bestimmten AWS Regionen, Konten und Diensten anzuzeigen.

Sie können Ereignisse aggregieren, um Konten in Ihrer Organisation zu identifizieren, die von einem Betriebsereignis betroffen sind, oder um über Sicherheitslücken informiert zu werden. Sie können diese Informationen dann verwenden, um Ereignisse zur Ressourcenwartung in Ihrem Unternehmen proaktiv zu verwalten und zu automatisieren. Verwenden Sie diese Funktion, um über bevorstehende Änderungen an AWS Diensten auf dem Laufenden zu bleiben, für die möglicherweise Aktualisierungen oder Codeänderungen erforderlich sind.

Es hat sich bewährt, die Funktion Delegierter Administrator zu verwenden, um den Zugriff auf die AWS Health Organisationsansicht an ein Mitgliedskonto zu delegieren. Dies erleichtert den operativen Teams den Zugriff auf die AWS Health Ereignisse in Ihrer Organisation. Mit der Funktion „Delegierter Administrator“ können Sie Ihr Verwaltungskonto einschränken und gleichzeitig den Teams den Überblick geben, den sie benötigen, um auf AWS Health Ereignisse reagieren zu können.

> **Important**
>
> - AWS Health Ereignisse, die für Konten in Ihrer Organisation gesendet wurden, werden in der Unternehmensansicht angezeigt, solange das Ereignis verfügbar ist (bis zu 90 Tage), auch wenn eines oder mehrere dieser Konten Ihre Organisation verlassen.
> - Organisatorische Ereignisse sind 90 Tage lang verfügbar, bevor sie gelöscht werden. Dieses Kontingent kann nicht erhöht werden.

Voraussetzungen

Bevor Sie die Organisationsansicht verwenden, müssen Sie:

- Sie müssen einer Organisation angehören, für die alle Funktionen aktiviert sind.
- Melden Sie sich als AWS Identity and Access Management (IAM-) Benutzer beim Verwaltungskonto an oder übernehmen Sie eine IAM-Rolle.

Sie können sich auch als Root-Benutzer (nicht empfohlen) im Verwaltungskonto Ihrer Organisation anmelden. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Sperren der Root-Benutzerzugriffsschlüssel für Ihr AWS Konto.

- Wenn Sie sich als IAM-Benutzer anmelden, verwenden Sie eine IAM-Richtlinie, die Zugriff auf die Aktionen AWS Health und Organisationen gewährt, z. B. die Richtlinie. AWSHealthFullAccess Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Topics

- Aktivieren der Organisationsansicht
- Organisationsansicht anzeigen
- Deaktivieren der Organisationsansicht
- Delegierte Administratoransichten für eine Organisation verwalten

Aktivieren der Organisationsansicht

Sie können die AWS Health Konsole verwenden, um eine zentrale Ansicht der Gesundheitsereignisse in Ihrer AWS Organisation zu erhalten.

Die Organisationsansicht ist in der AWS Health Konsole für alle AWS Support Tarife ohne zusätzliche Kosten verfügbar.

> **Note**
>
> Wenn Sie Benutzern den Zugriff auf diese Funktion im Verwaltungskonto gewähren möchten, müssen sie über Berechtigungen wie die AWSHealthFullAccess Richtlinie verfügen. Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Enabling organizational view (Console)

Sie können die Organisationsansicht von der AWS Health Konsole aus aktivieren. Sie müssen sich mit dem Verwaltungskonto Ihrer AWS Organisation anmelden.

Um das einzusehen AWS Health Dashboard für Ihre Organisation

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.

2. Wählen Sie im Navigationsbereich unter Status Ihrer Organisation die Option Konfigurationen aus.
3. Wählen Sie auf der Seite Organisationsansicht aktivieren die Option Organisationsansicht aktivieren aus.
4. (Optional) Wenn Sie Änderungen an Ihren AWS Organisationen vornehmen möchten, z. B. Organisationseinheiten (OUs) erstellen möchten, wählen Sie „Verwalten“ AWS Organizations.

   Weitere Informationen finden Sie unter Erste Schritte in AWS Organizations im AWS Organizations -Benutzerhandbuch.

> **Hinweise**
>
> - Wenn Sie die AWS Health Organisationsansicht aktivieren, läuft der anfängliche Ladevorgang des Kontos im Hintergrund ab und kann mehrere Minuten dauern. Sie können die AWS Health Konsole schließen und später zurückkehren, da Sie nicht warten müssen, bis der Vorgang abgeschlossen ist. Es kann bis zu 24 Stunden dauern, bis historische Integritätsereignisse (solche, die vor der Aktivierung der Funktion erstellt wurden) in Ihrer Unternehmensansicht angezeigt werden.
> - Wenn Sie einen AWS Business Support+-, AWS Enterprise Support- oder AWS Unified Operations-Plan haben, können Sie den DescribeHealthServiceStatusForOrganization API-Vorgang aufrufen, um den Status des Prozesses zu überprüfen.
> - Wenn Sie diese Funktion aktivieren, wird die `AWSServiceRoleForHealth_Organizations` serviceverknüpfte Rolle mit der `Health_OrganizationsServiceRolePolicy` AWS verwalteten Richtlinie auf das Verwaltungskonto in der Organisation angewendet. Weitere Informationen finden Sie unter Verwenden Sie serviceverknüpfte Rollen für AWS Health.

Enabling organizational view (CLI)

Sie können die Organisationsansicht mithilfe der EnableHealthServiceAccessForOrganization API-Operation aktivieren.

Sie können die AWS Command Line Interface (AWS CLI) oder Ihren eigenen Code verwenden, um diese Operation aufzurufen.

> **Note**
>
> - Sie müssen über einen Business- On-Ramp, Enterprise- oder Enterprise Support-Plan verfügen, um die AWS Health API aufrufen zu können.
> - Sie müssen den Endpunkt der Region USA Ost (Nord-Virginia) verwenden.

Example

Mit dem folgenden AWS CLI Befehl wird diese Funktion von Ihrem AWS Konto aus aktiviert. Sie können diesen Befehl vom Verwaltungskonto oder von einem Konto aus verwenden, das die Rolle mit den erforderlichen Berechtigungen übernehmen kann.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

In den folgenden Codebeispielen wird der EnableHealthServiceAccessForOrganization API-Vorgang aufgerufen.

Python

```
import boto3

client = boto3.client('health', region_name='us-east-1')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Sie können das AWS SDK für Version Java 2.0 für das folgende Beispiel verwenden.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
```

```
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
```

```
        }
    }
}
```

Weitere Informationen finden Sie im AWS -SDK for Java 2.0-Entwicklerhandbuch.

Wenn Sie diese Funktion aktivieren, wird die `AWSServiceRoleForHealth_Organizations` dienstverknüpfte Rolle mit der `Health_OrganizationsServiceRolePolicy` AWS verwalteten Richtlinie auf das Verwaltungskonto in der Organisation angewendet.

> **Note**
>
> Das Aktivieren dieser Funktion ist ein asynchroner Prozess, der einige Zeit in Anspruch nimmt. Sie können den DescribeHealthServiceStatusForOrganization Vorgang aufrufen, um den Status des Prozesses zu überprüfen.

Organisationsansicht anzeigen

Sie können die AWS Health Konsole verwenden, um eine zentrale Ansicht der Gesundheitsereignisse in Ihrer AWS Organisation zu erhalten.

Die Organisationsansicht ist in der AWS Health Konsole für alle AWS Support Tarife ohne zusätzliche Kosten verfügbar.

> **Note**
>
> Wenn Sie Benutzern den Zugriff auf diese Funktion im Verwaltungskonto gewähren möchten, müssen sie über Berechtigungen wie die AWSHealthFullAccess Richtlinie verfügen. Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Viewing organizational view events (Console)

Nachdem Sie die Organisationsansicht aktiviert haben, AWS Health werden Integritätsereignisse für alle Konten in Ihrer Organisation angezeigt.

Wenn ein Konto Ihrer Organisation beitritt, AWS Health wird das Konto automatisch zur Organisationsansicht hinzugefügt. Wenn ein Konto Ihre Organisation verlässt, werden neue

Ereignisse aus diesem Konto nicht mehr in der Organisationsansicht protokolliert. Vorhandene Ereignisse bleiben jedoch erhalten und Sie können sie bis zum 90-Tage-Limit abfragen.

AWS speichert die Richtliniendaten für das Konto 90 Tage lang ab dem Datum des Inkrafttretens der Schließung des Administratorkontos. Löscht am Ende des Zeitraums von 90 Tagen AWS dauerhaft alle Richtliniendaten für das Konto.

- Zum Aufbewahren von Erkenntnissen für mehr als 90 Tage können Sie die Richtlinien archivieren. Sie können auch eine benutzerdefinierte Aktion mit einer EventBridge Regel verwenden, um die Ergebnisse in einem S3-Bucket zu speichern.
- Solange die Richtliniendaten AWS erhalten bleiben, wird das Konto beim erneuten Öffnen des geschlossenen Kontos AWS erneut als Dienstadministrator zugewiesen und die Servicerichtliniendaten für das Konto wiederhergestellt.
- Weitere Informationen finden Sie unter Schließen eines Kontos.

Important

Für Kunden in den Regionen: AWS GovCloud (US)

- Sichern Sie vor dem Schließen Ihres Kontos die Richtliniendaten und löschen Sie dann Kontoressourcen. Nach dem Schließen des Kontos haben Sie keinen Zugriff mehr darauf.

Note

Wenn Sie diese Funktion aktivieren, kann die AWS Health Konsole öffentliche Ereignisse der letzten 7 Tage im AWS Health Dashboard — Status des Dienstes anzeigen. Diese öffentlichen Ereignisse sind nicht spezifisch für Konten in Ihrer Organisation. Ereignisse aus dem AWS Health Dashboard — Service Health bieten öffentliche Informationen über die regionale Verfügbarkeit von AWS Diensten.

Auf den folgenden Seiten können Sie Ereignisse aus organisatorischer Sicht einsehen:.

Offene und aktuelle Probleme

Auf der Registerkarte „Offene und aktuelle Probleme“ können Sie sich Ereignisse ansehen, die sich auf Ihre AWS Infrastruktur auswirken könnten, z. B. Änderungen an AWS-Services und Ressourcen, die sich auf Ihre Organisation auswirken.

Um Ereignisse der Organisation anzuzeigen

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Status Ihrer Organisation die Option Offen und aktuelle Probleme aus, um die kürzlich gemeldeten Ereignisse anzuzeigen.
3. Wählen Sie ein Ereignis aus. Auf der Registerkarte Details können Sie die folgenden Informationen über das Ereignis überprüfen:

   - Ereignisname
   - Status
   - Region/Verfügbarkeitszone
   - Betroffene Konten
   - Startzeit
   - Endzeit
   - Kategorie
   - Description

Geplante Änderungen

Verwenden Sie den Tab Geplante Änderungen, um bevorstehende Ereignisse anzuzeigen, die sich auf Ihr Unternehmen auswirken könnten. Diese Ereignisse können geplante Wartungsaktivitäten für Dienste beinhalten.

Andere Benachrichtigungen

Verwenden Sie den Tab Benachrichtigungen, um alle anderen Benachrichtigungen und laufenden Ereignisse der letzten sieben Tage anzuzeigen, die sich auf Ihr Unternehmen auswirken könnten. Dazu können Ereignisse wie Zertifikatsrotationen, Abrechnungsbenachrichtigungen und Sicherheitslücken gehören.

Ereignisprotokoll

Sie können auch die Registerkarte „Ereignisprotokoll“ verwenden, um AWS Health Ereignisse für die Organisation anzuzeigen. Das Spaltenlayout und das Verhalten ähneln denen der

Registerkarten „Offene und aktuelle Probleme“, mit der Ausnahme, dass die Registerkarte „Ereignisprotokoll“ zusätzliche Spalten und Filteroptionen enthält, z. B. die Kategorie „Ereignis“, „Status“ und „Startzeit“.

Um die Organisation anzuzeigen, können Sie Ereignisse auf der Registerkarte „Ereignisprotokoll“ anzeigen

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Status Ihrer Organisation die Option Ereignisprotokoll aus.
3. Wählen Sie unter Ereignisprotokoll den Namen des Ereignisses aus. Sie können die folgenden Informationen zu dem Ereignis überprüfen:
   - Ereignisname
   - Status
   - Region/Verfügbarkeitszone
   - Betroffene Konten
   - Startzeit
   - Endzeit
   - Kategorie
   - Description

Viewing affected accounts and resources (Console)

Unter Status Ihrer Organisation können Sie die Konten in Ihrer Organisation, die von dem Ereignis betroffen sind, sowie alle zugehörigen Ressourcen einsehen. Wenn beispielsweise eine bevorstehende Veranstaltung zur Wartung der Amazon Elastic Compute Cloud (Amazon EC2) - Instance ansteht, können Konten in Ihrer Organisation, die über Amazon EC2-Instances verfügen, auf der Registerkarte „Details“ angezeigt werden. Sie können die spezifischen Ressourcen identifizieren und dann den Kontoinhaber kontaktieren.

Um die betroffenen Konten und Ressourcen einzusehen

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Status Ihres Unternehmens eine der Registerkarten aus.

3. Wählen Sie ein Ereignis aus, das einen Wert für Betroffene Konten hat.
4. Wählen Sie den Tab Betroffene Konten.
5. Wählen Sie Kontodetails anzeigen, um die folgenden Informationen für die Konten anzuzeigen:

   - Konto-ID
   - Account name (Kontoname)
   - Primäre E-Mail-Adresse
   - Organisationseinheit (OU)
6. Erweitern Sie das Konto, um die betroffenen Ressourcen anzuzeigen.
7. Wenn es mehr als 10 Ressourcen gibt, wählen Sie Alle Ressourcen anzeigen, um sie anzuzeigen.
8. Gehen Sie wie folgt vor, um nach der Konto-ID für dieses bestimmte Ereignis zu filtern:

   a. Wählen Sie auf der Registerkarte Betroffene Konten die Option Filter hinzufügen aus, wählen Sie Konto-ID aus, und geben Sie dann die Konto-ID ein. Sie können jeweils nur eine Konto-ID eingeben.

   b. Wählen Sie Anwenden aus. Das von Ihnen eingegebene Konto wird in der Liste angezeigt.

Viewing organizational view events (CLI)

Nachdem Sie diese Funktion aktiviert haben, AWS Health beginnt die Aufzeichnung von Ereignissen, die sich auf Konten in der Organisation auswirken. Wenn ein Konto Ihrer Organisation beitritt, fügt das Konto AWS Health automatisch der Organisationsansicht hinzu.

> **Note**
>
> AWS Health zeichnet keine Ereignisse auf, die in Ihrer Organisation eingetreten sind, bevor Sie die Organisationsansicht aktiviert haben.

Wenn ein Konto Ihre Organisation verlässt, werden neue Ereignisse aus diesem Konto nicht mehr in der Organisationsansicht protokolliert. Vorhandene Ereignisse bleiben jedoch erhalten und Sie können sie bis zum 90-Tage-Limit abfragen.

AWS speichert die Richtliniendaten für das Konto 90 Tage lang ab dem Datum des Inkrafttretens der Schließung des Administratorkontos. Löscht am Ende des Zeitraums von 90 Tagen AWS dauerhaft alle Richtliniendaten für das Konto.

- Zum Aufbewahren von Erkenntnissen für mehr als 90 Tage können Sie die Richtlinien archivieren. Sie können auch eine benutzerdefinierte Aktion mit einer EventBridge Regel verwenden, um die Ergebnisse in einem S3-Bucket zu speichern.
- Solange die Richtliniendaten AWS erhalten bleiben, wird das Konto beim erneuten Öffnen des geschlossenen Kontos AWS erneut als Dienstadministrator zugewiesen und die Servicerichtliniendaten für das Konto wiederhergestellt.
- Weitere Informationen finden Sie unter Schließen eines Kontos.

> **Important**
>
> Für Kunden in den Regionen: AWS GovCloud (US)
>
> - Sichern Sie vor dem Schließen Ihres Kontos die Richtliniendaten und löschen Sie dann Kontoressourcen. Nach dem Schließen des Kontos haben Sie keinen Zugriff mehr darauf.

Sie können die AWS Health API-Operationen verwenden, um Ereignisse aus organisatorischer Sicht zurückzugeben.

Example: Ereignisse für die Organisationsansicht beschreiben

Der folgende AWS CLI Befehl gibt Integritätsereignisse für AWS Konten in Ihrer Organisation zurück.

```
aws health describe-events-for-organization --region us-east-1
```

Deaktivieren der Organisationsansicht

Wenn Sie keine Ereignisse für Ihre Organisation zusammenfassen möchten, können Sie diese Funktion über das Verwaltungskonto deaktivieren oder die Organisationsansicht mithilfe der DisableHealthServiceAccessForOrganizationAPI-Operation deaktivieren.

Disabling organizational view events (Console)

AWS Health beendet das Aggregieren von Ereignissen für alle anderen Konten in Ihrer Organisation. Sie können sich weiterhin frühere Ereignisse aus Ihrer Organisation ansehen, bis sie gelöscht werden.

Um die Organisationsansicht zu deaktivieren

1. Öffnen Sie Ihr AWS Health Dashboard zu https://health.aws.amazon.com/health/Hause.
2. Wählen Sie im Navigationsbereich unter Ihr Unternehmensstatus die Option Konfigurationen aus.
3. Wählen Sie auf der Seite Organisationsansicht aktivieren die Option Organisationsansicht deaktivieren aus.

Nachdem Sie diese Funktion deaktiviert haben, werden AWS Health keine Ereignisse aus Ihrer Organisation mehr aggregiert. Die dienstverknüpfte Rolle verbleibt jedoch im Verwaltungskonto, bis Sie sie über die AWS Identity and Access Management (IAM-) Konsole, die IAM-API oder () löschen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Disabling organizational view events (CLI)

Example

Mit dem folgenden AWS CLI Befehl wird diese Funktion in Ihrem Konto deaktiviert.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> Sie können die Organisationsfunktion auch deaktivieren, indem Sie den API-Vorgang Organizations Disable AWSService Access verwenden. AWS Health Beendet nach dem Aufrufen dieses Vorgangs die Aggregation von Ereignissen für alle anderen Konten in Ihrer Organisation. Wenn Sie die AWS Health API-Operationen für die Organisationsansicht aufrufen, wird ein Fehler AWS Health zurückgegeben. AWS Health aggregiert weiterhin Gesundheitsereignisse für Ihr AWS Konto.

Nachdem Sie diese Funktion deaktiviert haben, werden AWS Health keine Ereignisse aus Ihrer Organisation mehr aggregiert. Die dienstverknüpfte Rolle verbleibt jedoch im Verwaltungskonto, bis Sie sie über die AWS Identity and Access Management (IAM-) Konsole, die IAM-API oder löschen. AWS CLIWeitere Informationen finden Sie unter Löschen einer dienstbezogenen Rolle im IAM-Benutzerhandbuch.

Delegierte Administratoransichten für eine Organisation verwalten

Mit AWS Health können Sie die Funktion für delegierte Administratoren nutzen AWS Organizations , mit der ein anderes Konto als das Verwaltungskonto aggregierte AWS Health Ereignisse im AWS Health Dashboard oder programmgesteuert über die API anzeigen kann.AWS Health Die Funktion für delegierte Administratoren bietet verschiedenen Teams die Flexibilität, Gesundheitsereignisse in Ihrem Unternehmen einzusehen und zu verwalten. Es ist eine bewährte AWS Sicherheitsmethode, Verantwortlichkeiten nach Möglichkeit außerhalb des Verwaltungskontos zu delegieren.

Inhalt

- Registrierung eines delegierten Administrators für Ihre Unternehmensansicht
- Einen delegierten Administrator aus Ihrer Unternehmensansicht entfernen

Registrierung eines delegierten Administrators für Ihre Unternehmensansicht

Nachdem Sie die Organisationsansicht für Ihre Organisation aktiviert haben, können Sie bis zu fünf Mitgliedskonten in Ihrer Organisation als delegierter Administrator registrieren. Rufen Sie dazu den RegisterDelegatedAdministratorAPI-Vorgang auf. Nachdem Sie die Mitgliedskonten registriert haben, sind sie ein delegiertes Administratorkonto und können über das AWS Health Dashboard auf die AWS Health Organisationsansicht zugreifen. Wenn das Konto über einen Business -, Enterprise On-Ramp - oder Enterprise Support-Plan verfügt, können die delegierten Administratoren die AWS Health API verwenden, um auf die AWS Health Organisationsansicht zuzugreifen.

Um einen delegierten Administrator einzurichten, rufen Sie vom Verwaltungskonto in Ihrer Organisation aus den folgenden Befehl AWS Command Line Interface ()AWS CLI auf. Sie können diesen Befehl vom Verwaltungskonto oder von einem Konto aus verwenden, das die Rolle mit den erforderlichen AWS Identity and Access Management Berechtigungen übernehmen kann. Ersetzen Sie im folgenden Beispielbefehl ACCOUNT_ID durch die Mitgliedskonto-ID, die Sie zusammen mit dem AWS Health Dienstprinzipal „health.amazonaws.com“ registrieren möchten.

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Nachdem ein delegierter Administrator registriert wurde, haben Sie Einblick in alle Ereignisse, die sich auf Konten in Ihrer gesamten AWS Health Organisation auswirken. Sie können historische Ereignisse der letzten 90 Tage oder seit der ersten Aktivierung der Funktion zur Organisationsansicht anzeigen, je nachdem, welcher Zeitpunkt aktueller ist. Beachten Sie, dass die Aktivierung der Funktion für delegierte Administratoren ein asynchroner Vorgang ist und bis zu einer Minute in Anspruch nimmt.

Einen delegierten Administrator aus Ihrer Unternehmensansicht entfernen

Rufen Sie den API-Vorgang auf, um einem delegierten Administrator den Zugriff zu entziehen. DeregisterDelegatedAdministrator

Rufen Sie vom Verwaltungskonto Ihrer Organisation aus den folgenden AWS CLI Befehl auf, um ein Mitgliedskonto als delegierter Administrator zu entfernen. Ersetzen Sie im folgenden Beispielbefehl ACCOUNT_ID durch die Mitgliedskonto-ID, die Sie entfernen möchten.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Überwachung von Ereignissen in AWS Health mit Amazon EventBridge

Sie können Amazon verwenden EventBridge , um AWS Health Ereignisse zu erkennen und darauf zu reagieren. Ruft dann auf der Grundlage der von Ihnen erstellten Regeln eine EventBridge oder mehrere Zielaktionen auf, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben. Je nach Art des Ereignisses können Sie Ereignisinformationen erfassen, zusätzliche Ereignisse auslösen, Benachrichtigungen senden, Korrekturmaßnahmen ergreifen oder andere Aktionen ausführen. Sie können es beispielsweise verwenden, um E-Mail-Benachrichtigungen AWS Health zu erhalten, wenn Sie AWS Ressourcen in Ihrem System haben, für AWS-Konto die Updates geplant sind, wie z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Hinweise

- AWS Health stellt Ereignisse dauerhaft bereit und versucht, EventBridge mindestens einmal erfolgreich Ereignisse zuzustellen.
- Alle EventBridge Regeln, die Sie erstellen, können nur Benachrichtigungen für Sie empfangen AWS-Konto. Informationen zum Empfangen von Organisationsereignissen für andere Konten in Ihrem AWS Organizations Konto finden Sie unter Aggregieren von AWS Health Ereignissen mithilfe der Organisationsansicht und delegierten Administratorzugriff.
- Es kann bis zu einer Stunde dauern, bis Ereignisse im Bereich der öffentlichen Gesundheit versendet werden, nachdem Sie eine EventBridge Regel erstellt haben.

Im EventBridge Rahmen Ihres AWS Health Workflows können Sie zwischen mehreren Zieltypen wählen, darunter:

- AWS Lambda Funktionen
- Amazon Kinesis Data Streams
- Amazon-Simple-Queue-Service-(Amazon-SQS)-Warteschlangen
- Built-in Ziele (wie CloudWatch Alarmaktionen)
- Amazon Simple Notification Service (Amazon SNS)-Themen

Du kannst zum Beispiel eine Lambda-Funktion verwenden, um eine Benachrichtigung an einen Slack-Channel weiterzuleiten, wenn ein AWS Health Ereignis eintritt. Sie können Lambda auch verwenden, EventBridge um benutzerdefinierte Text- oder SMS-Benachrichtigungen mit Amazon SNS zu senden, wenn ein Ereignis eintritt. AWS Health

Beispiele für Automatisierungen und benutzerdefinierte Benachrichtigungen, die Sie als Reaktion auf AWS Health Ereignisse erstellen können, finden Sie in den AWS Health Tools unter. GitHub

Themen

- EventBridge Regeln erstellen für AWS-Region Abdeckung
- Überwachung kontospezifischer und öffentlicher Ereignisse für AWS Health
- Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge
- Aggregieren AWS Health Ereignisse mithilfe der Unternehmensansicht und des delegierten Administratorzugriffs
- Integration AWS Health Ereignisüberwachung und Benachrichtigungen mit JIRA und ServiceNow
- Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health
- Konfiguration von Amazon Q Developer in Chat-Anwendungen zum Senden von Benachrichtigungen über Ereignisse in AWS Health
- Automatisches Ausführen von Vorgängen auf EC2-Instances als Reaktion auf Ereignisse in AWS Health
- Referenz: AWS Health Veranstaltungen Amazon EventBridge schema

EventBridge Regeln erstellen für AWS-Region Abdeckung

Sie können für jede Region, für die Sie AWS Health Ereignisse erhalten möchten, eine EventBridge Regel erstellen. Um beispielsweise Ereignisse aus der Region Europa (Frankfurt) zu erhalten, können Sie eine Regel für diese Region erstellen.

Um die Zuverlässigkeit von AWS Health Benachrichtigungen zu erhöhen, können Sie Regeln in den dedizierten Backup-Regionen einrichten. In der AWS Standardpartition fungiert die Region USA West (Oregon) als Backup-Region für alle anderen Regionen, während die Region USA Ost (Nord-Virginia) als Backup-Region für die Region USA West (Oregon) dient. Wenn Integritätsereignisse auftreten, werden sie automatisch sowohl an die primäre Region als auch an die dafür vorgesehene Backup-Region gesendet. Wenn Sie beispielsweise Ereignisse in der Region Europa (Frankfurt)

überwachen, werden alle Gesundheitsereignisse sowohl in die Region Europa (Frankfurt) als auch in die Region USA West (Oregon) übermittelt. Dieses System stellt sicher, dass Sie auch dann weiterhin Gesundheitsbenachrichtigungen erhalten, wenn in Ihrer Hauptregion Probleme auftreten. Um eine Backup-Regel zu erstellen, folgen Sie dem Verfahren fürKonfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health.

Wenn Sie die Backup-Funktion lieber nicht verwenden möchten, müssen Sie Ihrer Backup-Regionsregel einen Filter hinzufügen. Implementieren Sie beispielsweise einen Filter für`detail.backupEvent = False`. Dadurch wird verhindert, dass Sie Backup-Ereignisse aus anderen Regionen erhalten.

Einrichtung für hohe Verfügbarkeit (optional)

Wenn Sie eine EventBridge Integration mit hoher Verfügbarkeit erstellen möchten, stellen Sie sicher, dass Sie Regeln sowohl in der relevanten Region als auch in der Backup-Region implementiert haben, und implementieren Sie dann die Deduplizierung mithilfe von. `detail.communicationId` Dadurch wird sichergestellt, dass Sie alle Ereignisse erhalten und gleichzeitig Duplikate vermieden werden. Weitere Informationen finden Sie unter Referenz: AWS Health Veranstaltungen Amazon EventBridge schema.

Vereinfachte Integration

Wenn Sie kontospezifische Ereignisse mehrerer Konten erfassen möchten AWS-Regionen, aber lieber nur eine einzige Regel konfigurieren möchten, ist eine vereinfachte Integration die geeignete Option. Um kontospezifische AWS Health Ereignisse aus allen Regionen der AWS Standardpartition zu empfangen, können Sie eine zentrale Regel in der Region USA West (Oregon) einrichten. Diese einzelne Regel aggregiert automatisch kontospezifische Ereignisse aus allen Standardpartitionsregionen. Sie werden jedoch keine Hochverfügbarkeitskonfiguration haben.

> **Note**
>
> Die vereinfachte Integration ermöglicht es Ihnen nicht, öffentliche Ereignisse zu empfangen, die im AWS Health Dashboard angezeigt werden. Eine vereinfachte Integration wird nur für die Erfassung von Ereignissen empfohlen, die eine Aktion erfordern. AWS Health Weitere Informationen zu öffentlichen und kontospezifischen Ereignissen finden Sie unter. Überwachung kontospezifischer und öffentlicher Ereignisse für AWS Health

Weltweite Ereignisse

Manche AWS Health Ereignisse sind es nicht Region-specific. Ereignisse, die nicht spezifisch für eine Region sind, werden als globale Ereignisse bezeichnet. Dazu gehören Ereignisse, für die gesendet wurde AWS Identity and Access Management (IAM). Um globale Ereignisse zu empfangen, müssen Sie eine Regel für die Region USA Ost (Nord-Virginia) erstellen.

Überwachung kontospezifischer und öffentlicher Ereignisse für AWS Health

Wenn Sie eine EventBridge Regel zur Überwachung von Ereignissen erstellen AWS Health, liefert die Regel sowohl kontospezifische Ereignisse als auch öffentliche Ereignisse:

- Account-specificEreignisse wirken sich auf Ihr Konto und Ihre Ressourcen aus, z. B. ein Ereignis, das Sie über ein erforderliches Update einer Amazon EC2-Instance oder über andere geplante Änderungsereignisse informiert.
- Öffentliche Ereignisse werden im AWS Health Dashboard — Service Health angezeigt. Öffentliche Veranstaltungen beziehen sich nicht auf die regionale Verfügbarkeit eines Dienstes AWS-Konten und bieten keine öffentlichen Informationen darüber.

> **Important**
>
> Um beide Ereignistypen zu empfangen, muss Ihre Regel den `"source": [ "aws.health"]` Wert verwenden. Platzhalter, z. B. entspricht `"source": [ "aws.health*"]` nicht dem Muster, das auf Ereignisse überwacht werden soll.

Mithilfe des Event-Parameters können Sie feststellen EventBridge, ob ein Ereignis öffentlich oder kontospezifisch ist. ScopeCode Ereignisse können das oder haben. `PUBLIC` `ACCOUNT_SPECIFIC` Sie können Ihre Regel auch nach diesem Parameter filtern.

Ein Beispiel für eine öffentliche Veranstaltung für Amazon Elastic Compute Cloud finden Sie unterVeranstaltung im Bereich der öffentlichen Gesundheit — Betriebsproblem bei Amazon EC2.

Backup-Regeln für AWS Health Veranstaltungen

Wenn Sie öffentliche Ereignisse von einem aus überwachen AWS-Region, empfehlen wir Ihnen, eine Backup-Regel zu erstellen. Öffentliche Ereignisse für AWS Health werden gleichzeitig sowohl an die betroffene Region als auch an die Backup-Region gesendet, wenn in der betroffenen Region eine gültige Regel festgelegt wurde.

> **Important**
>
> Wenn Sie in der betroffenen Region keine Regel haben, versendet die Backup-Region das öffentliche Ereignis nicht automatisch als Backup. Sie müssen in der betroffenen Region über eine gültige Regel verfügen, damit öffentliche Ereignisse in die Backup-Region übertragen werden können.

AWS Health sendet kontospezifische Ereignisse sowohl an die betroffene Region als auch an die Backup-Region, unabhängig von den in der betroffenen Region konfigurierten Regeln.

Wir empfehlen, AWS Health Ereignisse mithilfe von `eventARN` und zu deduplizieren, `communicationId` da diese Werte für AWS Health Nachrichten, die an die Backup-Region gesendet werden, konsistent bleiben.

Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge

AWS Health unterstützt die Paginierung von AWS Health Ereignissen, wenn die Liste `resources` `affectedEntities` oder die Größe der Nachricht die maximale Nachrichtengröße EventBridge von 256 KB überschreitet.

AWS Health schließt alle `detail.affectedEntities` Felder `resources` und in der Nachricht ein. Wenn diese Liste von `resources` `detail.affectedEntities` Werten 256 KB überschreitet, wird das Gesundheitsereignis auf mehrere Seiten AWS Health aufgeteilt und diese Seiten als einzelne Nachrichten veröffentlicht. EventBridge Jede Seite behält dieselben `eventARN` `communicationId` Endwerte bei, um die Liste von `resources` oder `detail.affectedEntities` nach Erhalt aller Seiten neu zusammenstellen zu können.

Diese zusätzlichen Nachrichten können zu unnötigen Nachrichten führen, z. B. wenn die EventBridge Regel an eine menschenlesbare Oberfläche wie E-Mail oder Chat gerichtet ist. Kunden mit

menschenlesbaren Benachrichtigungen können einen Filter für das `detail.page` Feld hinzufügen, sodass nur die erste Seite verarbeitet wird. Dadurch werden unnötige Nachrichten aus nachfolgenden Seiten entfernt.

Im Schema enthält jede CommunicationID die mit Bindestrich versehene Seitenzahl nach der CommunicationID, auch wenn es nur eine Seite gibt. Die Felder `detail.page` und `detail.totalPages` beschreiben die aktuelle Seitennummer und die Gesamtzahl der Seiten für das Ereignis. AWS Health Die in jeder paginierten Nachricht enthaltenen Informationen sind mit Ausnahme der Liste von `detail.affectedEntities` oder `resources` identisch. Diese Listen können rekonstruiert werden, nachdem alle Seiten empfangen wurden. Die Seiten der betroffenen Ressourcen und Entitäten sind unabhängig von der Reihenfolge.

Aggregieren AWS Health Ereignisse mithilfe der Unternehmensansicht und des delegierten Administratorzugriffs

AWS Health unterstützt die organisatorische Ansicht und den delegierten Administratorzugriff für auf AWS Health Amazon veröffentlichte Veranstaltungen. EventBridge Wenn die Organisationsansicht aktiviert ist AWS Health, erhält das Verwaltungskonto oder ein delegiertes Administratorkonto einen einzigen Feed mit AWS Health Ereignissen aus allen Konten innerhalb Ihrer Organisation in. AWS Organizations

Diese Funktion bietet eine zentrale Ansicht, die Sie bei der Verwaltung von AWS Health Ereignissen in Ihrer Organisation unterstützt. Durch das Einrichten der Organisationsansicht und einer EventBridge Regel im Verwaltungskonto werden die EventBridge Regeln für andere Konten in Ihrer Organisation nicht deaktiviert.

Weitere Informationen zur Aktivierung der Organisationsansicht und des delegierten Administratorzugriffs auf AWS Health finden Sie unter Aggregieren von Ereignissen AWS Health .

Integration AWS Health Ereignisüberwachung und Benachrichtigungen mit JIRA und ServiceNow

⚠ Mitteilung zum Ende des Supports

Am 31. März 2027 AWS endet die Unterstützung für. AWS Service Management Connector Nach dem 31. März 2027 können Sie nicht mehr auf die Service Management Connector-

Konsole oder die Service Management Connector-Ressourcen zugreifen. Weitere Informationen finden Sie unter AWS Service Management Connector Ende des Supports.

Mit dem Service Management Connector (SMC) können Sie AWS Health Ereignisse in JIRA integrieren und Betriebs- und Kontoinformationen abrufen, sich auf geplante Änderungen vorbereiten und Gesundheitsereignisse verwalten. ServiceNow Die SMC-Integration mit AWS Health kann gesendete Health-Ereignisse verwenden, EventBridge um JIRA-Tickets und -Vorfälle automatisch zu erstellen, zuzuordnen und zu aktualisieren. ServiceNow

Du kannst die Unternehmensansicht und den delegierten Administratorzugriff verwenden, um Gesundheitsereignisse im gesamten Unternehmen in JIRA einfach zu verwalten und ServiceNow AWS Health Informationen direkt in den Arbeitsablauf deines Teams zu integrieren.

Weitere Informationen zur ServiceNow Integration mit SMC finden Sie unter Integrieren in. AWS Health ServiceNow

Weitere Informationen zur JIRA Management Cloud-Integration mithilfe des SMC findest du AWS Health unter In JIRA.

Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health

Sie können eine EventBridge Amazon-Regel erstellen, um AWS Health Ereignisse programmgesteuert in andere Dienste, Anwendungen und Workloads zu integrieren. EventBridge bietet eine Drag-and-Drop-Konsolenschnittstelle und eine API zum Einrichten von Regeln, die ausgelöst werden, wenn ein passendes AWS Health Ereignis für Ihr Konto oder Ihre Organisation erstellt wird. Informationen zum Einrichten einer Regel EventBridge zur Erfassung von AWS Health Ereignissen finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von Regeln mit dem Enhanced Builder und Erstellen von Regeln mit dem Advanced Builder .

Abhängig von Ihrer Integration EventBridge können Sie der EventBridge Regel Parameter hinzufügen, um nur die AWS Health Ereignisse zu filtern, die Sie in Ihren Anwendungsfall integrieren möchten. Bei Anwendungsfällen zur Reaktion auf Vorfälle sollten Sie sich möglicherweise auf die `issue` Ereigniskategorie und bestimmte wichtige Dienste konzentrieren. Für Anwendungsfälle im Bereich Change Management, wie z. B. geplante Ereignisse im Lebenszyklus, sollten Sie sich auf AWS Health Ereignisse konzentrieren, die `ACTION_REQUIRED` im Feld Actionability aufgeführt sind. Für die Integration mit Sicherheitsanwendungsfällen sollten Sie sich möglicherweise auf alle

AWS Health Missbrauchsereignisse und AWS Health Ereignisse mit dem `SECURITY` Persona-Feld konzentrieren.

Anhand von Beispielanwendungsfällen können Sie überprüfen, ob Ihre Regel die von Ihnen benötigten Ereignisse erfasst. Beispiele für Anwendungsfälle finden Sie unterReferenz: AWS Health Veranstaltungen Amazon EventBridge schema. Sie finden sie auch in der EventBridge Konsole unter der Option Bereitgestellte Beispielereignisse verwenden im Bereich Eventmuster testen — optional

Mithilfe der API oder AWS Command Line Interface

Verwenden Sie für eine neue oder bestehende Regel den PutRule API-Vorgang oder den `aws events put-rule` Befehl, um das Ereignismuster zu aktualisieren. Einen AWS CLI Beispielbefehl finden Sie unter put-rule in der AWS CLI Befehlsreferenz.

Example Beispiel: Regeln für Probleme nur für den Amazon EC2-Service einrichten

Das folgende Ereignismuster erstellt eine Regel zur Überwachung von Problemereignissen für den Amazon EC2-Service.

```
{
  "detail": {
    "eventTypeCategory": [
      "issue"
    ],
    "service": [
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Example Beispiel: Regeln für alle erforderlichen Aktionen einrichten AWS Health Ereignisse, einschließlich geplanter Lebenszyklusereignisse

Das folgende Ereignismuster erstellt eine Regel zur Überwachung aller AWS Health Ereignisse, die Maßnahmen erfordern, einschließlich geplanter Lebenszyklusereignisse.

```
{
  "detail": {
    "eventTypeCategory": [
      "accountNotification",
      "scheduledChange"
    ],
    "actionability": [
      "ACTION_REQUIRED"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Example Beispiel: Regeln für alle einrichten AWS Health Ereignisse für mehrere Dienste und Kategorien von Ereignistypen

Das folgende Ereignismuster erstellt eine Regel zur Überwachung von Ereignissen für die Kategorien`issue`,`accountNotification`, und `scheduledChange` Ereignistypen für drei AWS Dienste: Amazon EC2 Auto Scaling, Amazon VPC und Amazon EC2.

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
```

```
    "aws.health"
  ]
}
```

Konfiguration von Amazon Q Developer in Chat-Anwendungen zum Senden von Benachrichtigungen über Ereignisse in AWS Health

Sie können AWS Health Ereignisse direkt in Ihren Chat-Clients wie Slack und Amazon Chime empfangen. Sie können dieses Ereignis verwenden, um aktuelle AWS Serviceprobleme zu identifizieren, die sich auf Ihre AWS Anwendungen und Infrastruktur auswirken könnten. Anschließend können Sie sich in Ihrem AWS Health Dashboard anmelden, um mehr über das Update zu erfahren. Wenn du beispielsweise in deinem AWS Account nach dem `AWS_EC2_INSTANCE_STOP_SCHEDULED` Ereignistyp Ausschau hältst, kann das AWS Health Ereignis direkt in deinem Slack-Kanal angezeigt werden.

Voraussetzungen

Bevor du loslegst, musst du über Folgendes verfügen:

- Ein Chat-Client, der mit Amazon Q Developer in Chat-Anwendungen konfiguriert wurde. Sie können Amazon Chime und Slack konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Q Developer in Chat-Anwendungen im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.
- Ein Amazon SNS-Thema, das Sie erstellt haben und das Sie abonniert haben. Wenn Sie bereits ein SNS-Thema haben, können Sie ein vorhandenes verwenden. Weitere Informationen finden Sie unter Erste Schritte mit Amazon SNS im Benutzerhandbuch für Amazon Simple Notification Service.

Um zu erhalten AWS Health Ereignisse mit Amazon Q Developer in Chat-Anwendungen

1. Folgen Sie den Anweisungen zum Einrichten einer Regel in Amazon EventBridge zur Erfassung von AWS Health Ereignissen, die unter Erstellen von Regeln mit dem Enhanced Builder und Erstellen von Regeln mit dem Advanced Builder im EventBridge Amazon-Benutzerhandbuch beschrieben sind. Weitere Informationen finden Sie unter Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health.

a. Wenn Sie mit der Einrichtung des Event-Musters fertig sind, fügen Sie der letzten Zeile des Musters ein Komma hinzu und fügen Sie die folgende Zeile hinzu, um unnötige Chat-Nachrichten aus paginierten AWS Health Ereignissen zu entfernen. Siehe Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge.

```
"detail.page": ["1"]
```

b. Wenn Sie das Ziel ausgewählt haben, wählen Sie ein SNS-Thema aus. Sie verwenden dasselbe SNS-Thema im Amazon Q Developer in der Chat-Anwendungskonsole.

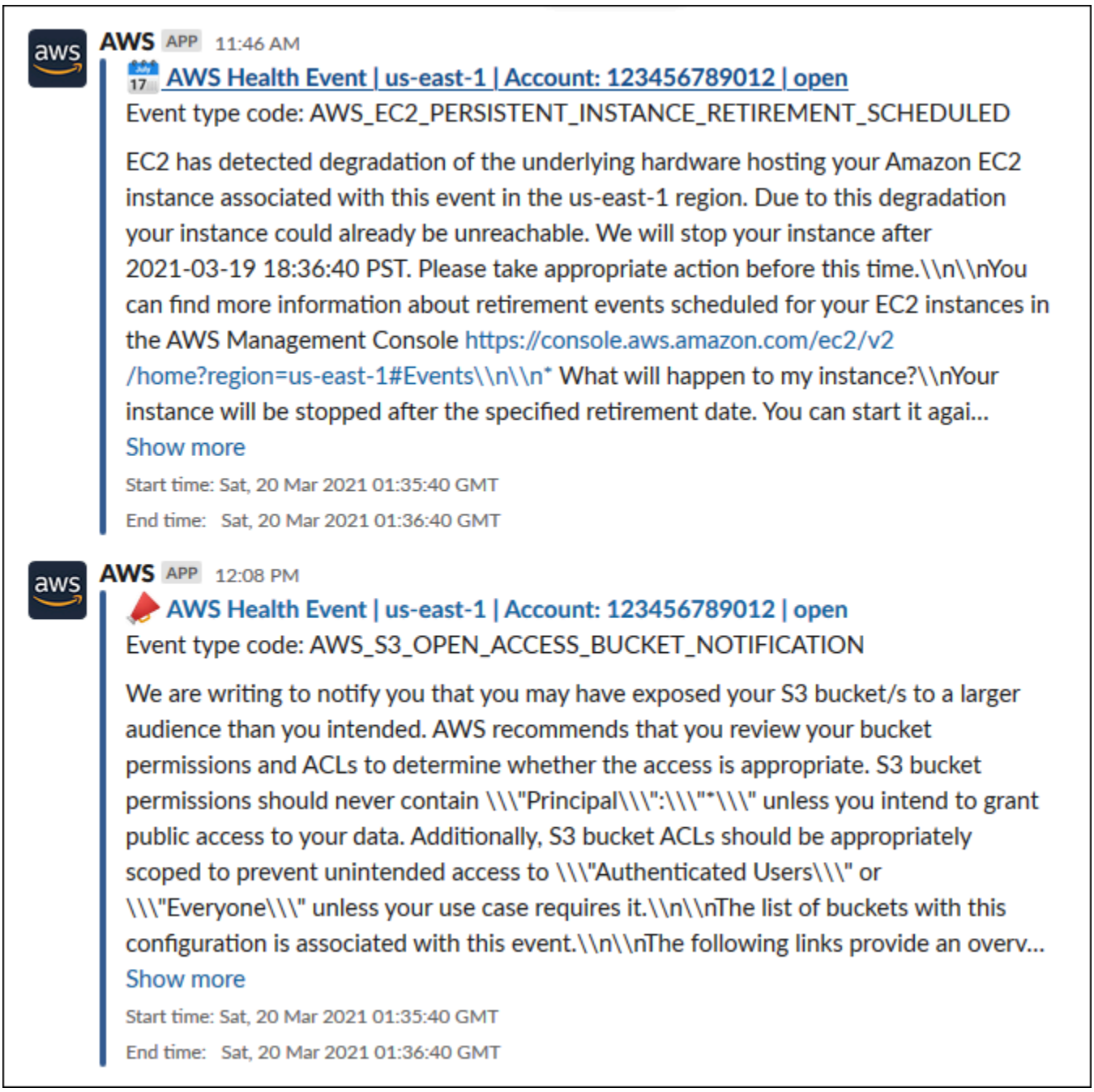
c. Schließen Sie den Rest des Verfahrens ab, um die Regel zu erstellen.

2. Navigieren Sie in der Chat-Anwendungskonsole zum Amazon Q Developer.
3. Wählen Sie Ihren Chat-Client, z. B. den Namen Ihres Slack-Kanals, und wählen Sie dann Bearbeiten.
4. Wähle im Abschnitt Benachrichtigungen — optional für Themen dasselbe SNS-Thema aus, das du in Schritt 1 angegeben hast.
5. Wählen Sie Speichern.

   Wenn ein Ereignis an Sie AWS Health gesendet wird EventBridge , das Ihrer Regel entspricht, wird das AWS Health Ereignis in Ihrem Chat-Client angezeigt.
6. Wählen Sie den Namen des Ereignisses, um weitere Informationen in Ihrem AWS Health Dashboard zu sehen.

Example: AWS Health Ereignisse, die an Slack gesendet wurden

Das Folgende ist ein Beispiel für zwei AWS Health Ereignisse für Amazon EC2 und Amazon Simple Storage Service (Amazon S3) in der Region USA Ost (Nord-Virginia), die im Slack-Kanal erscheinen.



Automatisches Ausführen von Vorgängen auf EC2-Instances als Reaktion auf Ereignisse in AWS Health

Sie können Aktionen automatisieren, die auf geplante Ereignisse für Ihre Amazon EC2-Instances reagieren. Wenn ein Ereignis an Ihr AWS Konto AWS Health gesendet wird, kann Ihre EventBridge Regel dann Ziele wie AWS Systems Manager Automatisierungsdokumente aufrufen, um Aktionen in Ihrem Namen zu automatisieren.

Wenn beispielsweise ein Ereignis zur Außerbetriebnahme einer Amazon EC2-Instance für eine vom Amazon Elastic Block Store (Amazon EBS) unterstützte EC2-Instance geplant ist, AWS Health wird der `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` Ereignistyp an Ihr Dashboard gesendet. AWS Health Wenn Ihre Regel diesen Ereignistyp erkennt, können Sie das Stoppen und Starten der Instance automatisieren. Auf diese Weise müssen Sie diese Aktionen nicht manuell ausführen.

> **Note**
>
> Um Aktionen für Ihre Amazon EC2-Instances zu automatisieren, müssen die Instances von Systems Manager verwaltet werden.

Weitere Informationen finden Sie unter Automatisieren von Amazon EC2 mit EventBridge im Amazon EC2-Benutzerhandbuch.

Voraussetzungen

Sie müssen eine AWS Identity and Access Management (IAM-) Richtlinie erstellen, eine IAM-Rolle erstellen und die Vertrauensrichtlinie der Rolle aktualisieren, bevor Sie eine Regel erstellen können.

Eine IAM-Richtlinie erstellen

Gehen Sie wie folgt vor, um eine vom Kunden verwaltete Richtlinie für Ihre Rolle zu erstellen. Diese Richtlinie gibt der Rolle die Erlaubnis, Aktionen in Ihrem Namen auszuführen. Dieses Verfahren verwendet den JSON-Richtlinieneditor in der IAM-Konsole.

So erstellen Sie eine IAM-Richtlinie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie den Tab JSON.
5. Kopieren Sie das folgende JSON und ersetzen Sie dann das Standard-JSON im Editor.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
```

```
}
```

a. Geben Sie im `Resource` Parameter für den Amazon-Ressourcennamen (ARN) Ihre AWS Konto-ID ein.

b. Sie können auch den Rollennamen ersetzen oder den Standardnamen verwenden. Dieses Beispiel verwendet *`AutomationEVRole`*.

6. Wählen Sie Next: Markierungen (Weiter: Markierungen).
7. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Richtlinie Metadaten hinzuzufügen.
8. Wählen Sie Weiter: Prüfen aus.
9. Geben Sie auf der Seite „Richtlinie überprüfen“ einen Namen ein, z. B. *`AutomationEVRolePolicy`* und optional eine Beschreibung.
10. Sehen Sie auf der Seite „Zusammenfassung“ nach, welche Berechtigungen die Richtlinie zulässt. Wenn Sie mit Ihrer Richtlinie zufrieden sind, wählen Sie Richtlinie erstellen aus.

Diese Richtlinie definiert die Aktionen, die die Rolle ausführen kann. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Erstellen einer IAM-Rolle

Nachdem Sie die Richtlinie erstellt haben, müssen Sie eine IAM-Rolle erstellen und die Richtlinie dann dieser Rolle anfügen.

Um eine Rolle für einen zu erstellen AWS Service nicht zulässig

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.
3. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität wählen) die Option AWS Service aus.
4. Wählen Sie EC2 für den Dienst aus, dem Sie die Übernahme dieser Rolle gestatten möchten.
5. Wählen Sie Weiter: Berechtigungen aus.
6. Geben Sie den Richtliniennamen ein, den Sie erstellt haben*`AutomationEVRolePolicy`*, z. B., und aktivieren Sie dann das Kontrollkästchen neben der Richtlinie.

7. Wählen Sie Weiter: Tags aus.
8. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Rolle Metadaten hinzuzufügen.
9. Wählen Sie Weiter: Prüfen aus.
10. Geben Sie für Role name (Rollenname) den Namen *AutomationEVRole* ein. Bei diesem Namen muss es sich um denselben Namen handeln, der im ARN der von Ihnen erstellten IAM-Richtlinie erscheint.
11. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die Rolle ein.
12. Prüfen Sie die Rolle und klicken Sie dann auf Create Role (Rolle erstellen).

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erstellen einer Rolle für einen AWS Dienst.

Aktualisieren Sie die Vertrauensrichtlinie

Schließlich können Sie die Vertrauensrichtlinie für die von Ihnen erstellte Rolle aktualisieren. Sie müssen dieses Verfahren abschließen, damit Sie diese Rolle in der EventBridge Konsole auswählen können.

Um die Vertrauensrichtlinie für die Rolle zu aktualisieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen.
3. Wählen Sie in der Liste der Rollen in Ihrem AWS Konto den Namen der Rolle aus, die Sie erstellt haben, z. B. *AutomationEVRole*
4. Klicken Sie auf der Registerkarte Trust Relationships (Vertrauensbeziehungen) auf Edit Trust Relationship (Vertrauensbeziehungen bearbeiten).
5. Kopieren Sie für das Richtliniendokument die folgende JSON-Datei, entfernen Sie die Standardrichtlinie und fügen Sie die kopierte JSON-Datei an ihrer Stelle ein.

   JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. Wählen Sie Update Trust Policy (Trust Policy aktualisieren).

Weitere Informationen finden Sie unter Ändern einer Rollenvertrauensrichtlinie (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie eine Regel für EventBridge

Gehen Sie wie folgt vor, um in der EventBridge Konsole eine Regel zu erstellen, mit der Sie das Stoppen und Starten von EC2-Instances automatisieren können, deren Außerbetriebnahme geplant ist.

So erstellen Sie eine Regel EventBridge für automatische Aktionen von Systems Manager

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich unter Events (Ereignisse) die Option Rules (Regeln) aus.
3. Geben Sie auf der Seite Regel erstellen einen Namen und eine Beschreibung für Ihre Regel ein.
4. Wählen Sie unter Muster definieren die Option Ereignismuster und dann Pre-defined Muster nach Dienst aus.
5. Wählen Sie für Service provider (Serviceanbieter) die Option AWS aus.
6. Wählen Sie als Dienstname die Option Health aus.
7. Wählen Sie als Ereignistyp die Option Spezifische Gesundheitsereignisse aus.
8. Wählen Sie Bestimmte Dienste und dann EC2 aus.
9. Wählen Sie Kategorie (n) für bestimmte Ereignistypen und dann ScheduledChange aus.

10. Wählen Sie „Code (s) für bestimmte Ereignistypen“ und dann den Code für den Ereignistyp.

    Wählen **`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`** Sie beispielsweise für Amazon EBS-backed EC2-Instances. Wählen Sie für vom Amazon EC2-Instance-Speicher unterstützte Instances. **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**

11. Wählen Sie Irgendeine Ressource.

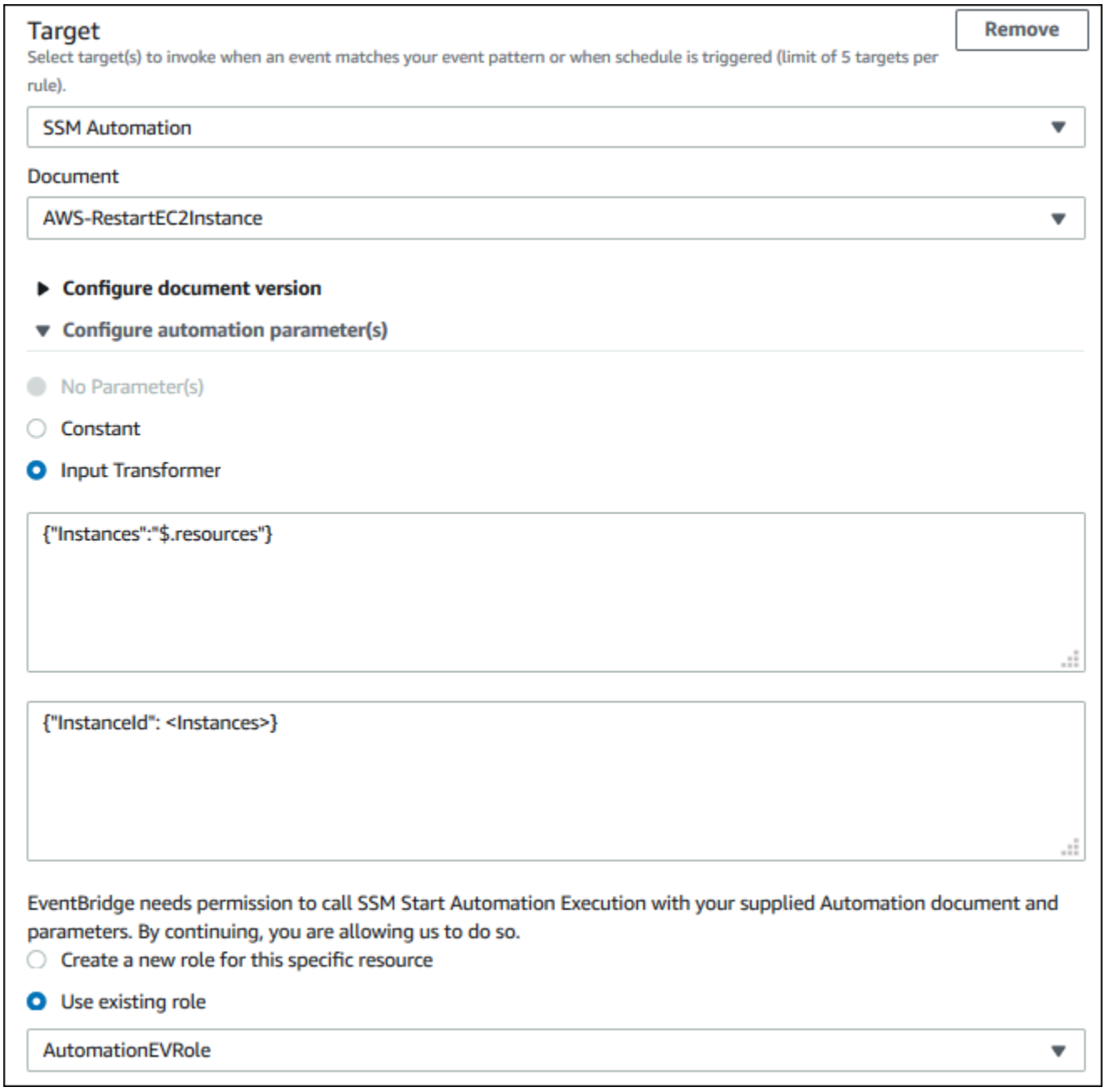
    Ihr Event-Muster wird dem folgenden Beispiel ähneln.

    Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Fügen Sie das Systems Manager Automation-Dokumentziel hinzu. Wählen Sie unter Ziele auswählen für Ziel die Option SSM Automation aus.
13. Wählen Sie `AWS-RestartEC2Instance` für Dokument aus.
14. Erweitern Sie das Feld Automationsparameter (n) konfigurieren und wählen Sie dann Input Transformer aus.
15. Geben Sie für das Feld Eingabepfad Folgendes ein**`{"Instances":"$.resources"}`**.
16. Geben Sie für das zweite Feld ein**`{"InstanceId": <Instances>}`**.
17. Wählen Sie Bestehende Rolle verwenden aus, und wählen Sie dann die IAM-Rolle aus, die Sie erstellt haben, z. B. *`AutomationEVRole`*

Ihr Ziel sollte wie im folgenden Beispiel aussehen.



> **Note**
>
> Wenn Sie noch keine IAM-Rolle mit den erforderlichen EC2- und Systems Manager-Berechtigungen und einer vertrauenswürdigen Beziehung haben, wird Ihre Rolle nicht in der Liste angezeigt. Weitere Informationen finden Sie unter Voraussetzungen.

18. Wählen Sie Erstellen aus.

Wenn in Ihrem Konto ein Ereignis eintritt, das Ihrer Regel entspricht, EventBridge wird das Ereignis an das von Ihnen angegebene Ziel gesendet.

Referenz: AWS Health Veranstaltungen Amazon EventBridge schema

Das Folgende ist das Schema für AWS Health Ereignisse. Der Inhalt des Parameters Details folgt in einer zweiten Tabelle. Beispielnutzlasten werden nach den Schematabellen bereitgestellt.

AWS Health Ereignisschema

AWS Health Ereignisschema

Parameter	Description	Erforderlich
Version	EventBridge Version, derzeit „0".	Ja
id	Die eindeutige Kennung für das EventBridge Ereignis.	Ja
Detailtyp	Die Art des Details. Für AWS Health Ereignisse werden die Werte &AWS Health Event und unterstützt AWS Health	Ja

Parameter	Description	Erforderlich
	`Abuse Event`	
source	Die Event-Bus-Quelle. Für AWS Health Ereignisse ist der unterstützte Wert `aws.health`	Ja

Parameter	Description	Erforderlich
Konto	Die Konto-ID, an die das AWS Health Ereignis gesendet wurde. **Note** Für Unternehmensansichten ist dies ein anderes Konto als das betroffene Konto, wenn es im Verwaltungskonto oder im Konto eines delegierten Administrators	Ja

Parameter	Description	Erforderlich
	eingegang en ist.	
variieren	Die Uhrzeit, an die die Benachric htigung gesendet EventBrid ge wurde. Format:`yyyy-mm-d dThh:mm:s sZ` .	Ja

Parameter	Description	Erforderlich
Region	Das AWS-Region , an das die Benachrichtigung übermittelt wurde. **Note** Dieses Feld gibt nicht die betroffene Region für dieses AWS Health Ereignis an. Diese Information wird unter gemeldet. `detail.entRegi`	Ja

Parameter	Description	Erforderlich
Ressourcen	Beschreibt die Liste der betroffenen Ressourcen, falls vorhanden, in einem Konto. Dieses Feld ist leer, wenn keine Ressourcen referenziert werden.	Nein
Detail	Der Abschnitt mit den Einzelheiten des AWS Health Ereignisses, wie in der Tabelle unmittelbar nach diesem Abschnitt beschrieben.	Ja

Schemainhalt des Parameters „Details“

Die folgende Tabelle dokumentiert den Inhalt des Detailparameters im AWS Health Eventschema.

AWS Health Ereignisschema: Inhalt der Detailparameter

Inhalt des Parameters „Detail“	Description	Erforderlich
EventARN	Die eindeutige Kennung für das AWS Health Ereignis für die bestimmte Region, einschließlich der Region und der Event-ID. **Note** Ein Event-ARN ist nicht eindeutig für eine bestimmte AWS-Konto oder eine bestimmte Region.	Ja
Service nicht zulässig	Die vom AWS Health Ereignis AWS-Service Betroffenen. Zum Beispiel Amazon EC2, Amazon Simple Storage Service, Amazon Redshift oder Amazon Relational Database Service.	Ja
eventTypeCode	Die eindeutige ID für den Ereignistyp. Zum Beispiel `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` und `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED`. Ereignisse, die Folgendes beinhalten, `MAINTENANCE_SCHEDULED` werden in der Regel	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
	etwa zwei Wochen vor der Startzeit veröffentlicht. **Note** Alle neuen geplanten Lebenszyklusereignisse haben den Ereignistyp `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT` .	
eventTypeCategory	Der Kategorie-Code des Ereignisses. Zu den unterstützten Werten gehören `issue` , `accountNotification` , `investigation` , und `scheduledChange` .	Ja
eventScopeCode	Gibt an, ob das AWS Health Ereignis kontospezifisch oder öffentlich ist. Unterstützte Werte sind `ACCOUNT_SPECIFIC` oder `PUBLIC` .	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
Kommunikations-ID	Eine eindeutige Kennung für diese Kommunikation für das AWS Health Ereignis. Nachrichten mit derselben Kommunikations-ID können Backup-Nachrichten oder Seiten eines einzelnen AWS Health Ereignisses sein. Diese Kennung kann zusammen mit der Konto-ID verwendet werden, um die Deduplizierung von Nachrichten zu erleichtern. Bei der Unterstützung der AWS Health Event-Paginierung enthält die Kommunikations-ID die Seitennummer, damit die Kommunikations-ID seitenübergreifend eindeutig bleibt, z. B. 12345678910-1. Weitere Informationen finden Sie unter Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge.	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
startTime	Die Startzeit des Ereignisses im AWS Health Format. `DoW, DD, MMM, YYYY, HH:MM:SS TZ` Die Startzeit für geplante Ereignisse kann in der Zukunft liegen.	Ja
endTime	Die Endzeit der AWS Health Veranstaltung, im Format:`DoW, DD MMM YYYY HH:MM:SS TZ`. Die Endzeit kann nicht für Ereignisse angegeben werden, die für einen zukünftigen Zeitpunkt geplant sind.	Nein
zuletzt UpdatedTime	Die Uhrzeit der letzten Aktualisierung für das AWS Health Ereignis im Format`DoW, DD MMM YYYY HH:MM:SS TZ`.	Ja
statusCode	Der Status des AWS Health Ereignisses. Zu den unterstützten Werten gehören `open`, `closed` und `upcoming`.	Ja
EventRegion	Die von diesem AWS Health Ereignis beschriebene betroffene Region.	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
Beschreibung des Ereignisses	Ein Abschnitt, der das AWS Health Ereignis beschreib t. Dazu gehören Felder für Sprache und Text zur Beschreibung des Ereigniss es. • Sprache — Der Code für die Sprache, die bei der AWS Health Veranstaltung verwendet wurde. Dies wird in der Regel von der Region bestimmt, in der die Veranstaltung veröffentlicht wird. In der `us-east-1` Region ist dies beispiels weise in der Regel der `Fallen_US`. • LatestDescription — Beschreibt das AWS Health Ereignis, wie es von der AWS Health API gerendert wird und normalerweise im AWS Health Dashboard angezeigt wird. **Note** Bei öffentlichen Veranstaltungen enthält dies nur das neueste Update und nicht den	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
	gesamten Verlauf des Ereignisses.	
Event-Metadaten	Zusätzliche Event-Metadaten, die für das AWS Health Er eignis bereitgestellt werden können. • <metadata key 1>— Zeichenfolgen aus Schlüssel-Wert-Paaren aus Metadaten: „keystring1": „keyvalue1" Die Schlüssel-Wert-Paare für Event-Metadaten werden von dem Dienst bestimmt, der das Ereignis gesendet hat. AWS Health	Nein

Inhalt des Parameters „Detail“	Description	Erforderlich
Betroffene Entitäten	Ein Array, das den Ressourcenwert und den Status der betroffenen Ressourcen innerhalb des Ereignisses beschreibt. AWS Health • entityValue — Die resource/entity ID. • lastUpdatedTime — Der Zeitpunkt, zu dem dieser resource/entity Status zuletzt aktualisiert wurde, im Format. `DoW, DD MMM YYYY HH:MM:SS TZ` • status — Der Status des Betroffenen. resource/entity Zu den unterstützten Werten gehören `IMPAIRED` `UNIMPAIRED` `PENDING`,`RESOLVED`, und`UNKNOWN`. **Note** Bei geplanten Lebenszyklusereignissen werden Aktualisierungen des Ressourcenstatus asynchron und regelmäßig durchgeführt. In seltenen Fällen kann es zu Verzögerungen von bis zu 72	Nein

Inhalt des Parameters „Detail“	Description	Erforderlich
	Stunden kommen. Weitere Informationen finden Sie unter Was kann ich erwarten, wenn ich eine Benachrichtigung über ein geplantes Lebenszyklusereignis erhalte?.	
Seite	Die Seite, die diese Nachricht darstellt. Weitere Informationen finden Sie unter Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge. **Note** Die Paginierung erfolgt nur bei Ressourcen. Wenn die Größenbeschränkung von 256 KB aus einem anderen Grund überschritten wird, schlägt die Kommunikation fehl.	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
Gesamtzahl der Seiten	Die Gesamtzahl der Seiten für dieses Gesundheitsereignis. Weitere Informationen finden Sie unter Anzeige von paginierten Listen von AWS Health Ereignisse am EventBridge. Anhand dieses Werts können Sie ermitteln, ob Sie alle Seiten einer mehrseitigen Mitteilung für ein Konto erhalten haben.	Ja
Ereignis sichern	Dieses Flag filtert Backup-Ereignisse in der angegebenen Backup-Region innerhalb einer Partition heraus, wenn Kunden Redundanz nicht nutzen möchten. Dieser Wert kann wahr oder falsch sein.	Ja
Betroffenes Konto	Die Konto-ID des betroffenen Kontos. Dies kann von dem Wert im `account` Feld abweichen, wenn dieses Integritätsereignis an ein Konto gesendet wird, das Teil eines Kontos ist, AWS Organizations und im Verwaltungskonto oder delegierten Administratorkonto empfangen wird.	Ja

Inhalt des Parameters „Detail“	Description	Erforderlich
Umsetzbarkeit	Metadaten zur programmatischen Bestimmung, bei welchen Ereignissen Maßnahmen erforderlich sind, ohne dass eine manuelle Überprüfung erforderlich ist. Möglicher (einzelner) Wert kann `ACTION_REQUIRED ACTION_MAY_BE_REQUIRED` , oder `INFORMATIONAL` sein.	Nein
Personas	Diese Liste von Metadaten aktiviert die programmatische Bestimmung, an welchen Stakeholder die Veranstaltung weitergeleitet werden soll. Mögliche (mehrere) Werte sind `OPERATIONAL SECURITY`, und. `BILLING`	Nein

Veranstaltung im Bereich der öffentlichen Gesundheit — Betriebsproblem bei Amazon EC2

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T09:01:22Z",
    "region": "af-south-1",
    "resources": [],
    "detail": {
```

```
        "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
        "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "statusCode": "open",
        "eventRegion": "af-south-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
        }],
        "affectedEntities": [],
        "page": "1",
        "totalPages": "1",
        "backupEvent": "false",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Ereignis — Problem mit der Elastic Load Balancing API

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-10T06:27:57Z",
    "region": "ap-southeast-2",
    "resources": [],
    "detail": {
```

```
        "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
        "service": "ELASTICLOADBALANCING",
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "ap-southeast-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "page": "1",
        "totalPages": "1",
        "backupEvent": "false",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Ereignis — Das Backup-Ereignis für das Amazon EC2 Instance Store-Laufwerk hat sich verschlechtert

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
```

```
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "backupEvent": "true",
        "affectedAccount": "123456789012",
        "personas": ["OPERATIONS"]
    }
}
```

Account-specific AWS Health Ereignis — Außerbetriebnahme der Amazon EC2-Instance

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2026-01-27T01:43:21Z",
    "region": "us-east-1",
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED_90353408594353983",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED",
        "eventTypeCategory": "scheduledChange",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "1234abc01232a4012345678-1",
        "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
```

```
        "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "eventMetadata": {
            "keystring1": "valuestring1",
            "keystring2": "valuestring2",
            "keystring3": "valuestring3",
            "keystring4": "valuestring4",
            "truncated": "true"
        },
        "affectedEntities": [{
            "entityValue": "arn:aws:ec2:us-east-1:123456789012:instance/
i-1234567890abcdef0",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
            "status": "PENDING"
        }],
        "affectedAccount": "123456789012",
        "page": "1",
        "totalPages": "1",
        "backupEvent": "false",
        "personas": ["OPERATIONS"],
        "actionability": "ACTION_REQUIRED"
    }
}
```

Account-specific AWS Health Ereignis — Lambda Planned Lifecycle-Ereignis

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T01:43:21Z",
    "region": "us-west-2",
    "resources": ["arn:lambda-1-101002929", "arn:lambda-1-101002930",
 "arn:lambda-1-101002931", "arn:lambda-1-101002932"],
```

```
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT_90353408594353980",
        "service": "LAMBDA",
        "eventTypeCode": "AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT",
        "eventTypeCategory": "scheduledChange",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "1234abc01232a4012345678-1",
        "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
        "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "eventMetadata": {
            "keystring1": "valuestring1",
            "keystring2": "valuestring2",
            "keystring3": "valuestring3",
            "keystring4": "valuestring4",
            "truncated": "true"
        },
        "affectedEntities": [{
            "entityValue": "arn:lambda-1-101002929",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002930",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:05:12 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002931",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:07:13 GMT",
            "status": "PENDING"
        }, {
            "entityValue": "arn:lambda-1-101002932",
            "lastUpdatedTime": "Thu, 26 Jan 2026 19:10:59 GMT",
            "status": "RESOLVED"
        }],
        "affectedAccount": "123456789012",
        "page": "1",
        "totalPages": "10",
        "backupEvent": "false",
```

```
        "personas": ["OPERATIONS"],
        "actionability": "ACTION_REQUIRED"
    }
}
```

Überwachen AWS Health

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Health anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AWS Health, melden, wenn etwas nicht stimmt, und gegebenenfalls Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

  Sie können Amazon verwenden, EventBridge um über AWS Health Ereignisse informiert zu werden, die sich auf Ihre Dienste und Ressourcen auswirken könnten. Wenn Sie beispielsweise ein Ereignis über Ihre Amazon EC2-Instances AWS Health veröffentlichen, können Sie diese Benachrichtigungen verwenden, um Maßnahmen zu ergreifen und Ihre Ressourcen nach Bedarf zu aktualisieren oder zu ersetzen. Weitere Informationen finden Sie unter Überwachung von Ereignissen in AWS Health mit Amazon EventBridge.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt werden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket. Sie können identifizieren, welche Benutzer und Konten aufgerufen wurden AWS, die Quell-IP-Adresse, von der aus die Aufrufe getätigt wurden, und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

- Protokollierung AWS Health API-Aufrufe mit AWS CloudTrail

Protokollierung AWS Health API-Aufrufe mit AWS CloudTrail

AWS Health ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt AWS Health. CloudTrail erfasst API-Aufrufe AWS Health als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Health Konsole und Codeaufrufen an die AWS Health API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an

einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für AWS Health. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der gesammelten Informationen können Sie ermitteln CloudTrail, an welche Anfrage gestellt wurde AWS Health, von welcher IP-Adresse die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Details.

Weitere Informationen CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS Health Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine unterstützte Eventaktivität in stattfindet AWS Health, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Eventverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Eventverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Health, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Health API-Operationen werden von der AWS Health API-Referenz protokolliert CloudTrail und sind darin dokumentiert. Beispielsweise generieren Aufrufe der `DescribeAffectedEntities` Operationen`DescribeEvents`,`DescribeEventDetails`, und Einträge in den CloudTrail Protokolldateien.

AWS Health unterstützt das Protokollieren der folgenden Aktionen als Ereignisse in CloudTrail Protokolldateien:

- Ob die Anfrage mit Root- oder IAM-Anmeldeinformationen gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Sie können Ihre Protokolldateien so lange in Ihrem Amazon S3-Bucket speichern, wie Sie möchten. Außerdem können Sie Amazon-S3-Lebenszyklusregeln definieren, um Protokolldateien automatisch zu archivieren oder zu löschen. Standardmäßig werden die Protokolldateien mit serverseitiger Amazon-S3-Verschlüsselung (SSE) verschlüsselt.

Um bei der Übermittlung der Protokolldatei benachrichtigt zu werden, können Sie so konfigurieren, CloudTrail dass Amazon SNS-Benachrichtigungen veröffentlicht werden, wenn neue Protokolldateien zugestellt werden. Weitere Informationen finden Sie unter Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail.

Sie können auch AWS Health Protokolldateien aus mehreren AWS Regionen und mehreren AWS Konten in einem einzigen Amazon S3-Bucket zusammenfassen.

Weitere Informationen finden Sie unter Empfangen von CloudTrail -Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail -Protokolldateien aus mehreren Konten.

Beispiel: AWS Health Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Logeintrag, der den DescribeEntityAggregates Vorgang demonstriert.

```
{
```

```
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Dokumenthistorie für AWS Health

In der folgenden Tabelle wird die Dokumentation für diese Version von beschrieben AWS Health.

- API-Version: 2016-08-04

In der folgenden Tabelle werden wichtige Aktualisierungen der AWS Health Dokumentation beschrieben, die am 28. August 2020 beginnen. Sie können den RSS-Feed abonnieren, um Benachrichtigungen über Aktualisierungen zu erhalten.

Änderung	Beschreibung	Datum
Es wurde klargestellt, dass öffentliche Veranstaltungen nicht verfügbar sind unter AWS-Benutzerbenachrichtigungen	Hinweisschilder hinzugefügt, um klarzustellen, dass öffentliche Veranstaltungen nicht über AWS verwaltete Benachrichtigungen in AWS-Benutzerbenachrichtigungen verfügbar sind. Um öffentliche Veranstaltungen zu erhalten, müssen Sie eine EventBridge Amazon-Regel oder eine User-configured Benachrichtigung (UCN) erstellen. Weitere Informationen finden Sie unter Öffentliche Veranstaltung.	26. August 2026
Es wurde ein Hinweis zum Zeitpunkt der Aktualisierung des Ressourcenstatus für geplante Lebenszyklusereignisse hinzugefügt	Es wurde ein Hinweis hinzugefügt, um klarzustellen, dass Aktualisierungen des Ressourcenstatus für geplante Lebenszyklusereignisse asynchron durchgeführt werden und in seltenen Fällen eine Verzögerung von bis zu	26. August 2026

	72 Stunden auftreten können. Weitere Informationen finden Sie unter Referenz: EventBridge Amazon-Schema für AWS Health Ereignisse.	
Klarer Geltungsbereich der Region für eine vereinfachte Integration	Der Abschnitt zur vereinfachten Integration wurde aktualisiert, um klarzustellen, dass eine Regel für eine einzelne Region nur kontospezifische Ereignisse, keine öffentlichen Ereignisse, aggregiert. Öffentliche Ereignisse werden nur an die betroffene Region und ihre Backup-Region übertragen. Weitere Informationen finden Sie unter Vereinfachte Integration.	2. Juli 2026
Hinweis zum Ende des Supports für AWS Service Management Connector hinzugefügt	Dem Abschnitt zur Service Management Connector-Integration wurde ein Hinweis zum Ende des Supports hinzugefügt. AWS wird den Support für den AWS Service Management Connector am 31. März 2027 beenden. Weitere Informationen finden Sie unter Ende des Supports für AWS Service Management Connector.	28. April 2026

Aktualisiert Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health	Das Verfahren zum Erstellen von EventBridge Regeln wurde vereinfacht, indem auf das EventBridge Amazon-Benutzerhandbuch verwiesen wurde, in dem allgemeine Schritte zur Regelerstellung beschrieben sind. Das Thema konzentriert sich jetzt auf AWS Health spezifische Filter- und Anwendungsfälle. Weitere Informationen finden Sie unter Konfiguration einer EventBridge Regel zum Senden von Benachrichtigungen über Ereignisse in AWS Health.	13. März 2026
Beispiele für das AWS HealthAmazon EventBridge Event-Schema wurden aktualisiert	Die Schemabeispiele wurden um Personas und Actionability-Felder erweitert. Beispiele hierfür sind ein Public Health Event für ein Betriebsproblem bei Amazon EC2, Account-specific Ereignisse für ein Problem mit der Elastic Load Balancing API und das Backup-Ereignis Amazon EC2 Instance Store Drive Performance Degraded sowie das Lambda Planned Lifecycle Event. Weitere Informationen finden Sie unter Referenz: Event-Schema. AWS HealthAmazon EventBridge	13. März 2026

AWS Health Benachrichtigungen verwalten in aktualisiert AWS-Benutzerbenachrichtigungen	Die Informationen in diesem Abschnitt wurden aktualisiert, um die Migration von AWS Health Ereignissen zu widerzuspiegeln AWS-Benutzerbenachrichtigungen. Weitere Informationen finden Sie unter AWS Health Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.	22. Dezember 2025
Aktualisierte kontospezifische und öffentliche Monitoring-Ereignisse für AWS Health	Diesem Abschnitt wurden Informationen hinzugefügt, die das Verhalten von Backup-Regeln für öffentliche und kontospezifische Ereignisse detailliert beschreiben. Weitere Informationen finden Sie unter Backup-Regeln für Ereignisse. AWS Health	11. Dezember 2025
Es wurden Informationen zu den Feldern Actionability und Personas für Gesundheitsereignisse hinzugefügt	Es wurden Informationen zu den Feldern Actionability und Personas im AWS Health Abschnitt Konzepte für und zum Schemainhalt des Parameters „Details“ im Abschnitt Reference: AWS Health events schema hinzugefügt. Amazon EventBridge Weitere Informationen finden Sie unter Konzepte für AWS Health und Referenz: AWS HealthAmazon EventBridge Event-Schema.	20. November 2025

Aktualisierter Abschnitt: Erstellen von EventBridge Regeln für die AWS-Region Berichterstattung	Die Informationen zur Erstellung von EventBridge Regeln wurden aktualisiert. Weitere Informationen finden Sie unter EventBridge Regeln für den AWS-Region Versicherungsschutz erstellen.	3. November 2025
Aktualisierter Abschnitt: AWS Health Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen	Die Informationen zu den Schritten zur Konfiguration Ihres Abonnements für AWS verwaltete Benachrichtigungen für AWS Health Ereignisse wurden aktualisiert. Weitere Informationen finden Sie unter AWS Health Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.	16. September 2025
Aktualisierter Abschnitt: Überwachung von Ereignissen AWS Health bei Amazon EventBridge	Aktualisierte Informationen im Hinweis zum AWS Health Versand von Ereignissen an EventBridge. Weitere Informationen finden Sie unter Ereignisse AWS Health bei Amazon überwachen EventBridge.	15. September 2025

Aktualisierter Abschnitt: AWS Health Dashboard	Optionale Schritte zum Abonnieren von RSS-Feeds für Gesundheitsereignisse wurden entfernt. Hinweis hinzugefügt, den Kunden nutzen können, um Benachrichtigungen über Gesundheitsereignisse zu erhalten EventBridge. Weitere Informationen finden Sie unter AWS Health Dashboard.	15. August 2025
Aktualisierter Abschnitt: Überwachung von Ereignissen AWS Health bei Amazon EventBridge	Das Thema Installation einer serviceverknüpften Rolle zur Verwendung von AWS Incident Detection and Response bei der Überwachung von Ereignissen AWS Health bei Amazon wurde entfernt EventBridge	8. August 2025
Aktualisierter Abschnitt: Überwachung von Ereignissen AWS Health bei Amazon EventBridge	Dem Abschnitt „Hinweise“ wurden Informationen hinzugefügt, die darauf hinweisen, dass es zu einer Verzögerung von bis zu einer Stunde kommen kann, bevor Sie Benachrichtigungen über Ereignisse im Bereich der öffentlichen Gesundheit erhalten. Weitere Informationen finden Sie unter Ereignisse AWS Health bei Amazon überwachen EventBridge	22. Juli 2025

Aktualisierter Abschnitt: Aktivierung der Organisationsansicht	Dem Abschnitt „Hinweise“ wurden Informationen hinzugefügt, die darauf hinweisen, dass alle historischen Gesundheitsereignisse in Ihrer Organisation AWS Health automatisch zusammengefasst werden, wenn Sie die Organisationsansicht aktivieren. Es kann bis zu 24 Stunden dauern, bis historische Ereignisse in Ihrer Unternehmensansicht angezeigt werden. Weitere Informationen finden Sie unter Organisationsansicht aktivieren	27. Juni 2025
Aktualisierter Abschnitt: Zusammenfassen von AWS Health Ereignissen für mehrere Konten	Der Hinweis, dass Ereignisse, die vor der Aktivierung der Organisationsansicht eingetreten sind, AWS Health nicht angezeigt werden, wurde entfernt. Weitere Informationen finden Sie unter AWS Health Ereignisse kontenübergreifend zusammenfassen	27. Juni 2025
WorkDocs veraltet	Die Verweise auf veraltet WorkDocs in Geplante Lebenszyklusereignisse für wurden entfernt. AWS Health	19. Juni 2025

Hinweis zum Zeitplan für die Migration AWS verwalteter Benachrichtigungen hinzugefügt	Ein Hinweis zu den wichtigsten Terminen für die E-Mail-Migration zu AWS verwalteten Benachrichtigungen wurde in hinzugefügt AWS-Benutzerbenachrichtigungen. Weitere Informationen finden Sie unter AWS Health Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.	28. April 2025
Die geplanten Lebenszyklusereignisse wurden aktualisiert	Geplante Lebenszyklusereignisse wurden aktualisiert und geben nun an, dass AWS Health Ereignisse 4 Jahre statt 90 Tage bei ungelösten Ressourcen gültig bleiben. Weitere Informationen findest du unter Was kann ich erwarten, wenn ich eine Benachrichtigung über ein geplantes Lebenszyklusereignis erhalte? Abschnitt unter Geplante Lebenszyklusereignisse für AWS Health.	18. April 2025

Die Beschreibung der Liste der betroffenen Ressourcen für geplante Lebenszyklusereignisse wurde aktualisiert	Die Liste der betroffenen Ressourcen für geplante Lebenszyklusereignisse wird in der Regel alle 24 Stunden aktualisiert. Es kann jedoch bis zu 72 Stunden dauern, bis der aktuelle Ressourcenstatus angezeigt wird. Weitere Informationen finden Sie im Abschnitt Veranstaltungsdetails unter Kontoereignisse im AWS Health Dashboard https://docs.aws.amazon.com/health/latest/ug/aws-health-account-views.html anzeigen.	7. April 2025
Eine häufig gestellte Frage zur Verwaltung von AWS Health Benachrichtigungen wurde hinzugefügt AWS-Benutzerbenachrichtigungen	Weitere Informationen finden Sie unter Benachrichtigungen verwalten in den AWS-Benutzerbenachrichtigungen häufig gestellten Fragen.	18. Februar 2025
Es wurden Informationen zu IPv6-only Anfragen an Endpunkte hinzugefügt.	Weitere Informationen finden Sie unter Endpunkte für AWS Health API-Anfragen https://docs.aws.amazon.com/health/latest/ug/health-api.html#endpoints auswählen.	28. Januar 2025
AWS Health Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen	Weitere Informationen finden Sie unter Benachrichtigungen verwalten in AWS-Benutzerbenachrichtigungen.	16. Januar 2025

JSON-Fehler bei der Überwachung von AWS Health Ereignissen mit Amazon wurde korrigiert EventBridge	Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen EventBridge.	3. September 2024
Aktualisierte Informationen zum Herunterladen der betroffenen Ressourcen	Weitere Informationen finden Sie unter Ansicht „Betroffene Ressourcen“.	27. Juli 2024
Der Datenschutz im Netzwerkverkehr wurde aus der Dokumentation des Sicherheitsabschnitts AWS Health entfernt	Weitere Informationen finden Sie unter Sicherheit in AWS Health.	27. März 2024
Das AWS Health Dashboard — Service Health und Geplante Lifecycle-Ereignisse wurden zur AWS Health Dokumentation aktualisiert.	Weitere Informationen finden Sie unter AWS Health Dashboard — Servicestatus und Geplante Lebenszyklusereignisse für AWS Health.	15. Februar 2024
Beim Erstellen einer EventBridge Regel für wurde ein doppelter Aufzählungspunkt entfernt AWS Health	Unter EventBridge Regel erstellen für wurde ein doppelter Aufzählungspunkt entfernt AWS Health.	4. Dezember 2023
Dokumentation für geplante Lifecycle-Ereignisse hinzugefügt	Weitere Informationen finden Sie unter Geplante Lebenszyklusereignisse für AWS Health.	31. Oktober 2023

Aktualisierte Dokumentation für `AWSHealthFullAccess`	Sie können die `AWSHealthFullAccess` verwaltete Richtlinie jetzt in der verwenden AWS GovCloud (US) Regions. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für AWS Health.	16. Oktober 2023
Dokumentation zur Konfiguration von AWS Benutzerbenachrichtigungen in hinzugefügt AWS Health.	Sie können jetzt AWS Benutzerbenachrichtigungen in konfigurieren AWS Health. Weitere Informationen finden Sie unter AWS Benutzerbenachrichtigungen konfigurieren für AWS Health.	30. August 2023
Dem Abschnitt „ AWS Health Ereignisse zusammenfassen“ wurde eine Dokumentation für die Funktion für delegierte Administratoren hinzugefügt.	Weitere Informationen finden Sie unter Organisationsansicht für delegierte Administratoren.	27. Juli 2023
Aktualisierung der SLR-Richtlinie	Aktualisierung der AWS verwalteten Richtlinie: Health_OrganizationsServiceRolePolicy. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Health.	19. Juli 2023

AWS Health Das Schema unterstützt jetzt Event-Metadaten	Sie können jetzt Event-Metadaten von AWS Health Ereignissen empfangen. Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon EventBridge überwachen.	20. Juni 2023
Die Dokumentation für Amazon EventBridge wurde aktualisiert	Sie können jetzt eine EventBridge Amazon-Regel verwenden, um sowohl kontospezifische als auch öffentliche Ereignisse zu überwachen. Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon EventBridge überwachen.	2. Mai 2023
Dokumentation für AWS verwaltete Richtlinien hinzugefügt	Dokumentation für die AWS verwalteten Richtlinien für AWS Health und Verwenden von dienstverknüpften Rollen für AWS Health hinzugefügt.	18. Januar 2023
Dokumentation zur Einstellung der Zeitzone hinzugefügt	Verwenden Sie die neue Zeitzonenfunktion, um das AWS Health Dashboard in Ihrer lokalen Zeitzone oder in UTC anzuzeigen. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard — Ihr Kontostatus und AWS Health Dashboard — Servicestatus.	21. September 2022

Aktualisierte Dokumentation	Dokumentation für AWS Health Aware hinzugefügt. Weitere Informationen finden Sie unter AWS Health Aware.	25. Mai 2022
Aktualisierte Dokumentation	Das Service Health Dashboard und das AWS Personal Health Dashboard wurden in das AWS Health Dashboard umbenannt. Weitere Informationen finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard — Ihr Kontostatus und AWS Health Dashboard — Servicestatus.	28. Februar 2022
Die Dokumentation für Amazon wurde aktualisiert EventBridge	Neues Thema AWS Health zur Verwendung von Amazon EventBridge zur Überwachung von Gesundheitsereignissen. Weitere Informationen finden Sie unter Überwachung von AWS Health Ereignissen mit Amazon EventBridge.	3. Februar 2022
Aktualisierte Dokumentation	Wenn Sie einen Enterprise On-Ramp Support-Plan haben, können Sie die AWS Health API verwenden.	24. November 2021
Dokumentation hinzugefügt	Neues Thema für AWS Health Konzepte. Weitere Informationen finden Sie unter Konzepte für AWS Health.	29. Juli 2021

Die Dokumentation für CloudWatch Veranstaltungen wurde aktualisiert	Es wurde ein Abschnitt hinzugefügt, in dem erklärt wird, wie eine Regel für mehrere Dienste und Ereignistypkategorien erstellt wird. Weitere Informationen finden Sie unter Eine Regel für mehrere Dienste und Kategorien erstellen.	7. Mai 2021
Die Dokumentation für CloudWatch Veranstaltungen wurde aktualisiert	Der Abschnitt wurde aktualisiert, um AWS Systems Manager Aktionen für Amazon CloudWatch Events-Regeln zu automatisieren. Weitere Informationen finden Sie unter Automatisieren von Aktionen für Amazon EC2-Instances.	28. April 2021
Die Dokumentation für Ereignisse wurde aktualisiert CloudWatch	Es wurde ein Abschnitt zum Empfangen von AWS Health Ereignissen in Ihrem Chat-Client hinzugefügt. Weitere Informationen finden Sie unter Empfangen von AWS Health Ereignissen mit Amazon Q Developer in Chat-Anwendungen.	16. März 2021

Aktualisierte Dokumentation	Die folgenden Themen werden aktualisiert: • Das Thema Zusammenfassen von AWS Health Ereignissen wurde aktualisiert • Das Thema „Monitor für AWS Health Ereignisse mit Amazon CloudWatch Events“ wurde neu organisiert und aktualisiert • Der Abschnitt zu ressourcen- und aktionsbasierten Bedingungen wurde aktualisiert	29. Januar 2021
Das AWS Health Dashboard für die Unternehmensansicht wurde in der AWS Health Konsole hinzugefügt	Sie können die AWS Health Konsole verwenden, um die Funktion „Organisationsansicht“ zu aktivieren. Anschließend können Sie Gesundheitsereignisse für Mitglieds konten in Ihrer AWS Organisation anzeigen.	14. Dezember 2020
Endpunkt mit hoher Verfügbarkeit: Demo	Sie können den Beispielcode verwenden, um den aktiven regionalen Endpunkt und die AWS Signaturregion für zu ermitteln AWS Health.	22. Oktober 2020

Aktualisierungen des AWS Health Benutzerhandbuchs	Das Unternehmen aktualisiert es und hat einen RSS-Feed hinzugefügt, sodass Sie die neuesten Aktualisierungen der AWS Health Dokumentation abonnieren können.	28. August 2020

Frühere Aktualisierungen

Änderungen	Beschreibung	Date
Das Thema der Organisat ionsansicht wurde aktualisiert, damit Beispiele enthalten sind.	Siehe Aggregieren AWS Health Ereignisse über Konten hinweg.	3. Juni 2020
Sicherheit und AWS Health	Es wurden Informationen zu Sicherheitsüberlegungen bei der Verwendung von AWS Health hinzugefügt. Siehe Sicherheit bei AWS Health.	5. Mai 2020
Es wurde ein neuer Abschnitt hinzugefügt, um zu erklären, wie die Organisationsansic ht für Ereignisse verwendet wird, die über alle Konten in AWS Organizations aggregier t wurden.	Siehe Aggregieren AWS Health Ereignisse über Konten hinweg.	18. Dezember 2019
Es wurde ein neuer Abschnitt „Ressourcen und Action-ba sed Bedingungen“ hinzugefü gt, in dem die von der AWS Health API ausgelösten Einschränkungen für Ereigniss e erläutert werden.	Siehe Identitäts- und Zugriffsm anagement für AWS Health.	2. August 2018

Änderungen	Beschreibung	Date
Es wurde ein Hinweis zur Sichtbarkeit von AWS Health Informationen hinzugefügt.	Siehe Identitäts- und Zugriffsmanagement für AWS Health.	16. August 2017
Service-Veröffentlichung.	AWS Health veröffentlicht.	1. Dezember 2016

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.