aws

User Guide

AWS Health

AWS Health: User Guide

Table of Contents

Was ist AWS Health?

AWS Healthbietet 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 Healthstellt relevante und aktuelle Informationen bereit, die Sie bei der Verwaltung laufender Ereignisse unterstützen. AWS Healthhilft Ihnen auch dabei, sich über geplante Aktivitäten im Klaren zu sein und sich darauf vorzubereiten. Der Service liefert Warnungen und Benachrichtigungen, die durch Statusänderungen von AWS-Ressourcen ausgelöst werden, sodass Sie nahezu in Echtzeit über die Ereignisse informiert werden, und unterstützt Sie mit Anleitungen bei der Behebung von Problemen.

Alle Kunden können das AWS HealthDashboard 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 HealthDashboard-Detailseite auf der

Informationen zu den Grundlagen AWS Health und zur Nutzung des Dienstes finden Sie unterVerwenden Sie AWS Health zum ersten Mal?.

Eine Liste der Begriffe, die Ihnen bei der Nutzung angezeigt werdenAWS Health, finden Sie unterKonzepte 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 Business-, Enterprise On-Ramp- oder Enterprise Support-Plan haben, können Sie die AWS Health API für die Integration mit internen Systemen und Systemen von Drittanbietern verwenden. Weitere Informationen finden Sie in der AWS Health-API-Referenz.
- Weitere Informationen zu verfügbaren AWS Support Plänen finden Sie unter AWS Support.

Verwenden Sie AWS Health zum ersten Mal?

Wenn Sie AWS Health zum ersten Mal verwenden, sollten Sie zunächst die folgenden Abschnitte lesen:

- Was ist AWS Health?— In diesem Abschnitt werden das zugrunde liegende Datenmodell, die unterstützten Operationen und die AWS SDKs beschrieben, die Sie für die Interaktion mit dem Service verwenden können.
- Konzepte für AWS Health— Lernen Sie die Grundlagen AWS Health und Begriffe kennen, denen Sie bei der Nutzung des Dienstes begegnen werden.
- Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus— Erfahren Sie, wie Sie Ereignisse und betroffene Entitäten anzeigen und erweiterte Filterung durchführen. Dieses Dashboard enthält Ereignisse, die für Ihr Konto und Ihre Organisation spezifisch sind.
- AWS Health Dashboard – Servicezustand— Falls Sie noch keine habenAWS-Konto, können Sie sich Informationen über den Status und den Status der AWS-Services einzelnen AWS-Region Elemente anzeigen lassen.
- AWS Health Ereignisse mit Amazon überwachen EventBridge— Sie können Amazon verwenden EventBridge , um Push-Benachrichtigungen von AWS Health zu erhalten.
- Zugreifen auf die AWS Health-API— Der AWS Health API-Abschnitt beschreibt die Operationen, mit denen Informationen über Ereignisse und Entitäten abgerufen werden.

AWS Healthstellt 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.

Sie können eine EventBridge Regel einrichten, um AWS Health Ereignisse bei Amazon zu empfangen EventBridge. Auf diese Weise können Sie mithilfe von Push-Benachrichtigungen das AWS Health Ereignismanagement automatisieren, indem Sie EventBridge Amazon-Regeln erstellen, um Maßnahmen zu ergreifen.

Wenn Sie einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan haben, können Sie programmgesteuert auf die im Dashboard angezeigten Informationen zugreifen. Sie können das AWS Command Line Interface (AWS CLI) verwenden oder Code schreiben, um Anfragen zu stellen, indem Sie entweder direkt die REST-API oder die SDKs verwenden. AWS

Weitere Informationen zur Verwendung von AWS Health Veranstaltungen bei Amazon finden Sie EventBridge unterAWS Health Ereignisse mit Amazon überwachen EventBridge. Weitere Informationen zur Verwendung von AWS Health mit der AWS CLI finden Sie in der AWS CLI-Referenz für AWS Health. Anweisungen zur Installation der AWS CLI finden Sie unter Installieren der AWS Command Line Interface.

Konzepte für AWS Health

Erfahren Sie mehr über AWS Health Konzepte und erfahren Sie, wie Sie den Service verwenden können, um die Integrität Ihrer Anwendungen, Dienste und Ressourcen in Ihrem zu gewährleistenAWS-Konto.

Themen

AWS Health event

AWS HealthEreignisse, auch Gesundheitsereignisse genannt, sind Benachrichtigungen, die im Namen anderer AWS Dienste AWS Health gesendet werden. Sie können diese Ereignisse nutzen, um sich über bevorstehende oder geplante Änderungen zu informieren, die sich auf Ihr Konto auswirken könnten. Sie AWS Health können beispielsweise ein Ereignis senden, wenn AWS Identity and Access Management (IAM) plant, eine verwaltete Richtlinie oder AWS Config eine verwaltete Regel abzulehnen. AWS Healthsendet auch Ereignisse, wenn es Probleme mit der Dienstverfügbarkeit in einem gibt. AWS-Region Sie können sich die Beschreibung des Ereignisses ansehen, um das Problem zu verstehen, die betroffenen Ressourcen zu identifizieren und die empfohlenen Maßnahmen zu ergreifen.

Es gibt zwei Arten von Gesundheitsereignissen:

Inhalt

Kontospezifisches Ereignis

Kontospezifische Ereignisse finden entweder bei Ihnen AWS-Konto oder bei einem Konto in Ihrer Organisation lokal statt. AWS Wenn es beispielsweise ein Problem mit einem Amazon Elastic Compute Cloud (Amazon EC2) Instance-Typ in einer Region gibt, die Sie verwenden, AWS Health bietet Informationen über das Ereignis und den Namen der betroffenen Ressourcen.

Sie können kontospezifische Ereignisse in Ihrem AWS HealthDashboard oder der AWS HealthAPI finden oder Amazon CloudWatch Events verwenden, um Benachrichtigungen zu erhalten.

Öffentliche Veranstaltung

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

Öffentliche Ereignisse findest du in deinem AWS Health Dashboard und im AWS Health Dashboard — Dienststatus.

Wenn Sie ein Konto haben, finden Sie weitere Informationen unterErste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus.

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

AWS Health-Dashboard

Wenn Sie ein Konto habenAWS-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 allgemeine Aufmerksamkeit wecken, z. B. ein bevorstehendes Wartungsproblem für einen Service in einer Region. Sie können das AWS Health Dashboard auch verwenden, um sich über Ereignisse zu informieren, die Sie direkt betreffen könnten, z. B. über eine veraltete Ressource in Ihrem Konto.

Sie können sich unter https://health.aws.amazon.com/health/home bei dem anmeldenAWS Management Console, um Ihr AWS Health Dashboard aufzurufen.

Weitere Informationen finden Sie unter Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus.

AWS HealthDashboard — Zustand des Dienstes

Wenn Sie noch kein Konto haben, können Sie das AWS Health Dashboard — Service Health unter https://health.aws.amazon.com/health/status verwenden, um sich öffentliche Veranstaltungen anzusehen. Bei öffentlichen Veranstaltungen handelt es sich um gemeldete ServiceproblemeAWS, die Aufschluss über die Verfügbarkeit von Diensten geben. Auf dieser Website werden nur öffentliche Ereignisse 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 – Servicezustand.

Code für den Veranstaltungstyp

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

Kategorien für Ereignistypen

Allen Gesundheitsereignissen ist eine Ereignistypkategorie zugeordnet. Bei einigen Ereignissen kann die Kategorie Ereignistyp im Ereignistypcode vorkommen, z. B. im `AWS_RDS_MAINTENANCE_SCHEDULED` Code. In diesem Beispiel ist die Kategorie geplant. Sie können diese Informationen verwenden, um sich ein umfassendes Bild von den Veranstaltungskategorien zu machen.

Wir empfehlen Ihnen, alle Kategorien von Ereignistypen zu überwachen. Beachten Sie, dass jede Kategorie für unterschiedliche Ereignistypen angezeigt wird. Sie können auch die DescribeEventTypesAPI-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 sie erfordern möglicherweise dringendes

Handeln von Ihnen. Wir empfehlen Ihnen, auf solche Ereignisse 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 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 Leistungseinbußen führen, oder lokale Probleme auf Ressourcenebene, auf die Sie aufmerksam machen sollten.

Im Folgenden finden Sie Beispiele für Ereignistypcodes für Probleme:

- `AWS_EC2_OPERATIONAL_ISSUE`— Ein Betriebsproblem bei einem Dienst, z. B. Verzögerungen bei der Nutzung eines Dienstes.
- `AWS_EC2_API_ISSUE`— Ein Betriebsproblem bei 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 Veranstaltungen informieren über bevorstehende Änderungen an Ihren Diensten und Ressourcen. Zu diesen Ereignissen gehören geplante Lebenszyklusereignisse wie end-of-support Benachrichtigungen und automatische Upgrades für verschiedene Versionen. Bei einigen Ereignissen wird möglicherweise empfohlen, Maßnahmen zu ergreifen, um Serviceunterbrechungen zu vermeiden, 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_SYSTEM_REBOOT_MAINTENANCE_SCHEDULED`— Eine Amazon EC2 EC2-Instance erfordert einen Neustart.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker erfordert ein Wartungsereignis, z. B. die Behebung eines Serviceproblems.
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS plant ein geplantes Lebenszyklusereignis, z. B. ein end-of-support Ereignis für eine seiner Versionen, für das Kundenmaßnahmen erforderlich sind.

> **Tip**
>
> Wenn Sie die AWS Health API oder die 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 Veranstaltungsstatus gibt an, ob das Gesundheitsereignis geöffnet, geschlossen oder bevorsteht. Sie können Gesundheitsereignisse bis zu 90 Tage lang im AWS Health Dashboard oder in der AWS Health API anzeigen.

Betroffene Entitäten

Betroffene Entitäten sind AWS Ressourcen, die von dem Ereignis betroffen sein könnten. Wenn Sie beispielsweise ein geplantes Ereignis für die Wartung von Amazon EC2 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 beheben, z. B. beim Erstellen oder Verfall von Ressourcen.

AWS HealthEreignisse 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. Dies können allgemeine Aktionen sein, z. B. das Senden aller geplanten Lebenszyklus-Ereignisnachrichten an

eine Chat-Oberfläche. Es kann sich aber auch um spezifische Aktionen handeln, z. B. das Auslösen eines Workflows in einem IT-Servicemanagement-Tool.

Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen EventBridge.

AWS Health-API

Sie können die AWS Health API verwenden, um programmgesteuert auf die Informationen zuzugreifen, die im AWS HealthDashboard 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 zur Organisationsansicht für Ihre AWS Organisation
- Filtern Sie Ihre Veranstaltungen nach bestimmten Diensten, Ereignistypkategorien und Ereignistypcodes

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

> **Note**
>
> Sie müssen über einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan von verfügen, AWS Supportum die AWS Health API verwenden zu können. Wenn Sie die AWS Health API von einem Konto aus aufrufen, das keinen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan hat, erhalten Sie eine `SubscriptionRequiredException` Fehlermeldung.

Organisationsansicht

Sie können diese Funktion verwenden, um alle Gesundheitsereignisse für AWS Konten in Ihrem Konto AWS Organizations in einer einzigen Ansicht im AWS Health Dashboard zusammenzufassen. 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 API aktivieren. Weitere Informationen finden Sie unter Aggregieren von AWS Health-Ereignissen über Konten mit Organisationsansicht.

AWS Health Dashboard – Servicezustand

Sie können das AWS Health Dashboard – Servicezustand verwenden, um den Zustand aller anzuzeigen AWS-Services. Auf dieser Seite werden gemeldete Serviceereignisse für Services in allen angezeigt AWS-Regionen. Sie müssen sich nicht anmelden oder über einen verfügen AWS-Konto , um auf die Seite AWS Health Dashboard – Servicezustand zuzugreifen.

> **Tip**
>
> Diese Website zeigt nur öffentliche Ereignisse an, die nicht spezifisch für ein sind AWS-Konto. Wenn Sie bereits über ein -Konto verfügen, empfehlen wir Ihnen, sich anzumelden, um Ihr - AWS Health Dashboard anzuzeigen und über Ereignisse zu informieren, die sich auf Ihr Konto und Ihre Services auswirken können. Weitere Informationen finden Sie unter Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus.

So zeigen Sie das AWS Health Dashboard – Servicezustand an

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

   > **Note**
   >
   > Wenn Sie bereits bei Ihrem angemeldet sind AWS-Konto, werden Sie zur Seite AWS Health Dashboard – Ihr Kontozustand weitergeleitet.

2. Wählen Sie unter Servicezustand die Option Öffnen und aktuelle Probleme aus, um kürzlich gemeldete Ereignisse anzuzeigen. Sie können die folgenden Informationen über das Ereignis anzeigen:

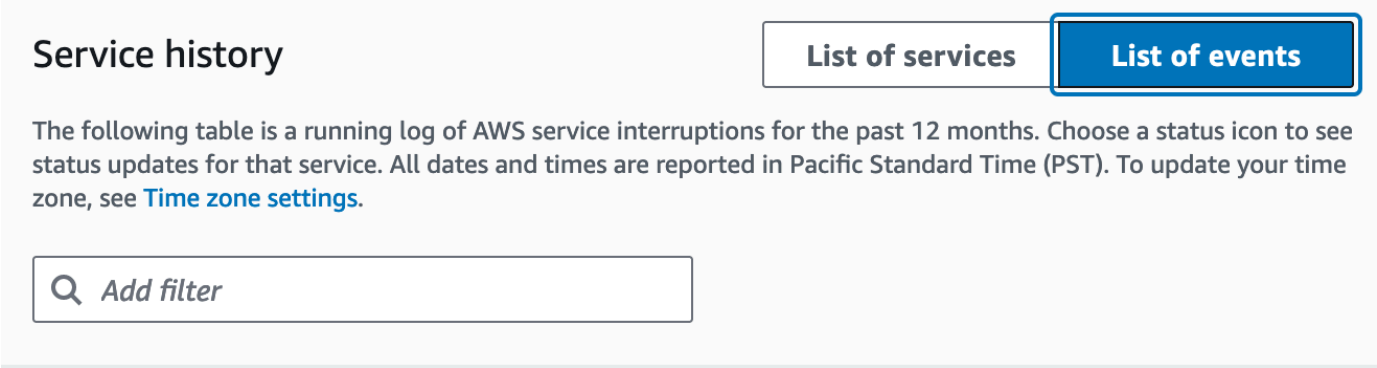
   - Der Ereignisname und die betroffene Region. Beispiel: Betriebsproblem – Amazon Elastic Compute Cloud (Nord-Virginia)
   - Der Servicename
   - Der Schweregrad des Ereignisses, z. B. Informativ oder Verschlechterung
   - Eine Zeitleiste der letzten Aktualisierungen für das Ereignis
   - Eine Liste der AWS-Services , die auch 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. (Optional) Wählen Sie neben dem Ereignis RSS aus, um einen RSS-Feed für dieses Ereignis zu abonnieren. Sie erhalten Benachrichtigungen über diesen spezifischen Service in der angegebenen AWS-Region.
4. Wählen Sie Serviceverlauf aus, um die Tabelle Serviceverlauf anzuzeigen. Diese Tabelle zeigt alle AWS-Service Unterbrechungen der letzten 12 Monate.

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

5. Wählen Sie neben einem laufenden Service-Ereignis das Statussymbol ( ), um weitere Informationen über das Ereignis anzuzeigen.
6. (Optional) Um dies als Liste historischer Ereignisse anzuzeigen, wählen Sie die Schaltfläche Ereignisliste. Wählen Sie ein beliebiges Ereignis in der Ereignisspalte aus, um weitere Informationen zu diesem spezifischen Ereignis im Popup-Seitenbereich anzuzeigen.



> **Note**
>
> Wenn Sie nach September 2023 ein beliebiges öffentliches Ereignis auswählen, wird die URL im Browser mit einem Link zu diesem öffentlichen AWS Health Ereignis gefüllt.

Nachdem Sie diesen Link ausgewählt haben, navigieren Sie zur Ereignisliste mit diesem Ereignis-Pop-up.

7. (Optional) Wählen Sie RSS aus, um einen RSS-Feed zu abonnieren. Sie erhalten Benachrichtigungen über diesen spezifischen Service in der angegebenen AWS-Region.
8. (Optional) Sie können die Ereignisse in Ihrer lokalen Zeitzone oder UTC anzeigen. Weitere Informationen finden Sie unter Einstellungen für die Zeitzone.
9. (Optional) Wenn Sie über ein -Konto verfügen, wählen Sie Kontozustand öffnen, um sich anzumelden. Nachdem Sie sich angemeldet haben, können Sie Ereignisse anzeigen, die für Ihr Konto spezifisch sind. Weitere Informationen finden Sie unter Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus.

Geplante Lebenszyklusereignisse für AWS Health

Erfahren Sie mehr über geplante Lebenszyklusereignisse für AWS Health.

Themen

Was sind geplante Lebenszyklusereignisse?

AWS Health kommuniziert wichtige Änderungen, die sich auf die Verfügbarkeit Ihrer Anwendungen auswirken können. Im -Modell der AWS geteilten Verantwortung AWS ergreift Maßnahmen, um die zugrunde liegende Hardware und Infrastruktur, die Ihre Ressourcen unterstützt, auf dem neuesten Stand und sicher zu halten. Einige Änderungen erfordern jedoch ein Kundenverhalten oder eine Koordination, um Auswirkungen auf Ihre Anwendungen zu vermeiden. AWS Health benachrichtigt Sie im Voraus über wichtige Änderungen wie:

- Ende des Supports für Open-Source-Software – Einige AWS-Services führen Open-Source-Versionen von Software aus. Wenn die Open-Source-Community die Unterstützung für Softwareversionen beendet, AWS informiert Sie, wenn Sie Maßnahmen ergreifen müssen, um ein Upgrade durchzuführen und Auswirkungen auf Ihre Anwendungen zu vermeiden.
  - Ende des Supports für Amazon RDS for MySQL-Engine-Version
  - Ende des Supports für die Amazon-EKS-Kubernetes-Version
- Änderungen, die sich auf AWS-eigene Ressourcen auswirken, die möglicherweise Ihre Aktion erfordern.
  - Ablauf von Amazon-RDS-Zertifizierungsstellenzertifikaten.
  - Amazon WorkDocs Companion erreicht das Ende seiner Lebensdauer und ist nicht mehr verfügbar.

> **Note**
>
> Alle Benachrichtigungen, die diesen Kriterien entsprechen, werden über AWS Health als geschehene Lebenszyklusereignisse gemeldet.

- Dynamischer Ressourcen-Burndown und verbesserte Metadaten: Ab dem Zeitpunkt, an dem Sie die Benachrichtigung erhalten, bis zur Lebensdauer des AWS Health Ereignisses werden Ihre betroffenen Ressourcen dem AWS Health Ereignis als betroffene Entitäten mit einem bestimmten Entitätsstatus zugeordnet. Betroffene Ressourcen werden gegebenenfalls im ARN-Format angegeben. Wenn Ihre betroffenen Ressource(n) Kundenaktionen erfordern, werden sie mit dem Status „PENDING“ aufgeführt. Wenn Ihre betroffene Ressource(n) die erforderliche Aktion ausgeführt hat oder die Ressourcen gelöscht wurden, wird der Status auf „RESOLVED“ 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 Updates bereitgestellt werden, werden Ressourcen keinen Status zugewiesen, anstatt Ressourcen mit dem Status „PENDING“ oder „RESOLVED“.
> - Aktualisierungen des Ressourcenstatus werden in den Regionen AWS GovCloud (US) und China nicht unterstützt.

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

Die AWS Health Erfahrung mit geplanten Lebenszyklusereignissen hilft Ihren Teams, mehr über bevorstehende Lebenszyklusänderungen zu erfahren und den Abschluss von Aktionen zu verfolgen.

Typkategorie: Geplante Änderung

Ereignistypcode : 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.

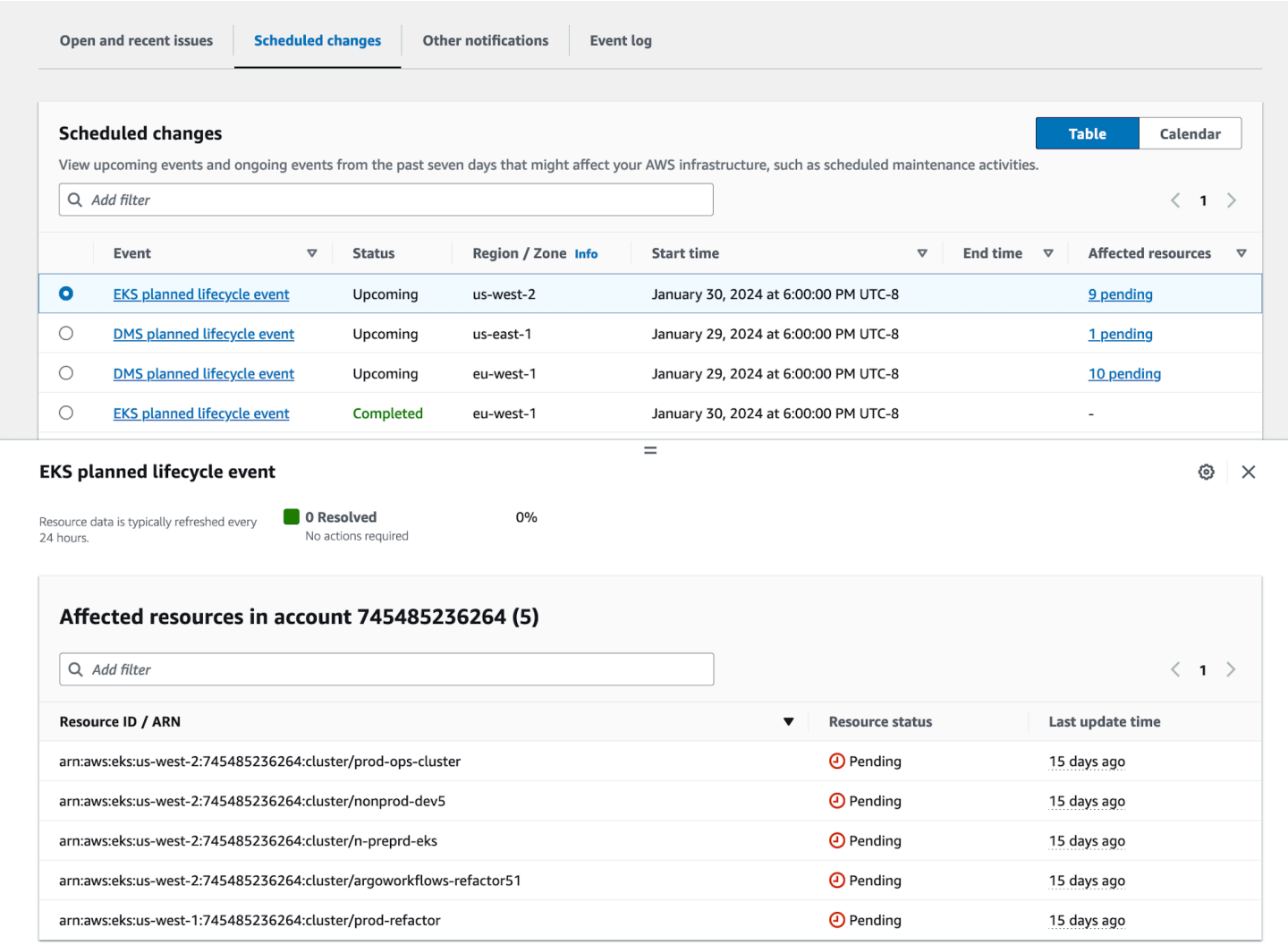
Endzeit des Ereignisses: Die Endzeit des Ereignisses ist das Datum, an dem die Änderung für alle AWS Ressourcen abgeschlossen wird. Beachten Sie, dass die Endzeit nicht immer angegeben ist. Es ist wichtig, die Startzeit als Änderungsdatum zu behandeln.

> **Note**
>
> Organisationen können erwarten, dass sie einen einzelnen Ereignis-ARN für jedes geplante Lebenszyklusereignis erhalten, gruppiert nach Region, in der es betroffene Ressourcen gibt. Sie können jedoch mehrere ARNs erhalten, wenn die Organisation über eine große Anzahl betroffener - AWS-Konten oder -Ressourcen verfügt.

Früher Einblick in geplante Lebenszyklusereignisse: Geplante Lebenszyklusereignisse sind so konzipiert, dass sie nach Möglichkeit eine Mindestvorlaufzeit von 180 Tagen für Hauptversionen/Änderungen und 90 Tagen für Nebenversionen/Änderungen haben.

Dynamischer Ressourcen-Burndown und verbesserte Metadaten: Ab dem Zeitpunkt, an dem Sie die Benachrichtigung erhalten, bis zur Lebensdauer des AWS Health Ereignisses werden Ihre betroffenen Ressourcen dem AWS Health Ereignis als betroffene Entitäten mit einem bestimmten Entitätsstatus zugeordnet. Betroffene Ressourcen werden gegebenenfalls im ARN-Format angegeben. Wenn Ihre betroffenen Ressource(n) Kundenaktionen erfordern, werden sie mit dem Status „PENDING“ aufgeführt. Wenn Ihre betroffene Ressource(n) die erforderliche Aktion ausgeführt hat oder die Ressourcen gelöscht wurden, wird der Status auf „RESOLVED“ aktualisiert.

> **Note**
>
> - AWS Health -Benachrichtigungen bieten nach Möglichkeit Statusaktualisierungen im Laufe der Zeit, mit Ausnahme der 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.

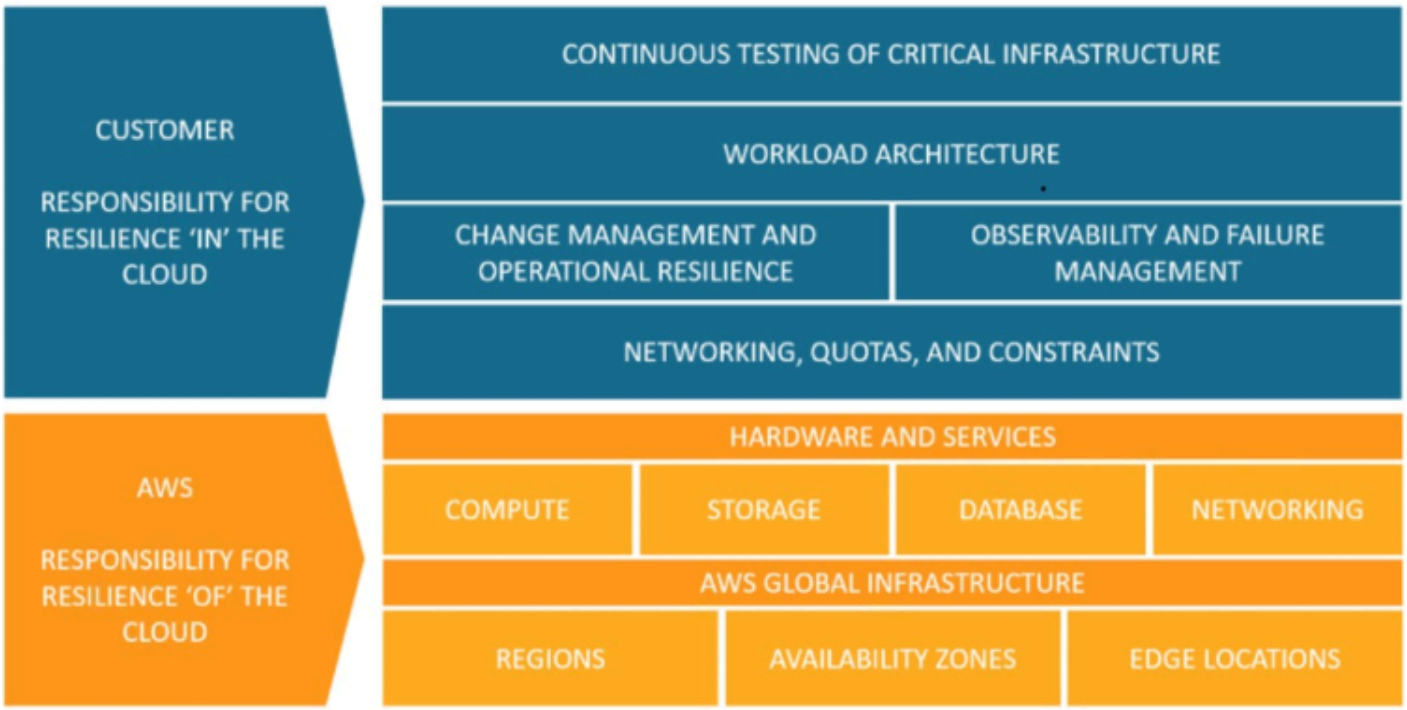


Nachdem das geplante Ereignisdatum abgelaufen ist:

1. Falls zutreffend, implementiert der Service die beschriebene Änderung möglicherweise jederzeit nach dem Startdatum des Ereignisses an Ihrer Ressource.
2. Wenn Sie alle Ressourcen vor dem Ende des Supports auflösen, ändert sich Ihr AWS Health Ereignis in den Status „Geschlossen“.
3. Wenn Sie über ausstehende Ressourcen nach dem Datum verfügen, das nicht behoben ist, bleibt das AWS Health Ereignis nach dem Start- oder Enddatum 90 Tage lang offen. Dann wird das Ereignis gelöscht.

Modell der geteilten Verantwortung für Ausfallsicherheit

Sicherheit und Compliance sind gemeinsame Verantwortlichkeiten zwischen AWS und dem Kunden. Abhängig von den bereitgestellten Services kann dieses gemeinsame Modell dazu beitragen, den Betriebsaufwand des Kunden zu entlasten. Dies liegt daran, dass die Komponenten vom Host-Betriebssystem und der Virtualisierungsebene bis zur physischen Sicherheit der Einrichtungen, in denen der Service ausgeführt wird, AWS betreibt, verwaltet und steuert. Der Kunde übernimmt zusätzlich zur Konfiguration der von bereitgestellten Sicherheitsgruppen AWS-Firewall die Verantwortung und Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheitspatches) und anderer zugehöriger Anwendungssoftware. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.



Zugreifen auf geplante Lebenszyklusereignisse

Geplante Lebenszyklusereignisse können über mehrere Kanäle aufgerufen und überwacht werden:

- Verwenden von Amazon EventBridge
- Verwenden des AWS Health Dashboards
  - Kalenderansicht
  - Ansicht der betroffenen Ressourcen

- Verwenden der AWS Health -API

Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus

Sie können Ihr AWS Health Dashboard verwenden, um mehr über AWS Health Ereignisse zu erfahren. Diese Ereignisse können sich auf Ihr AWS-Services oder auswirkenAWS-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. Sie können offene, aktuelle und geplante Änderungen einsehen. Sie können auch Benachrichtigungen und ein Ereignisprotokoll einsehen, in dem alle Ereignisse der letzten 90 Tage aufgeführt sind.
- Ereignisse Ihrer Organisation — Auf dieser Seite werden Ereignisse angezeigt, die für Ihre Organisation spezifisch sind, inAWS 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 keine habenAWS-Konto, können Sie sich mit der über AWS Health Dashboard – Servicezustand die allgemeine Verfügbarkeit von Diensten 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.

Inhalt

- Ereignistypen
- Kalenderansicht
- Ansicht der betroffenen Ressourcen
- Einstellungen für die Zeitzone
- Gesundheit Ihres Unternehmens
- Amazon konfigurieren EventBridge
- AWS HealthBewusst
- Warnungen für AWS Health-Ereignisse

Ihre Kontoereignisse im AWS Health Dashboard anzeigen

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

Um Kontoereignisse in Ihrem AWS Health Dashboard einzusehen

1. Öffnen Sie Ihr AWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Im Navigationsbereich können Sie unter Ihr Kontostatus die folgenden Optionen auswählen:
    a. Offene und aktuelle Probleme — Sehen Sie sich kürzlich geöffnete und geschlossene Ereignisse an.
    b. Geplante Änderungen — Sehen Sie sich bevorstehende Ereignisse an, die sich auf Ihre Dienste und Ressourcen auswirken könnten.
    c. Andere Benachrichtigungen — Sehen Sie sich alle anderen Benachrichtigungen und laufenden Ereignisse der letzten sieben Tage an, die sich auf Ihr Konto auswirken könnten.
    d. Ereignisprotokoll — Alle Ereignisse der letzten 90 Tage anzeigen.

Offene und aktuelle Probleme

Auf der Registerkarte Offene und aktuelle Probleme findest du alle aktuellen Ereignisse der letzten sieben Tage, die sich auf dein Konto auswirken könnten.

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

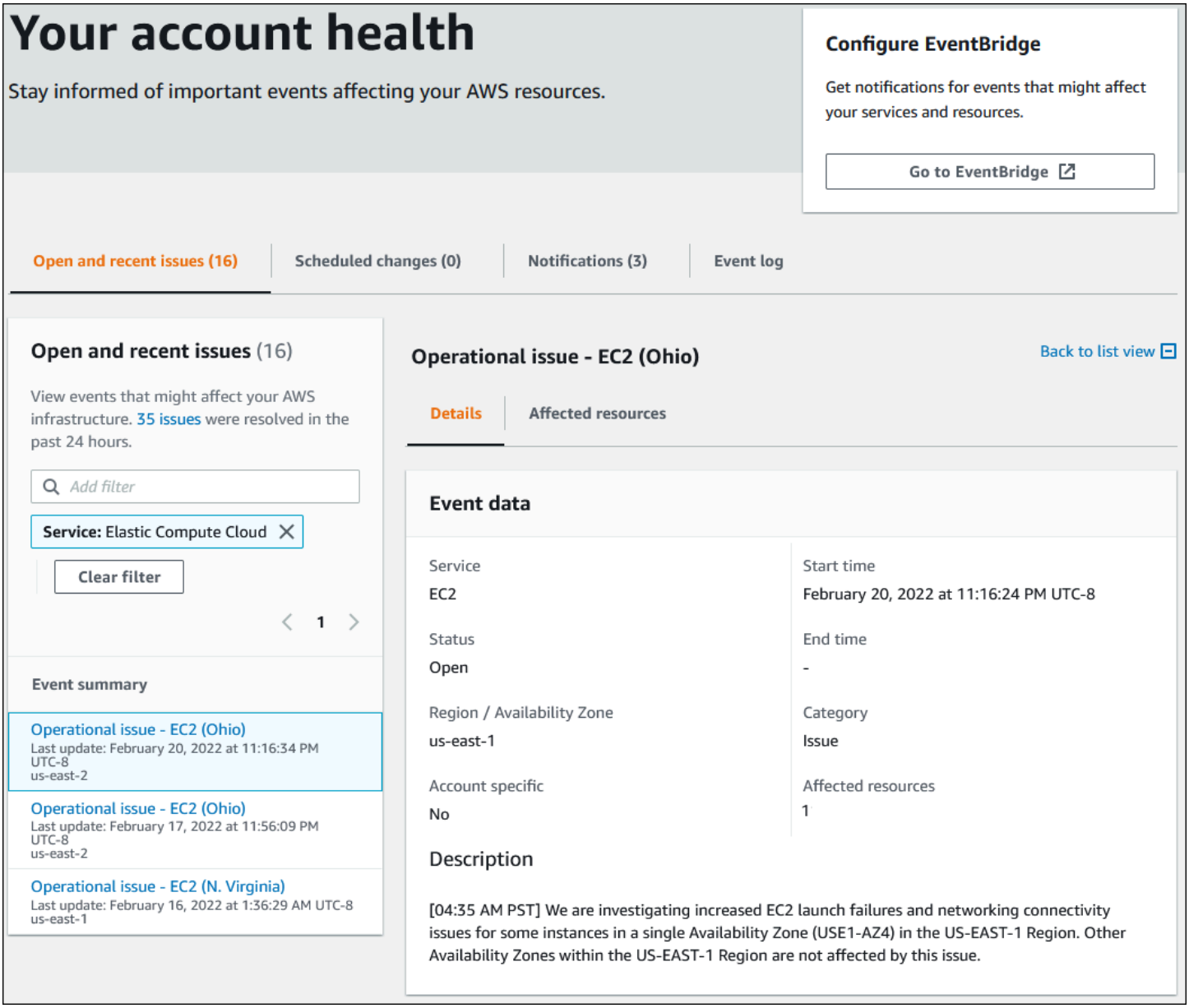
Sie können die Ereignisse filtern, die auf einer beliebigen Registerkarte angezeigt werden, indem Sie Optionen aus der Filterliste auswählen. Sie können die Ergebnisse beispielsweise nach Availability Zone, Region, Endzeit des Ereignisses oder Uhrzeit der letzten Aktualisierung AWS-Service usw. eingrenzen.

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

> **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 zu Betriebsproblemen für Amazon Elastic Compute Cloud (Amazon EC2)

Die folgende Abbildung zeigt ein Ereignis für Startfehler und Verbindungsprobleme für Amazon EC2 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, bei denen Maßnahmen zur Behebung erforderlich sind. Um Ihnen bei der Planung dieser Aktivitäten zu helfen, steht eine Kalenderansicht zur Verfügung, sodass Sie diese geplanten Änderungen einem Monatskalender zuordnen können. Filter sind verfügbar. Weitere Informationen zu geplanten Lebenszyklusereignissen finden Sie unterGeplante Lebenszyklusereignisse für AWS Health.

Andere Benachrichtigungen

Verwenden Sie den Tab Benachrichtigungen, um alle anderen Benachrichtigungen und laufenden Ereignisse der letzten sieben Tage einzusehen, die sich auf Ihr 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.

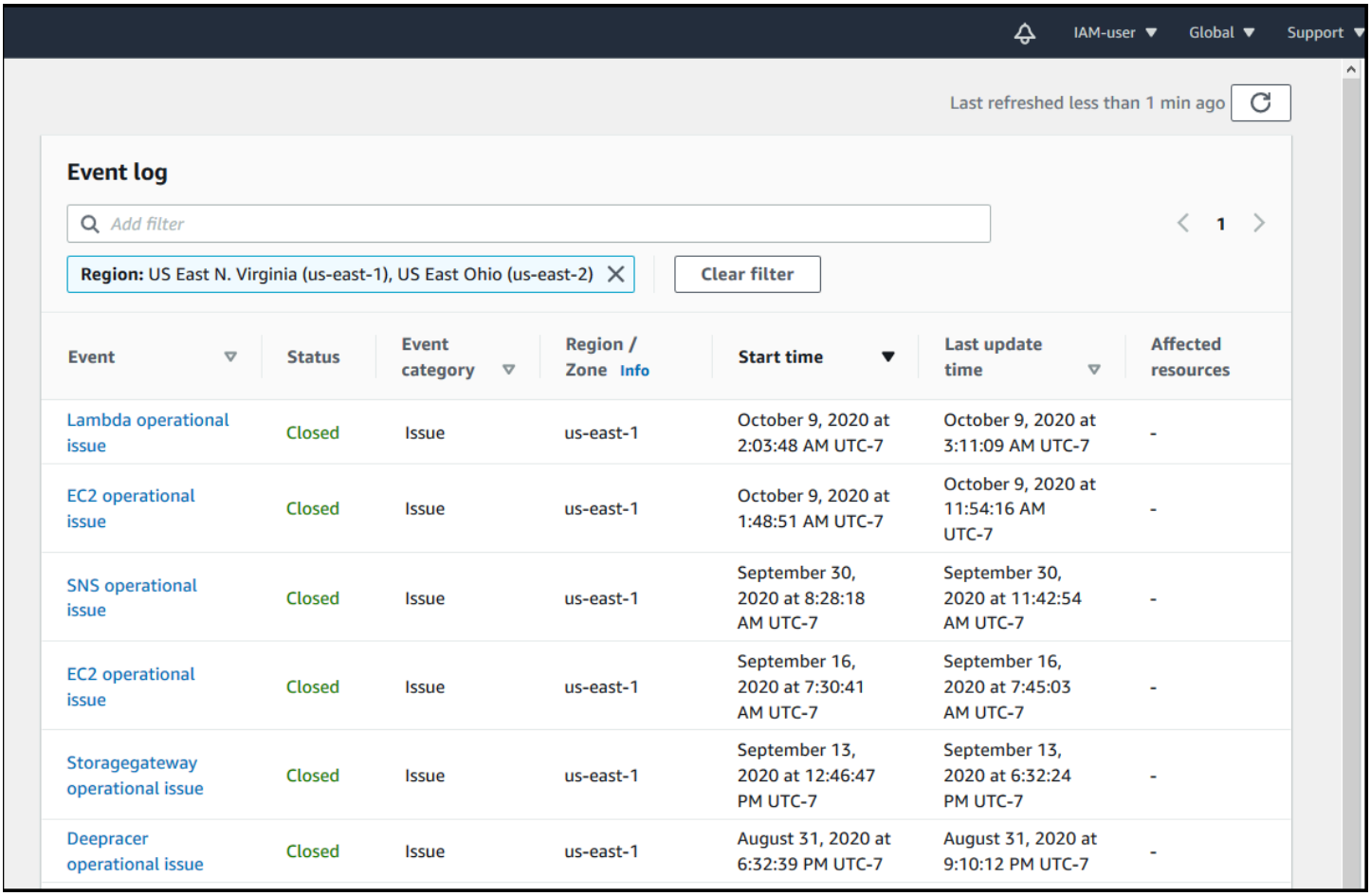
Wenn Sie ein Ereignis in der Ereignisprotokolltabelle auswählen, wird der Detailbereich mit Informationen zu dem Ereignis und der Liste der betroffenen Ressourcen angezeigt. Weitere Informationen finden Sie unter Ereignisdetails.

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

- Availability Zone
- Endzeit
- Veranstaltung
- Ereignis ARN
- Kategorie „Ereignis“
- Uhrzeit der letzten Aktualisierung
- Region
- Ressourcen-ID//ARN
- Service
- Start time (Startzeit)
- Status

Example : Ereignisprotokoll

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



Ereignisdetails

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

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

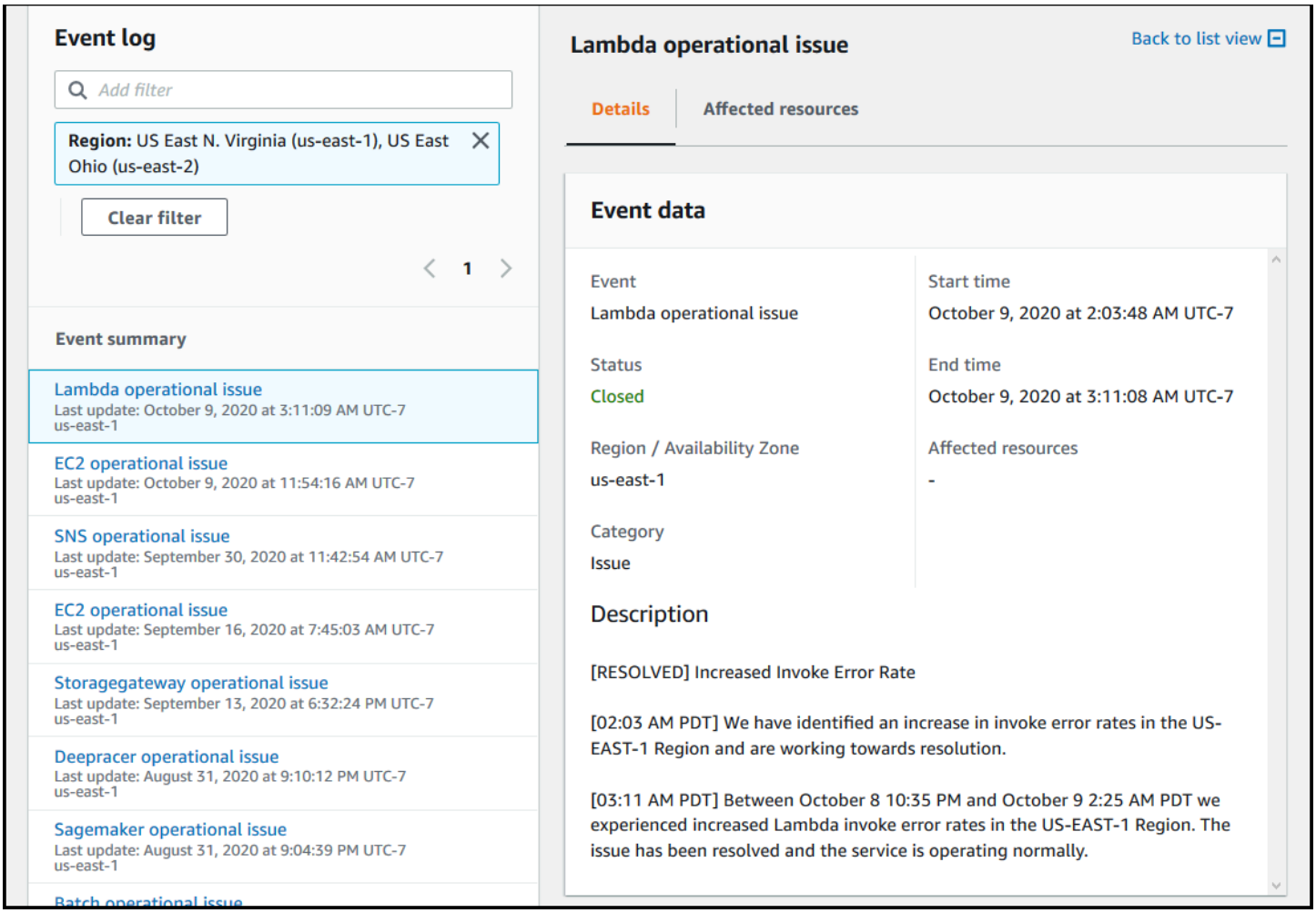
Auf der Registerkarte Betroffene Ressourcen werden die folgenden Informationen zu allen AWS Ressourcen angezeigt, die von dem Ereignis betroffen sind:

- 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 normalerweise alle 24 Stunden aktualisiert.

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 Typen von AWS Health-Ereignissen:

- Öffentliche Ereignisse sind Serviceereignisse, die nicht kontospezifisch sind. Wenn es beispielsweise ein Problem mit Amazon EC2 in einer gibtAWS-Region, AWS Health liefert Informationen über das Ereignis, auch wenn Sie in dieser Region keine Dienste oder Ressourcen nutzen.
- Kontospezifische Ereignisse sind spezifisch für Ihr Konto oder ein Konto in Ihrer Organisation. Wenn es beispielsweise ein Problem mit einer Amazon EC2 EC2-Instance in einer Region gibt, die Sie verwenden, AWS Health bietet Informationen über das Ereignis und die Liste der betroffenen Amazon EC2 EC2-Instances.

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

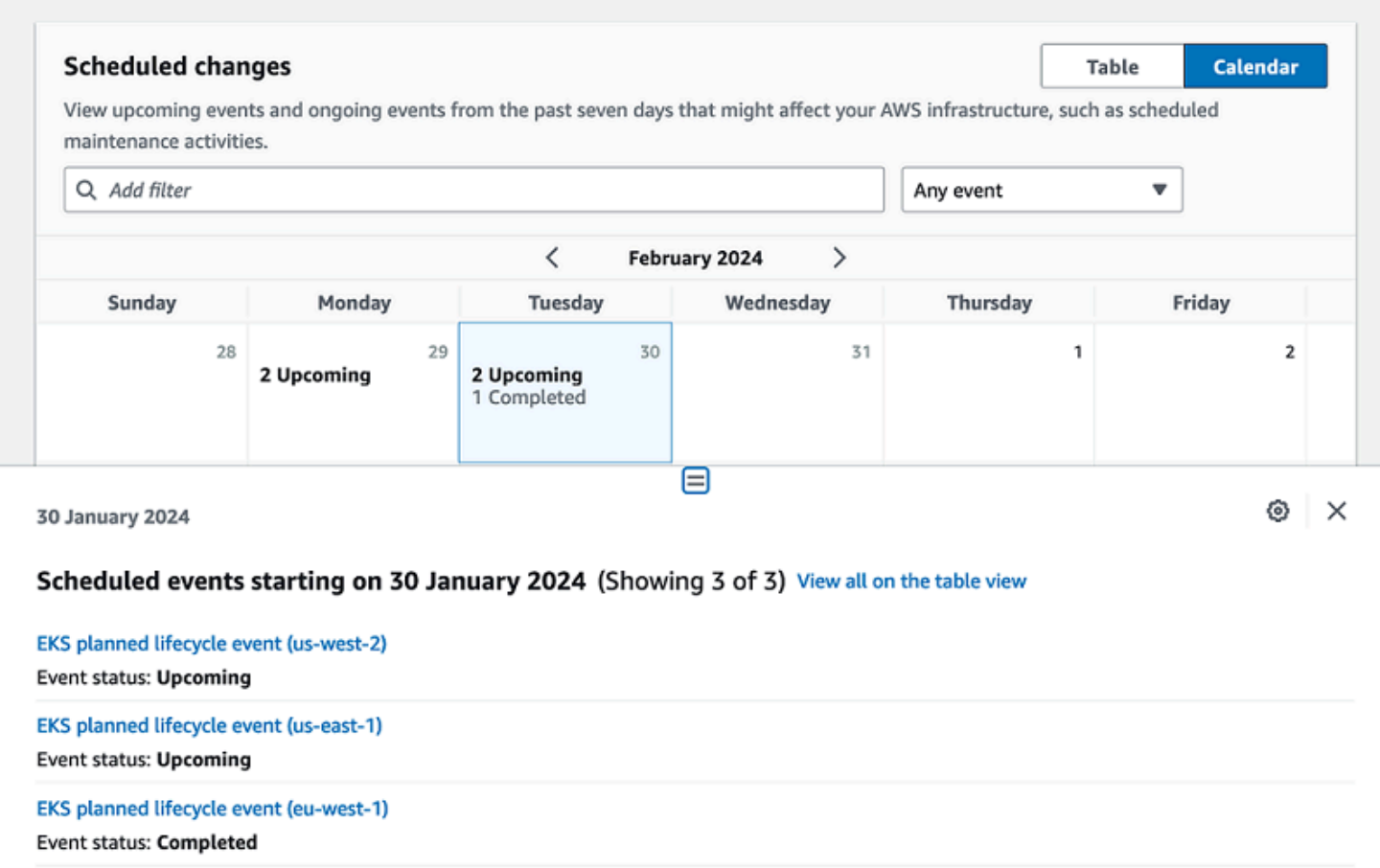
- Wählen Sie im AWS Health Dashboard den Tab Betroffene Ressourcen für ein Ereignis aus. Ereignisse mit Ressourcen sind spezifisch für Ihr Konto. Ereignisse ohne Ressourcen sind öffentlich und sind nicht spezifisch für Ihr Konto. Weitere Informationen finden Sie unter Erste Schritte mit deinem AWS Health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

Kalenderansicht

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 bis zu 3 Monate in der Vergangenheit und ein Jahr in der future sehen.

AWS HealthEreignisse werden nach Datum sortiert angezeigt. Wählen Sie ein Datum aus, um einen Seitenbereich mit weiteren Details zum AWS Health Ereignis anzuzeigen. Bevorstehende 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 von AWS Health Ereignissen 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.

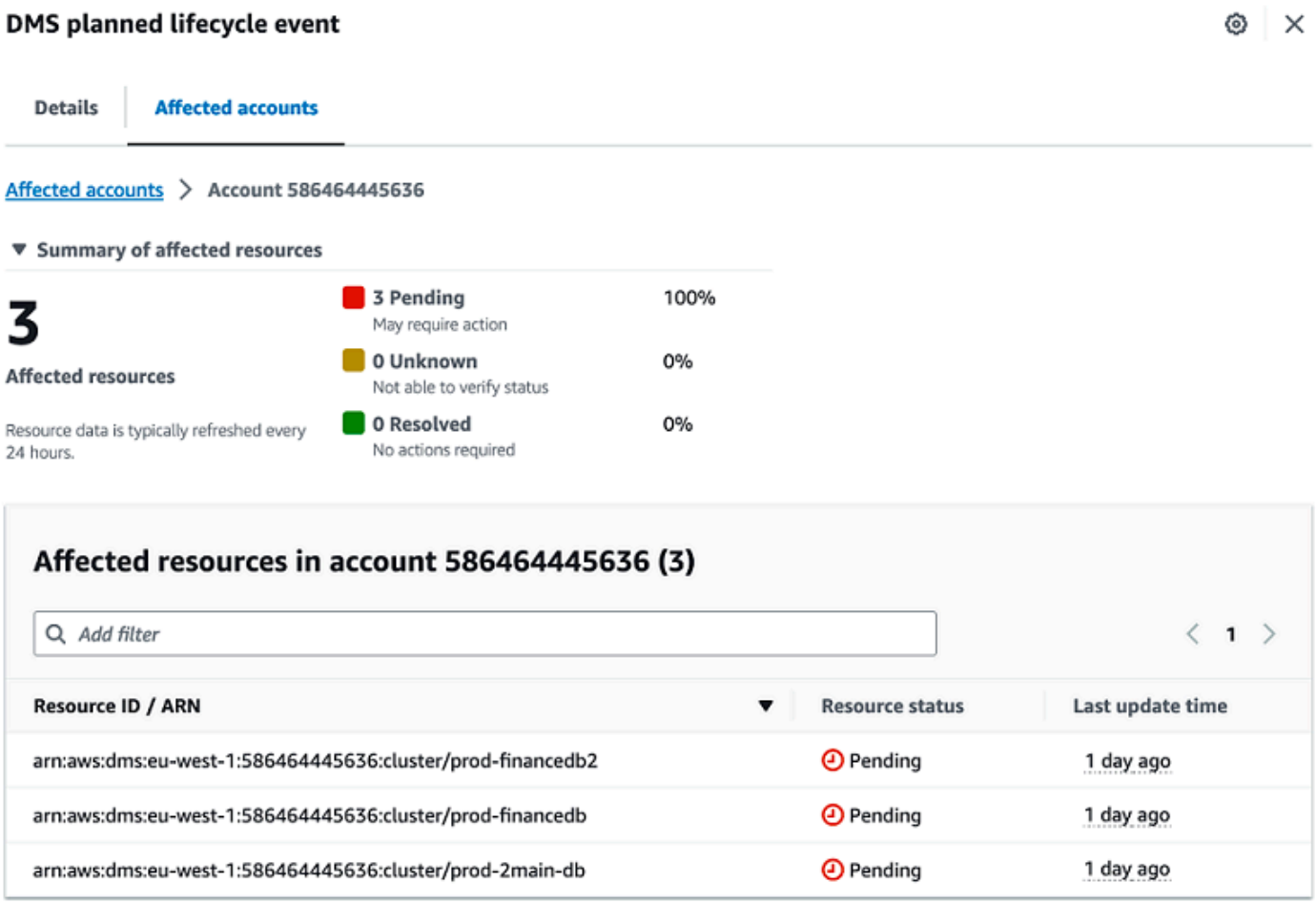


Ansicht der betroffenen Ressourcen

Bei geplanten Lebenszyklusereignissen informieren AWS Health Ereignisse in der Regel täglich über den Status der betroffenen Ressourcen. Um den Status anzuzeigen, wählen Sie das AWS Health Ereignis aus. Der Status wird auf der Registerkarte „Betroffene Ressourcen“ im Seitenbereich angezeigt.

Bei AWS Health Ereignissen auf Kontoebene wird oben auf der Registerkarte „Betroffene Ressourcen“ eine Zusammenfassung des Status der betroffenen Ressourcen angezeigt. 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 bei AWS Health Ereignissen eine Zusammenfassung des Status aller betroffenen Ressourcen für alle enthaltenen Konten angezeigt. Im Anschluss an die 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 organisatorischen Liste der betroffenen Konten zurückkehren können. Eine Zusammenfassung des Status der betroffenen Ressourcen wird oben im geteilten Bereich angezeigt.



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 alle öffentlichen Ereignisse auf die von Ihnen angegebene Zeitzone aktualisiert.

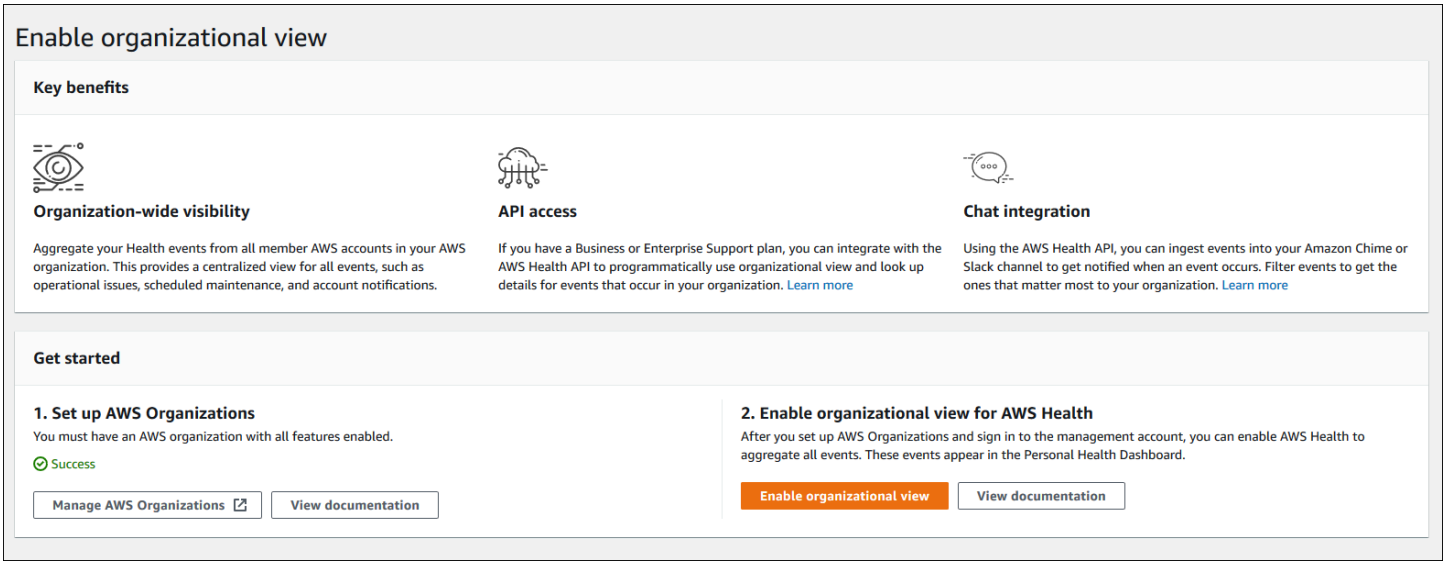
Um Ihre Zeitzoneneinstellungen zu aktualisieren

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-Präferenzen 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 die Option Zeitzoneneinstellungen aus.
5. Wählen Sie eine Zeitzone für Ihre AWS Health Dashboard-Sitzungen aus. Wählen Sie dann Save changes (Änderungen speichern).

Gesundheit Ihres Unternehmens

AWS Healthintegriert sich in, 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 von AWS Health-Ereignissen über Konten mit Organisationsansicht.



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 Sie 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 AWS Health Ereignisse mit Amazon überwachen EventBridge.

AWS HealthBewusst

Du kannst mit der AWS Health API beginnen, indem du AWS HealthAware verwendest — eine kostengünstige Anwendung, mit der du Integritätsereignisse an Slack, JIRA ServiceNow und mehr senden kannst. Kostenlose Live-Webinare sind jetzt verfügbar.

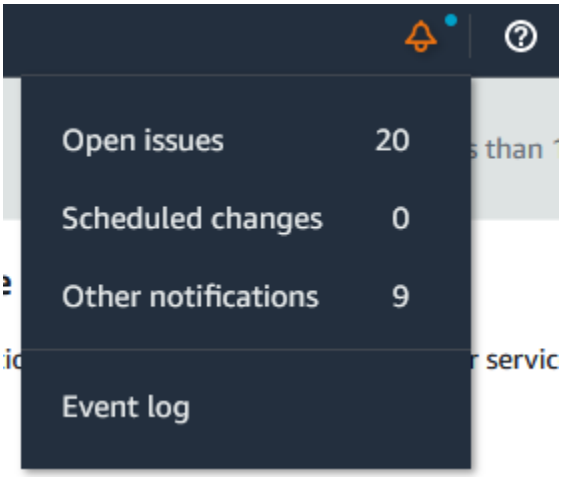
Warnungen für AWS Health-Ereignisse

Ihr AWS Health Dashboard hat in der Navigationsleiste der Konsole ein Glockensymbol mit einem Warnmenü. Diese Funktion zeigt die Anzahl der letzten AWS Health-Ereignisse an, die in jeder Kategorie auf dem Dashboard 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 navigieren, um weitere Informationen zu erhalten.

Example : Ereignisse öffnen

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


Open issues 20
Scheduled changes 0
Other notifications 9
Event log

konfigurierenAWSBenutzerbenachrichtigungen fürAWS Health

AWS Healthbietet Informationen zu Serviceabläufen, z. B. zu Betriebsproblemen, geplanten Wartungsarbeiten und geplanten Ereignissen im Softwarelebenszyklus. Für einen umfassenden Einblick inAWS HealthEs hat sich bewährt, anhand von Ereignisdetails wie den IDs der betroffenen Ressourcen, dem aktuellen Status (offen oder geschlossen) und dem Ressourcenstatus zu verfahrenAWS HealthEndpunkte, wie z. B.AWS HealthAPI, die aws.health-Quelle bei Amazon EventBridge, und dieAWS HealthArmaturenbrett. Diese Endpunkte bieten die detailliertesten Echtzeitinformationen zu laufenden Ereignissen und Änderungen, die sich auf Ihre Workloads auswirken könnten.

AWSBenachrichtigungen für Benutzerbenachrichtigt Sie über zusätzliche UX-Kanäle (E-Mail, Chat oder Push-Benachrichtigungen anAWSKonsole (mobile Anwendung).AWS HealthEreignisbenachrichtigungen enthalten nicht so viele detaillierte Daten wie die oben aufgeführten Endpunkte. Sie bieten jedoch eine einfache und effektive Möglichkeit, die Beteiligten über Probleme und Änderungen zu informieren. Auf der Grundlage der von Ihnen erstellten Regeln erstellt und sendet Benutzerbenachrichtigungen eine Benachrichtigung, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben. Sie können auswählen, an welche UX-Zustellungskanäle eine Benachrichtigung gesendet wird, und die Aggregation einrichten, um die Anzahl der Benachrichtigungen zu reduzieren, die für bestimmte Ereignisse generiert werden. Benachrichtigungen sind auch im Console Notifications Center sichtbar. Sie können beispielsweise Chat-Benachrichtigungen erhalten, wenn Sie Ressourcen in IhremAWSKonten, für die Updates geplant sind, z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Um mehr über die Einrichtung zu erfahrenAWSBenutzerbenachrichtigungen finden Sie unterErste Schritte mitAWSBenachrichtigungen für Benutzer.

Zugreifen auf die AWS Health-API

AWS Healthist ein RESTful-Webservice, 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 Anforderungen zu signieren und zu authentifizieren. Weitere Informationen zu denAWS Health Operationen und Parametern finden Sie in der AWS HealthAPI-Referenz.

> **Note**
>
> Sie benötigen einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan von AWS Supportzur Nutzung derAWS Health API. Wenn Sie dieAWS Health API von einemAWS Konto aus aufrufen, das keinen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan hat, erhalten Sie eine`SubscriptionRequiredException` Fehlermeldung.

Sie können dieAWS SDKs verwenden, um dieAWS Health REST-API-Aufrufe zu verpacken, was Ihre Anwendungsentwicklung vereinfachen kann. Sie geben IhreAWS Anmeldeinformationen an, und diese Bibliotheken übernehmen die Authentifizierung und fordern die Signatur für Sie an.

AWS Healthbietet auch einAWS Health DashboardAWS Management Console, in dem Sie Ereignisse und betroffene Entitäten anzeigen und nach ihnen suchen können. Siehe Erste Schritte mit deinem AWS Health Dashboard — Dein Kontostatus.

Endpunkte

DieAWS Health API folgt einer Anwendungsarchitektur für und verfügt über zwei regionale Endpunkte in einer aktiv-passiven Konfiguration. AWS HealthStellt zur Unterstützung von aktivem und passivem DNS-Failover einen einzigen, globalen Endpunkt bereit. Sie können eine DNS-Suche für den globalen Endpunkt durchführen, um den aktiven Endpunkt und die entsprechendeAWS Signaturregion zu ermitteln. Auf diese Weise wissen Sie, welchen Endpunkt Sie in Ihrem Code verwenden müssen, sodass Sie die neuesten Informationen abrufen könnenAWS Health.

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

Die folgende Tabelle stellt die Standardkonfiguration dar.

Beschreibung	Region „Signieren“	Endpunkt	Protocol (Protokoll)
Aktiv	us-east-1	health.us-east-1.amazonaws.com	HTTPS
Passiv	us-east-2	health.us-east-2.amazonaws.com	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 für den globalen Endpunkt CNAME durch und extrahieren Sie dann dieAWS Region aus dem aufgelösten Namen.

Example : DNS-Suche am globalen Endpunkt

Der folgende Befehl schließt eine DNS-Suche auf dem Endpunkt global.health.amazonaws.com ab. Der Befehl gibt dann den Endpunkt us-east-1 Region zurück. Diese Ausgabe sagt Ihnen, für welchen Endpunkt Sie verwenden solltenAWS 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 gebenAWS Health Daten zurück. Die neuestenAWS Health Daten sind jedoch nur am aktiven Endpunkt verfügbar. Die Daten vom

passiven Endpunkt werden irgendwann mit dem aktiven Endpunkt übereinstimmen. Wir empfehlen, dass Sie alle Workflows neu starten, wenn sich der aktive Endpunkt ändert.

Verwenden der Demo für Hochverfügbarkeitsendpunkte

AWS HealthVerwendet in den folgenden Codebeispielen eine DNS-Suche mit dem globalen Endpunkt, um den aktiven regionalen Endpunkt und die Signaturregion zu ermitteln. Dann startet der Code den Workflow neu, wenn sich der aktive Endpunkt ändert.

Themen

Verwenden der Java Demo von

Voraussetzung

Du musst Gradle installieren.

Um das Java-Beispiel zu verwenden

1. Laden Sie die Demo fürAWS 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 IhreAWS 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 Ereignisausgabe

Das Codebeispiel gibt das letzteAWS Health Ereignis der letzten sieben Tage in IhremAWS Konto zurück. Im folgenden Beispiel enthält die Ausgabe einAWS Health Ereignis für denAWS 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 HealthClient im Interface in der AWS SDK for JavaAPI-Referenz und im Quellcode.
- Weitere Informationen über die Bibliothek, die in dieser Demo für DNS-Lookups verwendet wird, finden Sie im dnsjava in GitHub.

Verwenden der Python-Demo von

Voraussetzung

Sie müssen Python 3 installieren.

Um das Python-Beispiel zu verwenden

1. Laden Sie die Demo fürAWS 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 IhreAWS 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 Ereignisausgabe

Das Codebeispiel gibt das letzteAWS Health Ereignis der letzten sieben Tage in IhremAWS Konto zurück. Die folgende Ausgabe gibt einAWS Health Ereignis für eineAWS 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 zum finden Sie in der`Health. Client` AWSSDK for Python (Boto3) -API Reference.
- Weitere Informationen über die Bibliothek, die in dieser Demo für DNS-Lookups verwendet wird, finden Sie im dnspython-Toolkit und im Quellcode auf GitHub.

Signieren von AWS Health-API-Anforderungen

Wenn Sie dieAWS SDK oder dieAWS Command Line Interface (AWS CLI) verwenden, um Anforderungen an zuAWS senden, signieren diese Tools die Anforderungen automatisch mit dem Zugriffsschlüssel, den Sie bei der Konfiguration der Tools angeben. Wenn SieAWS SDK for Java beispielsweise die Endpunktdemo mit hoher Verfügbarkeit verwenden, müssen Sie Anforderungen nicht selbst signieren.

Java-Codebeispiele

Weitere Beispiele zur Verwendung derAWS Health API mit demAWS SDK for Java finden Sie in diesem Beispielcode.

Wenn Sie Anforderungen senden, empfehlen wir dringend, nicht dieAWS Root-Konto-Anmeldeinformationen für den regulären Zugriff auf zu verwendenAWS Health. Sie können die Anmeldeinformationen eines IAM-Benutzers nutzen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Sperren der Root-Benutzerzugriffsschlüssel IhresAWS Kontos.

Wenn Sie dieAWS SDK oder die nicht verwendenAWS CLI, müssen Sie Ihre Anforderungen selbst signieren. Wir empfehlen,AWS Signature Version 4 zu verwenden. Weitere Informationen dazu finden Sie unter Signieren von AWS API-Anforderungen im Allgemeine AWS-Referenz.

Unterstützte Operationen in AWS Health

AWS Health unterstützt die folgenden Operationen für den Abruf von Informationen zu Ereignissen, die sich auf ein AWS-Konto beziehen:

- Die von AWS Health unterstützten Ereignistypen.
- Informationen zu einem oder mehreren Ereignissen, die bestimmten Filterkriterien entsprechen.
- Informationen zu den Entitäten, die von einem oder mehreren Ereignissen betroffen sind.

- Kategoriebasierte Anzahl der Ereignisse oder Entitäten, die bestimmten Filterkriterien entsprechen.

Alle Operationen sind nicht mutierend. Das bedeutet, sie rufen Daten ab, ändern sie aber nicht. In den folgenden Abschnitten werden die in AWS Health verfügbaren Operationen zusammengefasst:

Event types (Ereignistypen)

DieDescribeEventTypesOperation ruft Ereignistypen ab, die dem optionalen angegebenen Filter entsprechen. Ein Ereignistyp ist eine Vorlagendefinition eines EreignissesAWSService, Ereignistypcode und Kategorie. Der Ereignistyp und das Ereignis entsprechen der Klasse und dem Objekt in der objektorientierten Programmierung. Die Anzahl der von AWS Health unterstützten Ereignistypen wird beständig erhöht.

Ereignisse

DieDescribeEventsOperation ruft zusammenfassende Informationen zu Ereignissen ab, die mit einem zusammenhängenAWSKonto. Diese Ereignisse können mit AWS-Betriebsproblemen, geplanten Änderungen an der AWS-Infrastruktur sowie mit Sicherheits- und Fakturierungsbenachrichtigungen in Zusammenhang stehen. DieDescribeEventDetails-Operation ruft detaillierte Informationen zu einem oder mehreren Ereignissen abAWSService, Region, Availability Zone, Start- und Endzeit des Ereignisses sowie eine Textbeschreibung.

Betroffene Entitäten

DieDescribeAffectedEntities-Operation ruft Informationen über Entitäten ab, die von einem oder mehreren Ereignissen betroffen sind. Die Ergebnisse können mit weiteren Kriterien gefiltert werden, einschließlich Status, die den AWS-Ressourcen möglicherweise zugewiesen wurden.

Aggregation

DieDescribeEventAggregatesOperation ruft eine Anzahl der Ereignisse in jeder Ereignistypkategorie ab, optional gefiltert nach anderen Kriterien. DieDescribeEntityAggregatesOperation ruft eine Anzahl der Entitäten (Ressourcen) ab, die von einem oder mehreren angegebenen Ereignissen betroffen sind.

AWS Organizations und Organisationsansicht

DescribeEventsForOrganization

DescribeEventsForOrganizationgibt zusammenfassende Informationen über Ereignisse im gesamtenAWS Organizations, die den angegebenen Filterkriterien entsprechen

DescribeAffectedAccountsForOrganization

DescribeAffectedAccountsForOrganizationgibt eine Liste vonAWSKonten in derAWS Organizationsdie von dem bereitgestellten Ereignis betroffen sind.

DescribeEventDetailsForOrganization

DescribeEventDetailsForOrganizationgibt detaillierte Informationen zu einem oder mehreren angegebenen Ereignissen für ein oder mehrere Konten inAWS Organizations.

DescribeAffectedEntitiesForOrganization

DescribeAffectedEntitiesForOrganizationgibt eine Liste von Entitäten zurück, die von einem oder mehreren Ereignissen für ein oder mehrere Konten in Ihrer Organisation betroffen sind, basierend auf den Filterkriterien

EnableHealthServiceAccessForOrganization

EnableHealthServiceAccessForOrganizationOperation gewährt dieAWS HealthServiceberechtigung zur Interaktion mitAWS Organizationsim Namen des Kunden und wendet eine mit Service verknüpfte Rolle auf das Verwaltungskonto in Ihrer Organisation an.

DisableHealthServiceAccessForOrganization

DisableHealthServiceAccessForOrganizationVorgang widerruft die Berechtigung fürAWS HealthDienst zur InteraktionAWS Organizationsim Namen des Kunden.

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganizationOperation liefert Statusinformationen zum Aktivieren oder DeaktivierenAWS Healthum mit Ihrer Organisation zusammenzuarbeiten

Weitere Informationen zu diesen Operationen finden Sie im AbschnittAWS HealthAPI-Referenz.

Java-Codebeispiel für die AWS Health-API

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

Schritt 1: Initialisieren von Anmeldeinformationen

Für die Kommunikation mit der AWS Health-API sind gültige Anmeldeinformationen erforderlich. Sie können das key pair jedes IAM-Benutzers von einemAWSKonto.

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 einesAWS HealthAPI-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 vonAWS Health-API-Operationen um Ereignisinformationen zu erhalten

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 in AWS Health

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Health, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Health. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Health , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Health Ressourcen unterstützen.

Themen

Datenschutz in AWS Health

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Health. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen 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 unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. 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).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- 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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 AWS Health 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 erfahren Sie, wie Daten AWS Health verschlüsselt werden.

Datenverschlüsselung bezieht sich auf den Schutz von Daten während der Übertragung (wenn sie vom Dienst zu Ihrem AWS Konto übertragen werden) und im Ruhezustand (während sie in AWS Diensten gespeichert werden). 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 Daten, die von gespeichert werden, AWS Health sind im Ruhezustand verschlüsselt.

Verschlüsselung während der Übertragung

Alle Daten, die zu und von AWS Health ihnen gesendet werden, werden bei der Übertragung verschlüsselt.

Schlüsselverwaltung

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

Identity and Access Management für AWS Health

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

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Health

Dienstbenutzer — Wenn Sie den AWS Health Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Health Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Problembehandlung bei AWS Health Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS Health haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Health Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Health. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Health Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Health, finden Sie unterWie AWS Health funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Health verfassen können. Beispiele für AWS Health identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. AWS Health Beispiele für identitätsbasierte Richtlinien

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann.

Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert,

so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services können Sie Aktionen ausführen, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen

auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien 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. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. 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 könnten beispielsweise eine Richtlinie erstellen, die einem IAM-Benutzer nur den Zugriff auf bestimmte Amazon EC2 EC2-Ereignisse in der ermöglicht. AWS Health Dashboard

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 Services, die ACLs unterstützen. AWS WAF 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, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle

oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Health funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs verwenden AWS Health, sollten Sie wissen, mit welchen IAM-Funktionen Sie diese verwenden können. AWS HealthEinen allgemeinen Überblick darüber, wie AWS Health und andere AWS Dienste mit IAM funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Services That Work with IAM.

Themen

- Identitätsbasierte AWS Health -Richtlinien
- Ressourcenbasierte AWS Health -Richtlinien
- Autorisierung auf der Basis von AWS Health -Tags
- AWS Health IAM-Rollen

Identitätsbasierte AWS Health -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 auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

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 DescribeEventDetailsAPI-Vorgangs einzusehen, nehmen Sie die `heath:DescribeEventDetails` Aktion in die Richtlinie auf.

Richtlinienerklärungen müssen ein `Action` `NotAction` Oder-Element enthalten. AWS Health definiert einen 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 Definierte Aktionen von.

Ressourcen

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

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

```
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 AWS Service Namespaces.

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 DescribeEventsVorgang gibt beispielsweise Informationen über Ereignisse zurück, die bestimmte Filterkriterien 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 DescribeAffectedEntitiesund DescribeEventDetailsAPI-Operationen. 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 Defined by (Ressourcen definiert von). 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 kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

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

Die DescribeEventDetailsAPI-Operationen DescribeAffectedEntitiesund unterstützen die `health:service` Bedingungsschlüssel `health:eventTypeCode` und.

Eine Liste der AWS Health Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Health im IAM-Benutzerhandbuch. 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

Ressourcenbasierte AWS Health -Richtlinien

Bei ressourcenbasierten Richtlinien handelt es sich um JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal auf der AWS Health Ressource ausführen kann und unter welchen Bedingungen. AWS Health unterstützt ressourcenbasierte Berechtigungsrichtlinien für Gesundheitsereignisse. Ressourcenbasierte Richtlinien ermöglichen die Erteilung von Nutzungsberechtigungen für andere -Konten pro Ressource. 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 Prinzipal und die Ressource in unterschiedlichen AWS Konten befinden, müssen Sie der Prinzipalentität auch die Erlaubnis erteilen, auf die Ressource zuzugreifen. 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 unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

AWS Health unterstützt nur ressourcenbasierte Richtlinien für die DescribeAffectedEntitiesund DescribeEventDetailsAPI-Operationen. Sie können diese Aktionen in einer Richtlinie angeben, um zu definieren, welche Haupteinheiten (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

Autorisierung auf der Basis von AWS Health -Tags

AWS Health unterstützt das Markieren von Ressourcen oder das Steuern des Zugriffs anhand von Stichwörtern nicht.

AWS Health IAM-Rollen

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

Verwenden temporärer 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 Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen GetFederationToken.

AWS Health unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

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

Sie können den EnableHealthServiceAccessForOrganizationVorgang verwenden, um die mit dem Dienst verknüpfte Rolle im Konto zu erstellen. Wenn Sie diese Funktion jedoch deaktivieren möchten, müssen Sie zuerst den DisableHealthServiceAccessForOrganizationVorgang 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 von AWS Health-Ereignissen über Konten mit Organisationsansicht.

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 mit der AWS Management Console 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

- Bewährte Methoden für Richtlinien
- Verwenden der AWS Health -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugriff auf die AWS Health Dashboard und die API AWS Health
- Ressourcen- und aktionsbasierte Bedingungen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Health Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den 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 AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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 für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS 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 zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert 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 Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Verwenden der AWS Health -Konsole

Um auf die AWS Health Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den AWS Health Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. 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:

- Aktiviert oder deaktiviert die Funktion zur Ansicht der AWS Health Organisation für alle Konten in einer AWS Organisation
- Das AWS Health Dashboard in der AWS Health Konsole
- AWS Health API-Operationen und Benachrichtigungen
- Informationen zu Konten anzeigen, die Teil Ihrer AWS Organisation sind
- Zeigen Sie die Organisationseinheiten (OU) des Verwaltungskontos an

Example : AWSHealthFullAccess

```
{
    "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 von serviceverknüpften Rollen für AWS Health.

Sie müssen Benutzern, die nur die API 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 API AWS CLI oder AWS .

```
{
    "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": "*"
        }
    ]
}
```

Zugriff auf die AWS Health Dashboard und die API AWS Health

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

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

Standardmäßig haben IAM-Benutzer keinen Zugriff auf die AWS Health Dashboard oder die AWS Health API. Sie gewähren Benutzern Zugriff auf die AWS Health Informationen Ihres Kontos, indem Sie IAM-Richtlinien einem einzelnen Benutzer, einer Benutzergruppe oder einer Rolle zuordnen. 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 Anzeigeberechtigungen AWS Health Dashboard hat schreibgeschützten Zugriff auf Gesundheitsinformationen aller AWS Dienste auf dem Konto. Dazu können unter anderem AWS Ressourcen-IDs wie Amazon EC2 EC2-Instance-IDs, EC2-Instance-IP-Adressen und allgemeine Sicherheitsbenachrichtigungen gehören. Wenn eine IAM-Richtlinie beispielsweise nur Zugriff auf 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 gepostet 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 Operationen wie DescribeEventsund verwenden DescribeEventDetails, um Informationen über AWS Health Ereignisse für Ihr Konto abzurufen.
- Organisationskonto — Sie können Vorgänge wie DescribeEventsForOrganizationund verwenden DescribeEventDetailsForOrganization, um Informationen über AWS Health Ereignisse für Konten abzurufen, 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 AWS Health Dashboard und AWS Health. AWS Health unterstützt die Zugriffskontrolle für Ereignisse auf der Grundlage des `eventTypeCode` AND-Dienstes.

Zugriffsbeschreibung

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

Example : Zugriffsbeschreibung

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

Zugriffsverweigerung

Diese Richtlinienerklärung verweigert den Zugriff auf AWS Health Dashboard und die AWS Health API. Ein IAM-Benutzer mit dieser Richtlinie kann die AWS Health Dashboard API-Operationen nicht einsehen AWS Management Console und keine der AWS Health API-Operationen aufrufen.

Example : Zugriffsverweigerung

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

Organisationsansicht

Wenn Sie die organisatorische Ansicht 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 Durch AWS Health APIs definierte Aktionen und Benachrichtigungen.

> **Note**
>
> Sie müssen die Anmeldeinformationen des Verwaltungskontos einer Organisation verwenden, um auf die AWS Health APIs für AWS Organizations zugreifen zu können. Weitere Informationen finden Sie unter Aggregieren von AWS Health-Ereignissen über Konten mit Organisationsansicht.

Erlauben Sie den Zugriff auf die AWS Health Unternehmensansicht

Diese Richtlinienerklärung gewährt Zugriff auf alle AWS Health AWS Organizations Aktionen, die Sie für die Funktion „Organisationsansicht“ benötigen.

Example : Erlaubt den Zugriff auf die AWS Health Organisationsansicht

```
{
    "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 auf die AWS Health Organisationsansicht verweigern

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

Example : Verweigern Sie den Zugriff auf die AWS Health Organisationsansicht

```
{
    "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, dem/der Sie Berechtigungen erteilen möchten, bereits über eine IAM-Richtlinie verfügt, können Sie die AWS Health-spezifische Richtlinienanweisung zu dieser Richtlinie hinzufügen.

Ressourcen- und aktionsbasierte Bedingungen

AWS Health unterstützt IAM-Bedingungen für die DescribeAffectedEntitiesund DescribeEventDetailsAPI-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 DescribeAffectedEntitiesund die DescribeEventDetailsAPI unterstützen Berechtigungen auf Ressourcenebene. Sie können beispielsweise eine Richtlinie erstellen, um bestimmte AWS Health Ereignisse zuzulassen oder abzulehnen.
> - Die DescribeEventDetailsForOrganizationAPI-Operationen DescribeAffectedEntitiesForOrganizationund unterstützen keine Berechtigungen auf Ressourcenebene.
> - Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Health APIs und Benachrichtigungen in der Serviceautorisierungsreferenz.

Example : Aktionsbasierte Bedingung

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

```
{
    "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 : Ressourcenbasierte Bedingung

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

```
{
  "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 : Zustand eventTypeCode

Diese Grundsatzerklärung gewährt Zugriff auf AWS Health Dashboard und die AWS Health `Describe*` API-Operationen, verweigert jedoch den Zugriff auf alle AWS Health Ereignisse, `eventTypeCode` die den entsprechenden Bedingungen entsprechen`AWS_EC2_*`.

```
{
    "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 DescribeEventDetailsOperationen DescribeAffectedEntitiesund aufrufen und nicht berechtigt sind, auf das AWS Health Ereignis zuzugreifen, wird der `AccessDeniedException` Fehler angezeigt. Weitere Informationen finden Sie unter Problembehandlung bei AWS Health Identität und Zugriff.

Problembehandlung bei 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 durchzuführen in AWS Health
- Ich bin nicht berechtigt, iam auszuführen: PassRole

- Ich möchte meine Zugriffsschlüssel anzeigen
- Ich bin Administrator und möchte anderen den Zugriff ermöglichen AWS Health
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Health Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Health

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

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

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

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

Ich bin nicht berechtigt, iam auszuführen: 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.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte 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 ermöglichen AWS Health

Um anderen den Zugriff zu ermöglichen AWS Health, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend

müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in AWS Health gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Health Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (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 dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für AWS Health

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

Sie können eine dienstbezogene Rolle zur Einrichtung verwenden, um das manuelle Hinzufügen der erforderlichen Berechtigungen AWS Health zu vermeiden. AWS Health definiert die Berechtigungen ihrer dienstbezogenen 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.

Berechtigungen von serviceverknüpften Rollen für AWS Health

AWS Health hat zwei dienstbezogene Rollen:

- AWSServiceRoleForHealth_Organizations— Diese Rolle vertraut darauf, dass AWS Health (`health.amazonaws.com`) die Zugriffsrolle AWS-Services für Sie übernimmt. Dieser Rolle ist die `Health_OrganizationsServiceRolePolicy` AWS verwaltete Richtlinie zugeordnet.
- AWSServiceRoleForHealth_EventProcessor— Diese Rolle vertraut darauf, dass der AWS Health Dienstprinzipal (`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 AWS Incident Detection and Response zu erstellen. Bei dieser Regel handelt es sich um die Infrastruktur, die Sie benötigen AWS-Konto , um Informationen zur Änderung des Alarmstatus von Ihrem Konto an zu übermitteln 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 EnableHealthServiceAccessForOrganizationVorgang aufrufen, AWS Health erstellt diese dienstbezogene Rolle im Konto für Sie.

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

Bearbeiten einer serviceverknüpften Rolle für AWS Health

AWS Health erlaubt Ihnen nicht, die dienstbezogene 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 DisableHealthServiceAccessForOrganizationVorgang 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, wenden Sie sich an sie AWS Support und bitten Sie sie, Ihre Workloads aus AWS Incident Detection and Response zu entfernen. Nach Abschluss dieses Vorgangs können Sie eine der 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 dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete 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 Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie 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: AWSHealth_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 mit dem Dienst verknüpften Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Health.

Die verwaltete Richtlinie verfügt über die folgenden Berechtigungen, um den Zugriff auf die EventBridge Amazon-Regel für AWS Incident Detection and Response 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.

```
{
    "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 der AWS verwalteten 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 mit dem Dienst verknüpften Rolle, Aktionen für Sie abzuschließen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Health.

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

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

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

```
{
    "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 der AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSHealthFullAccess

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

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Aktiviert oder deaktiviert die AWS Health Funktion zur Ansicht der Organisation für alle Konten in einer AWS Organisation und zeigt die Organisationseinheiten (OU) des Verwaltungskontos an
- `health`— Zugriff auf die AWS Health API-Operationen und Benachrichtigungen
- `iam`— Erstellt eine IAM-Rolle, die mit dem AWS Health Dienst verknüpft ist

```
{
    "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 unter[AWS Health Aktualisierungen der AWS verwalteten Richtlinien](#).

AWS Health Aktualisierungen der AWS verwalteten Richtlinien

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

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

AWS Health

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: AWSHealthFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Health hat die AWSHealthFullAccess Richtlinie auf Regionen 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, mit denen eine dienstbezogene Rolle die Konten und AWS Dienste beschreiben kann, mit AWS Organizations denen sie verwendet werden können.	19. Juli 2023
Änderungsprotokoll veröffentlicht	Änderungsprotokoll für die AWS Health verwalteten Richtlinien.	13. Januar 2023

Anmeldung und Überwachung 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 können, 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 Kennzahlen Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon EventBridge liefert eine Reihe near-real-time von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Rechnen. Sie können Regeln schreiben, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen, wenn diese Ereignisse eintreten. Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen EventBridge.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Aufrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.

Weitere Informationen finden Sie unter Überwachung AWS Health.

Überprüfung der Einhaltung der Vorschriften für AWS Health

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz 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 hoher Redundanz 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 in mehreren Availability Zones gespeichert und repliziert. Dieser Ansatz stellt sicher, dass Sie über die AWS Health Dashboard oder die AWS Health API-Operationen auf sie zugreifen können. Sie können AWS Health Ereignisse bis zu 90 Tage nach ihrem Auftreten 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.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Health über das Netzwerk. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. 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-Steuerung fallen in die gemeinsame AWS Verantwortung von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Bewährte Methoden für die Sicherheit für AWS Health

Sehen Sie sich die folgenden bewährten Methoden für die Arbeit mit an AWS Health.

Gewähren Sie AWS Health Benutzern die geringstmöglichen Berechtigungen

Befolgen Sie das Prinzip der geringsten Rechte, indem Sie die Mindestanzahl von Zugriffsrichtlinienberechtigungen für Ihre -Benutzer und -Gruppen verwenden. Sie könnten beispielsweise einem AWS Identity and Access Management (IAM-) Benutzer Zugriff auf den AWS 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 AWS Health Dashboard

Suchen Sie AWS Health Dashboard regelmäßig nach Ereignissen, 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 deinem AWS Health Dashboard — Dein Kontostatus.

Integrieren Sie AWS Health mit Amazon Chime oder Slack

Sie können Ihre AWS Health Chat-Tools integrieren. Durch diese 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 AWS Health Ereignisse

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 regionsspezifisch, 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. In diesem Fall 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 AWS Health Ereignisse mit Amazon überwachen EventBridge.

Aggregieren von AWS Health-Ereignissen über Konten mit Organisationsansicht

Standardmäßig können SieAWS Healthum die anzusehenAWS HealthEreignisse eines einzigenAWSKonto. Wenn Sie AWS Organizations verwenden, können Sie AWS Health-Ereignisse auch zentral in Ihrer Organisation anzeigen. Diese Funktion bietet Zugriff auf dieselben Informationen wie Operationen mit einzelnen Konten. Mithilfe von Filtern können Sie Ereignisse nach AWS-Regionen, Konten und Services anzeigen.

Sie können Ereignisse zusammenfassen, um Konten in Ihrem Unternehmen zu identifizieren, die von einem betrieblichen Ereignis 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-Services auf dem Laufenden zu bleiben, die Aktualisierungen oder Codeänderungen erfordern könnten.

Es ist eine bewährte Methode, die zu verwendenDelegierter AdministratorFunktion zur Delegierung des Zugriffs aufAWS HealthOrganisatorische Ansicht eines Mitgliedskontos. Dies erleichtert den operativen Teams den Zugriff aufAWS HealthEreignisse in Ihrer Organisation. Mit der Funktion „Delegierter Administrator“ können Sie Ihr Verwaltungskonto einschränken und Teams gleichzeitig die Transparenz bieten, die sie benötigen, um entsprechend zu handeln.AWS HealthEreignisse.

Important

- AWS Health nimmt keine Ereignisse auf, die in Ihrer Organisation aufgetreten sind, bevor Sie die Organisationsansicht aktiviert haben. Wenn beispielsweise ein Mitgliedskonto (111122223333) in Ihrer Organisation ein Ereignis für Amazon Elastic Compute Cloud (Amazon EC2) erhalten hat, bevor Sie diese Funktion aktiviert haben, wird dieses Ereignis nicht in Ihrer Organisationsansicht angezeigt.
- AWS HealthEreignisse, die für Konten in Ihrer Organisation gesendet wurden, werden in der Organisationsansicht 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 beim Verwaltungskonto an alsAWS Identity and Access Management(IAM) - Benutzer oder übernehmen Sie eine IAM-Rolle.

  Sie können sich auch als Root-Benutzer (nicht empfohlen) im Verwaltungskonto Ihrer Organisation anmelden. Weitere Informationen finden Sie unterSperren Sie IhreAWSBenutzerzugriffsschlüssel für das Stammkontoin derIAM-Benutzerhandbuch.
- Wenn Sie sich als IAM-Benutzer anmelden, verwenden Sie eine IAM-Richtlinie, die Zugriff auf dieAWS Healthund Maßnahmen der Organisationen, wie dieAWSHealthFullAccessPolitik. Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Themen

Organisationsansicht (Konsole)

Sie können dieAWS Health Konsole verwenden, um eine zentrale Ansicht der Gesundheitsereignisse in IhrerAWS Organisation zu erhalten.

Die Organisationsansicht ist in derAWS Health Konsole für alleAWS Support Pläne ohne zusätzliche Kosten verfügbar.

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

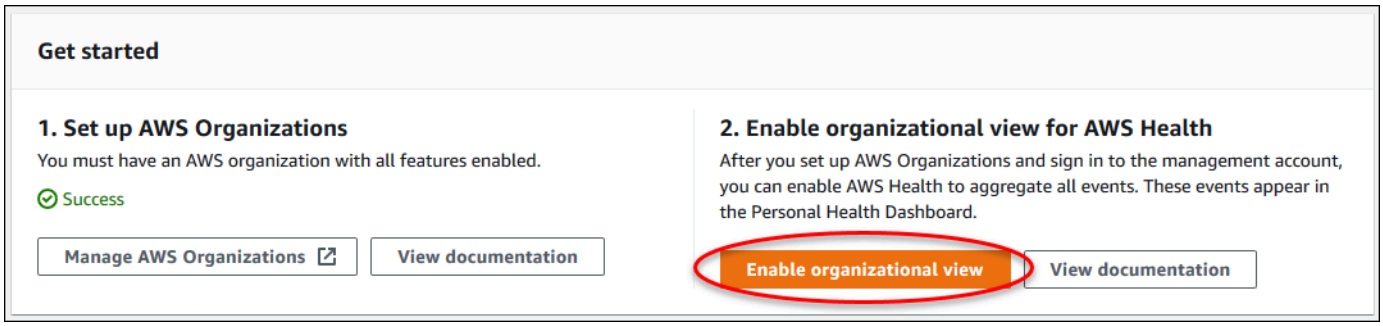
Inhalt

Organisationsansicht aktivieren (Konsole)

Sie können die Organisationsansicht über dieAWS Health Konsole aktivieren. Sie müssen sich beim Verwaltungskonto IhrerAWS Organisation anmelden.

So zeigen Sie dasAWS Health Dashboard für Ihre Organisation an

1. Öffne deinAWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Your organization health die Option Configurations aus.
3. Wählen Sie auf der Seite Organisationsansicht aktivieren die Option Organisationsansicht aktivieren aus.



4. (Optional) Wenn Sie Änderungen an IhrenAWS Organisationen vornehmen möchten, z. B. Organisationseinheiten (OUs) erstellen möchten, wählen Sie VerwaltenAWS Organizations.

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

Hinweise

- Das Aktivieren dieser Funktion ist ein asynchroner Prozess, der einige Zeit in Anspruch nimmt. Je nach Anzahl der Konten in Ihrer Organisation kann das Laden der Konten einige Minuten dauern. Du kannst dieAWS Health Konsole später verlassen und nachschauen.
- Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den DescribeHealthServiceStatusForOrganizationAPI-Vorgang aufrufen, um den Status des Prozesses zu überprüfen.
- 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. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Health.

Ereignisse aus der Organisationsansicht anzeigen (Konsole)

Nachdem Sie die Organisationsansicht aktiviert haben,AWS Health zeigt Gesundheitsereignisse für alle Konten in Ihrer Organisation an.

Wenn ein Konto Ihrer Organisation beitritt, fügt das Konto AWS Health automatisch der Organisationsansicht hinzu. 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 ab dem Datum der Schließung Ihres Administratorkontos. Am Ende des 90-Tage-Zeitraums löscht 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 AWS die Richtliniendaten beibehält, weist AWS das Konto als Service-Administrator erneut zu, wenn Sie das geschlossene Konto wieder eröffnen. Die Service-Richtliniendaten für das Konto werden wiederhergestellt.
- Weitere Informationen finden Sie unter Schließen eines Kontos.

Important

Für Kunden in den AWS GovCloud (US)-Regionen:

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

Note

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

Sie können Ereignisse in der Organisationsansicht auf den folgenden Seiten anzeigen:.

Themen

Offene und aktuelle Ausgaben

Auf der Registerkarte Offene und aktuelle Probleme können Sie Ereignisse einsehen, die sich auf IhreAWS Infrastruktur auswirken könnten, z. B. Änderungen anAWS-Services und Ressourcen, die sich auf Ihre Organisation auswirken.

So zeigen Sie Ereignisse an der Organisationsansicht

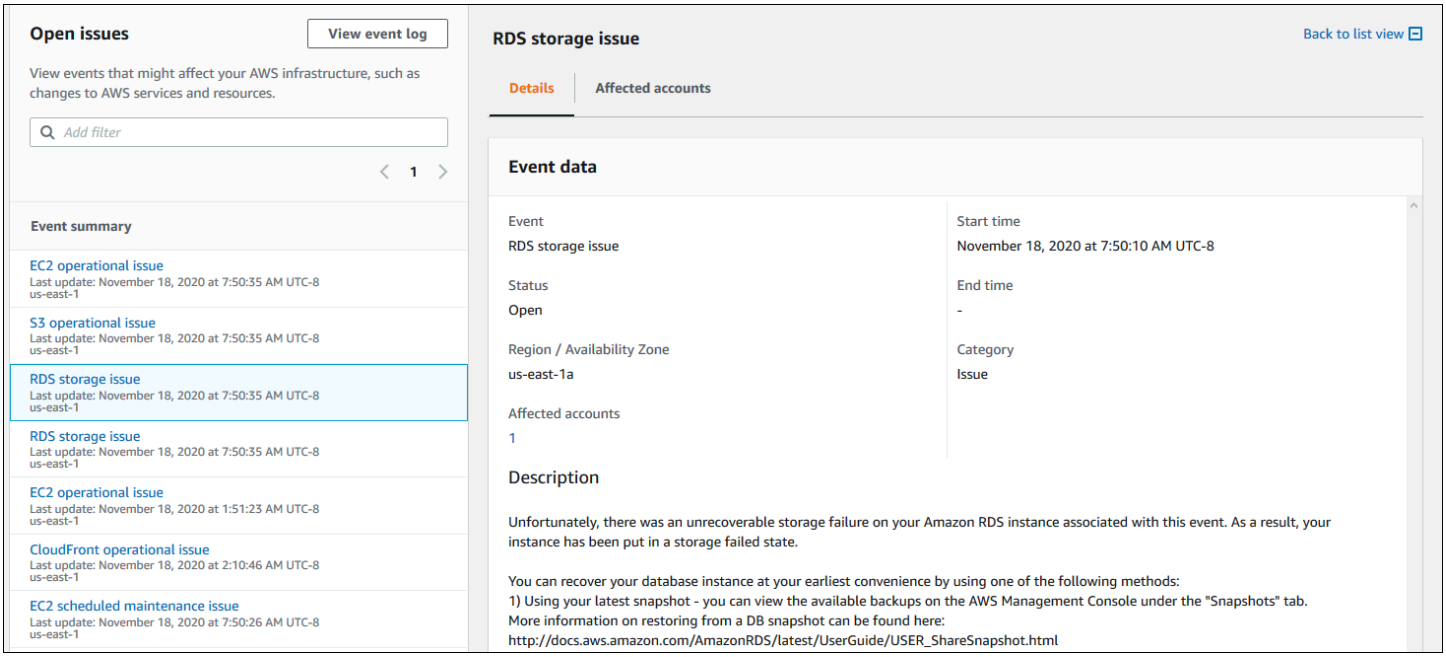
1. Öffne deinAWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Ihr Unternehmen die Option Offene und aktuelle Probleme aus, um die kürzlich gemeldeten Ereignisse anzuzeigen.

3. Wählen Sie ein Ereignis aus. Auf der Registerkarte Details können Sie die folgenden Informationen zur Veranstaltung überprüfen:

   - Event name (Ereignisname)
   - Status
   - Region/Availability Zone
   - Betroffene Konten
   - Start time (Startzeit)
   - Endzeit
   - Kategorie
   - Beschreibung

Example : Offene Themen für die Organisationsansicht

Das folgende Amazon Relational Database Service (Amazon RDS) -Ereignis wird auf der Registerkarte Offene und aktuelle Probleme in der Organisationsansicht angezeigt und betrifft ein Konto in der Organisation.



Geplante Änderungen

Verwenden Sie den Tab Geplante Änderungen, um bevorstehende Ereignisse anzuzeigen, die sich auf Ihre Organisation auswirken könnten. Diese Ereignisse können geplante Wartungsaktivitäten für Dienstleistungen beinhalten.

Andere Benachrichtigungen

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

Ereignisprotokoll

Sie können auch die Registerkarte „Ereignisprotokoll“ verwenden, umAWS Health Ereignisse für die organisatorische Ansicht anzuzeigen. Das Layout und das Verhalten der Spalten ähneln denen der Registerkarte „Offen“ und „Aktuelle Probleme“, mit der Ausnahme, dass die Registerkarte „Ereignisprotokoll“ zusätzliche Spalten und Filteroptionen enthält, z. B. die Kategorie „Ereignis“, „Status“ und „Startzeit“.

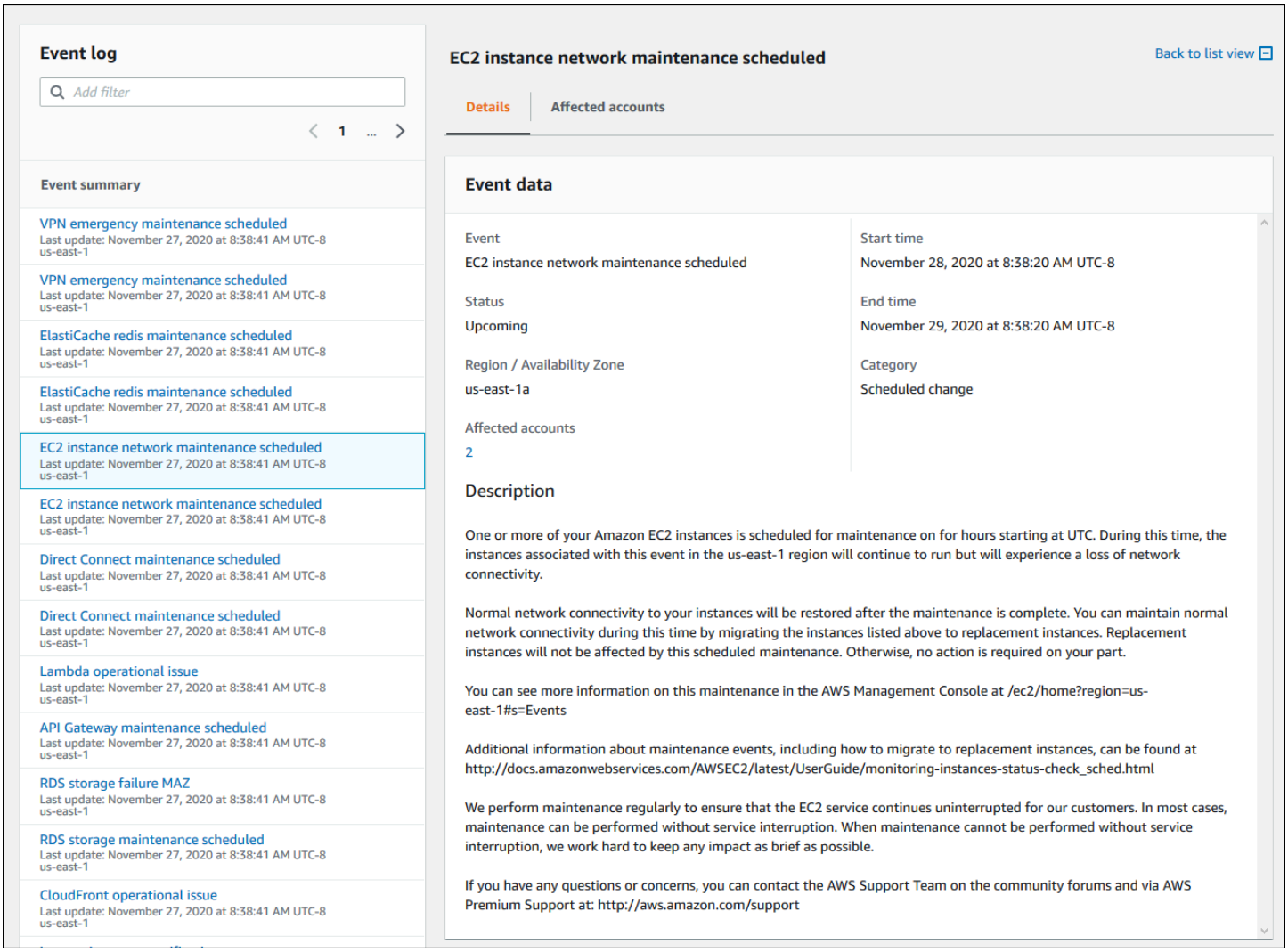
So zeigen Sie Ereignisse in der Organisationsansicht auf der Registerkarte Ereignisprotokoll an

1. Öffne deinAWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Your organization health die Option Event Log aus.
3. Wählen Sie unter Ereignisprotokoll den Namen des Ereignisses aus. Sie können die folgenden Informationen zur Veranstaltung überprüfen:

   - Event name (Ereignisname)
   - Status
   - Region/Availability Zone
   - Betroffene Konten
   - Start time (Startzeit)
   - Endzeit
   - Kategorie
   - Beschreibung

Example : Registerkarte „Ereignisprotokoll“ zur organisatorischen Ansicht

Das folgende Beispiel für ein Amazon DynamoDB DynamoDB-Ereignis (DynamoDB) wird auf der Registerkarte „Ereignisprotokoll“ angezeigt und betrifft zwei Konten in der Organisation.

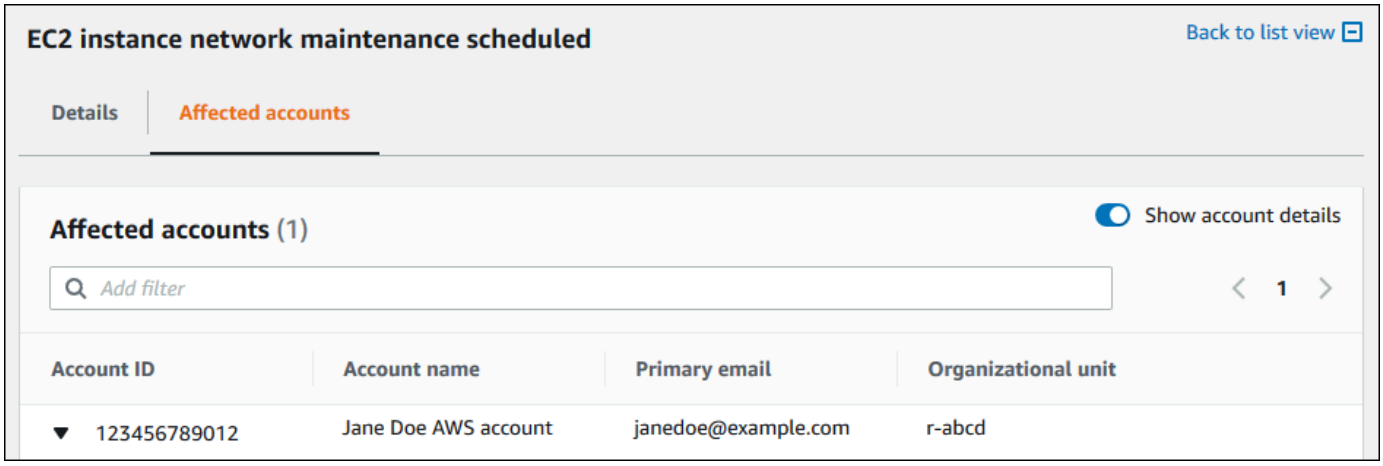


Betroffene Konten und Ressourcen anzeigen (Konsole)

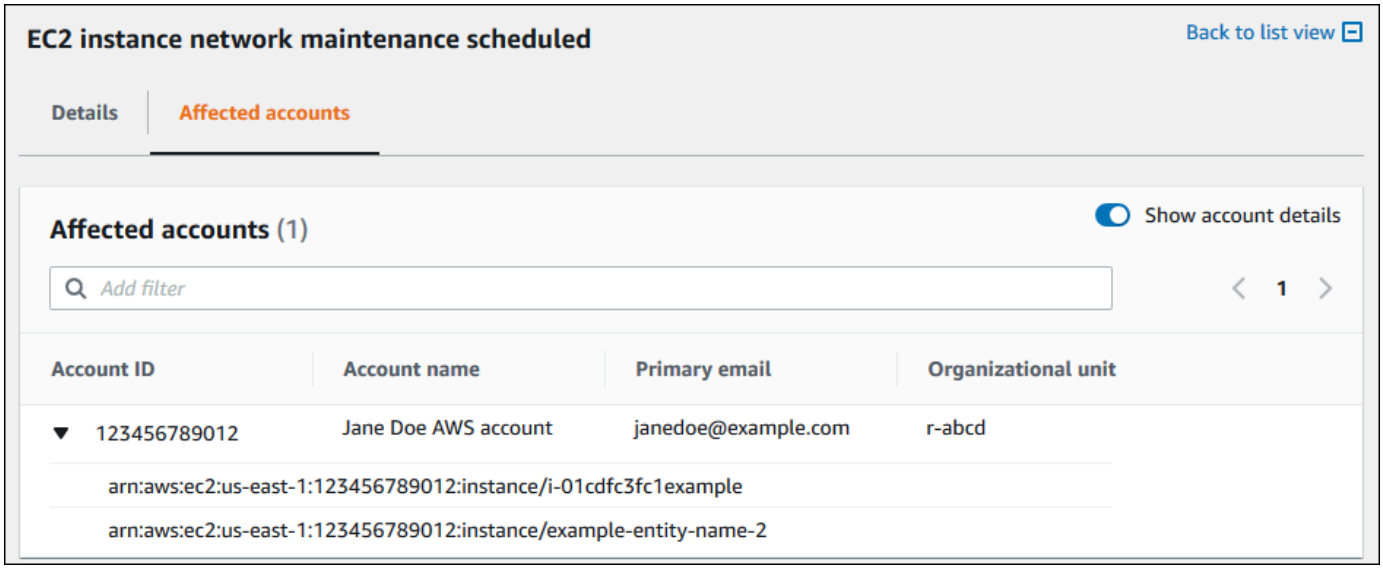
Unter Gesundheit Ihrer Organisation können Sie die Konten in Ihrer Organisation einsehen, die von dem Ereignis betroffen sind, sowie alle zugehörigen Ressourcen. Beispielsweise können bei einer bevorstehenden Veranstaltung die Wartung von Amazon Elastic Elastic Elastic Elastic Elastic Elastic Elastic Elastic Compute Compute Cloud (Amazon EC2 EC2 Instance-Typ für die Anwendungsausführung) 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. Öffne deinAWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Ihre Organisationsansicht 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)
   - Primärer Knoten
   - 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, wählen Sie Konto-ID und geben Sie dann die Konto-ID ein. Sie können jeweils nur eine Konto-ID gleichzeitig eingeben.

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

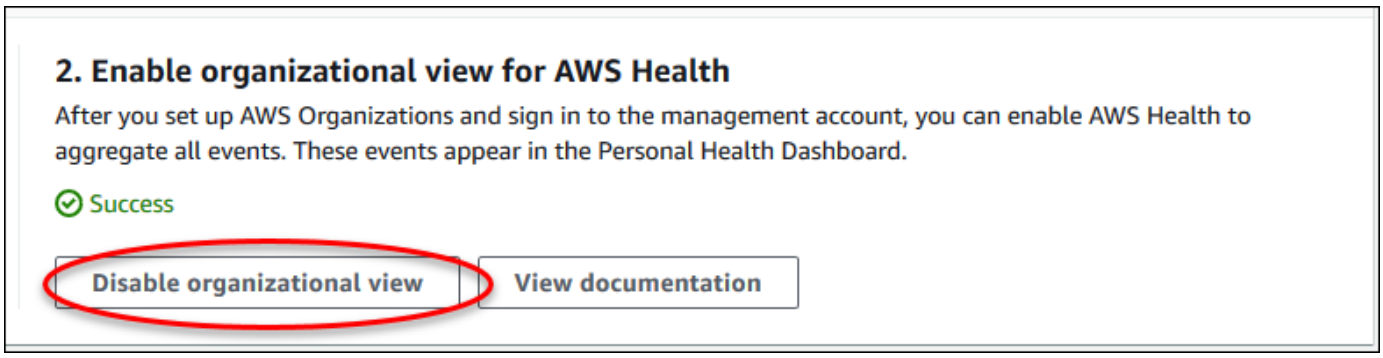
Organisationsansicht deaktivieren (Konsole)

Wenn Sie Ereignisse für Ihre Organisation nicht aggregieren möchten, können Sie diese Funktion im Verwaltungskonto deaktivieren.

AWS Healthbeendet die Aggregation von Ereignissen für alle anderen Konten in Ihrer Organisation. Sie können sich weiterhin frühere Ereignisse Ihrer Organisation ansehen, bis sie gelöscht werden.

So deaktivieren Sie die Organisationsansicht

1. Öffne deinAWS Health Dashboard unter https://health.aws.amazon.com/health/home.
2. Wählen Sie im Navigationsbereich unter Your organization health die Option Configurations aus.
3. Wählen Sie auf der Seite Organisationsansicht aktivieren die Option Organisationsansicht deaktivieren aus.



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

Organisatorische Ansicht (CLI)

Sie können die Funktion zur Organisationsansicht auch über dieAWS Command Line Interface(AWS CLI) statt derAWS HealthKonsole. Wenn Sie die Konsole verwenden möchten, lesen Sie Organisationsansicht aktivieren (Konsole).

> **Note**
>
> Wenn Sie Benutzern Zugriff auf das Verwaltungskonto für die Funktion zur Organisationsansicht gewähren möchten, müssen diese über Berechtigungen verfügen, wie z. B.AWSHealthFullAccessPolitik. Weitere Informationen finden Sie unter AWS Health Beispiele für identitätsbasierte Richtlinien.

Inhalt

Organisationsansicht (CLI) aktivieren

Sie können die Organisationsansicht aktivieren, indem Sie denEnableHealthServiceAccessForOrganizationAPI-Betrieb.

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

> **Note**
>
> - Du musst eine habenGeschäft,Einstiegsrampe für Unternehmen, oderUnternehmenUnterstützungsplan zum Anrufen derAWS HealthAPI.
> - Sie müssen den Endpunkt 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 derEnableHealthServiceAccessForOrganizationAPI-Betrieb.

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Sie können das AWS-SDK for Java Version 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`AWSServiceRoleForHealth_Organizations` Rolle im Zusammenhang mit Dienstleistungenmit dem`Health_OrganizationsServiceRolePolicy` AWSDie verwaltete Richtlinie wird auf das Verwaltungskonto in der Organisation angewendet.

> **Note**
>
> Das Aktivieren dieser Funktion ist ein asynchroner Prozess, der einige Zeit in Anspruch nimmt. Du kannst die anrufenDescribeHealthServiceStatusForOrganizationVorgang, um den Status des Prozesses zu überprüfen.

Ereignisse aus der Organisationsansicht anzeigen (CLI)

Nachdem Sie diese Funktion aktiviert haben, beginnt AWS Health mit der Aufnahme 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 nimmt keine Ereignisse auf, die in Ihrer Organisation aufgetreten 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 ab dem Datum der Schließung Ihres Administratorkontos. Am Ende des 90-Tage-Zeitraums löscht AWS dauerhaft alle Richtliniendaten für das Konto.

- Zum Aufbewahren von Erkenntnissen für mehr als 90 Tage können Sie die Richtlinien archivieren. Sie können eine benutzerdefinierte Aktion auch mit einem verwendenEventBridgeRegel zum Speichern der Ergebnisse in einem S3-Bucket.
- Solange AWS die Richtliniendaten beibehält, weist AWS das Konto als Service-Administrator erneut zu, wenn Sie das geschlossene Konto wieder eröffnen. Die Service-Richtliniendaten für das Konto werden wiederhergestellt.
- Weitere Informationen finden Sie unterEin Konto schließen.

> **Important**
>
> Für Kunden in den AWS GovCloud (US)-Regionen:
>
> - Bevor Sie Ihr Konto schließen, sichern Sie die Kontoressourcen und löschen Sie sie anschließend. Nach dem Schließen des Kontos haben Sie keinen Zugriff mehr darauf.

Sie können die AWS Health-API-Operationen verwenden, um Ereignisse aus der Organisationsansicht 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
```

Weitere AWS Health-API-Operationen finden Sie im folgenden Abschnitt.

Organisationsansicht (CLI) deaktivieren

Sie können die Organisationsansicht deaktivieren, indem Sie denDisableHealthServiceAccessForOrganizationAPI-Betrieb.

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 die Organisationen verwendenDeaktiviereAWSServiceAccessAPI-Betrieb. Nachdem Sie diesen Vorgang aufgerufen haben, stoppt AWS Health die Aggregation von Ereignissen für alle anderen Konten in Ihrer Organisation. Wenn Sie die AWS Health-API-Vorgänge für die Organisationsansicht aufrufen, wird AWS Health einen Fehler zurückgegeben. AWS Health aggregiert weiterhin Zustandsereignisse für Ihr AWS-Konto.

Nachdem Sie diese Funktion deaktiviert haben, werden Ereignisse aus Ihrer Organisation nicht mehr von AWS Health aggregiert. Die mit dem Dienst verknüpfte Rolle verbleibt jedoch im Verwaltungskonto, bis Sie sie über dasAWS Identity and Access Management(IAM) -Konsole, IAM-API oderAWS CLI. Weitere Informationen finden Sie unterLöschen einer dienstverknüpften Rollein derIAM-Benutzerhandbuch.

AWS Health-API-Operationen für die Organisationsansicht

Sie können die folgenden AWS Health-API-Operationen für die Organisationsansicht verwenden:

- DescribeEventsForOrganization— Gibt zusammenfassende Informationen über Ereignisse in der gesamten Organisation zurück.
- DescribeAffectedAccountsForOrganization— Gibt eine Liste vonAWSKonten in der Organisation, die von dem angegebenen Ereignis betroffen sind.
- DescribeEventDetailsForOrganization— Gibt detaillierte Informationen zu den angegebenen Ereignissen für ein oder mehrere Konten in der Organisation zurück.
- DescribeAffectedEntitiesForOrganization— Gibt eine Liste von Entitäten zurück, die von einem oder mehreren Ereignissen für ein oder mehrere Konten in einer Organisation betroffen waren.

Sie können die folgenden Operationen verwenden, um es zu aktivieren oder zu deaktivieren:AWS Healthaus der Zusammenarbeit mit Organisationen:

- EnableHealthServiceAccessForOrganization— ZuschüsseAWS HealthErlaubnis zur Interaktion mit Organisationen und wendet die SLR auf das Verwaltungskonto in der Organisation an.
- DisableHealthServiceAccessForOrganization— Widerruft die Erlaubnis fürAWS Healthum mit Organisationen zu interagieren.
- DescribeHealthServiceStatusForOrganization— Gibt Statusinformationen darüber zurück, obAWS Healthist für Ihre Organisation aktiviert.

Sie müssen über einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan verfügen, um diese API-Operationen aufrufen zu können. Wenn Sie die Operationen `DescribeEventForOrganization` und `DescribeAffectedAccountsForOrganization` von einem Konto aus aufrufen, das mindestens über einen Business-Supportplan verfügt, können Sie unabhängig von der Supportstufe der einzelnen Konten Informationen zu jedem Konto in der Organisation zurückgeben. Sehen Sie sich die folgenden Beispiele an.

Example Beispiel: Eine Organisation mit Konten, die über Business- und Developer-Support-Pläne verfügen

- Sie haben drei Konten in Ihrer Organisation. Das Verwaltungskonto hat einen Business-Support-Plan und die anderen beiden Konten haben einen Entwickler-Supportplan.
- Du rufst die`DescribeEventForOrganization`API-Vorgang vom Verwaltungskonto oder von einem Konto aus, das die Rolle mit den erforderlichen Berechtigungen übernehmen kann.
- AWS Health gibt Informationen für alle drei Konten zurück.

Wenn du den anrufst`DescribeEventDetailsForOrganization`und`DescribeAffectedEntitiesForOrganizati` Operationen von einem Konto aus, das mindestens über einen Business-Support-Plan verfügt. Sie können nur Informationen über Konten in der Organisation zurückgeben, die über einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan verfügen.

Example Beispiel: Eine Organisation mit Konten, die über ein Enterprise-, Business- und Developer-Support-Paket verfügen

- Sie haben fünf Konten in Ihrer Organisation. Das Verwaltungskonto hat einen Enterprise-Support-Plan, zwei Konten haben einen Business-Supportplan und zwei Konten haben einen Entwickler-Supportplan.
- Du rufst die`DescribeEventDetailsForOrganization`API-Betrieb vom Verwaltungskonto aus.

- AWS Health gibt nur Informationen für die Konten zurück, die über einen Enterprise- oder Business-Support-Plan verfügen. Die Konten mit einem Developer-Support-Plan werden in `failedSet` der Antwort angezeigt.

Organisationsansicht des delegierten Administrators

MitAWS Health, können Sie die Funktion für delegierte Administratoren von nutzenAWS Organizationsdas ermöglicht einem anderen Konto als dem Verwaltungskonto die aggregierte AnsichtAWS HealthEreignisse auf derAWS HealthArmaturenbrettoder programmgesteuert über dieAWS HealthAPI. Die Funktion für delegierte Administratoren bietet verschiedenen Teams die Flexibilität, Gesundheitsereignisse in Ihrem gesamten Unternehmen einzusehen und zu verwalten. Es ist einAWSBewährte Sicherheitspraxis, um Verantwortlichkeiten nach Möglichkeit außerhalb des Verwaltungskontos zu delegieren.

Inhalt

Registrieren Sie einen delegierten Administrator 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 denRegisterDelegatedAdministratorAPI-Betrieb. Nachdem Sie die Mitgliedskonten registriert haben, sind sie delegierte Administratorkonten und können auf dieAWS Healthorganisatorische Sicht aus derAWS HealthArmaturenbrett. Wenn das Konto einen hatGeschäft,Einstiegsrampe für Unternehmen, oderUnternehmenSupportplan, dann können die delegierten Administratoren denAWS HealthAPI für den Zugriff aufAWS Healthorganisatorische Sicht.

Um einen delegierten Administrator einzurichten, rufen Sie vom Verwaltungskonto in Ihrer Organisation aus den folgendenAWS Command Line Interface(AWS CLI) -Befehl. Sie können diesen Befehl vom Verwaltungskonto oder von einem Konto aus verwenden, das die Rolle übernehmen kann, mit den erforderlichenAWS Identity and Access Managementberechtigungen. Ersetzen Sie im folgenden BeispielbefehlKONTO-IDmit der Mitgliedskonto-ID, die Sie registrieren möchten, zusammen mit derAWS HealthServicechef „health.amazonaws.com“.

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

Nachdem ein delegierter Administrator registriert wurde, haben Sie Einblick in alleAWS HealthEreignisse, die Konten in Ihrer gesamten Organisation betreffen. Sie können historische Ereignisse der letzten 90 Tage oder seit der ersten Aktivierung der Funktion „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.

Entfernen Sie einen delegierten Administrator aus Ihrer Organisationsansicht

Um einem delegierten Administrator den Zugriff zu entziehen, rufen Sie denDeregisterDelegatedAdministratorAPI-Betrieb.

Rufen Sie vom Verwaltungskonto Ihrer Organisation aus Folgendes aufAWS CLIBefehl zum Entfernen eines Mitgliedskontos als delegierter Administrator. Ersetzen Sie im folgenden BeispielbefehlKONTO-IDmit der Mitgliedskonto-ID, die Sie entfernen möchten.

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

AWS Health Ereignisse mit Amazon überwachen 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 einleiten, Benachrichtigungen senden, Korrekturmaßnahmen ergreifen oder andere Aktionen ausführen. Sie können es beispielsweise verwenden, AWS Health um E-Mail-Benachrichtigungen zu erhalten, wenn Sie über AWS Ressourcen verfügen, für AWS-Konto die Updates geplant sind, z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances.

Hinweise

- AWS Health führt Ereignisse nach bestem Wissen und Gewissen durch. Es kann nicht immer garantiert werden, dass Veranstaltungen zugestellt werden EventBridge.
- Alle EventBridge Regeln, die Sie erstellen, können nur Benachrichtigungen für Sie erhalten AWS-Konto. Informationen zum Empfangen von Organisationsereignissen für andere Konten innerhalb Ihres AWS Organizations Accounts finden Sie unter Zusammenfassen von AWS Health Ereignissen mithilfe der Organisationsansicht und delegierter Administratorzugriff.

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

- AWS Lambda Funktionen
- Amazon-Kinesis-Data-Streams
- Amazon-Simple-Queue-Service-(Amazon-SQS)-Warteschlangen
- Integrierte Ziele (z. B. CloudWatch Alarmaktionen)
- Amazon Simple Notification Service (Amazon SNS)-Themen

Sie können beispielsweise eine Lambda-Funktion verwenden, um eine Benachrichtigung an einen Slack-Channel weiterzuleiten, wenn ein AWS Health Ereignis eintritt. Oder Sie können Lambda

verwenden, EventBridge um benutzerdefinierte Text- oder SMS-Benachrichtigungen mit Amazon SNS zu senden, wenn ein AWS Health Ereignis eintritt.

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

Themen

Über uns AWS-Regionen für AWS Health

Sie müssen für jede Region, für die Sie AWS Health Ereignisse empfangen möchten, eine EventBridge Regel erstellen. Wenn Sie keine Regel erstellen, erhalten Sie keine Ereignisse. Um beispielsweise Ereignisse aus der Region USA West (Oregon) zu empfangen, müssen Sie eine Regel für diese Region erstellen.

Die Einrichtung einer zusätzlichen Regel in einer Backup-Region erhöht die Widerstandsfähigkeit Ihrer Workflows, falls Ihre Hauptregel von einem laufenden Ereignis betroffen sein sollte. Öffentliche Ereignisse für AWS Health werden gleichzeitig sowohl an die betroffene Region als auch an eine Backup-Region gesendet. Weitere Informationen finden Sie unter Über öffentliche Veranstaltungen für AWS Health. Für alle Regionen in der AWS-Standardpartition können Sie eine Regel in USA West (Oregon) als Backup einrichten, um weiterhin Ereignisse zu empfangen, auch wenn Ihre primäre Region von einem anhaltenden Problem betroffen ist. Die Backup-Region für die Region USA West (Oregon) ist die Region USA Ost (Nord-Virginia).

Wenn Sie beispielsweise Ereignisse in der Region Europa (Frankfurt) überwachen und diese Region vorübergehend nicht verfügbar ist, AWS Health wird das Ereignis auch in die Region USA West (Oregon) übertragen. Als Nächstes sendet Ihre EventBridge Backup-Regel das Ereignis an die von Ihnen angegebenen Ziele. Gehen Sie wie folgt vor, um eine Backup-Regel für die Region USA West (Oregon) zu erstellen, Eine EventBridge Regel erstellen für AWS Health und verwenden Sie diese.

Einige AWS Health Ereignisse sind nicht regionsspezifisch. 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) für die primäre Region und die Region USA West (Oregon) als Backup-Region erstellen.

Um globale Ereignisse in der Region zu empfangen AWS GovCloud (US), müssen Sie eine Regel in der Region AWS GovCloud (USA West) erstellen.

Über öffentliche Veranstaltungen für AWS Health

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

- Kontospezifische Ereignisse wirken sich auf Ihr Konto und Ihre Ressourcen aus, z. B. ein Ereignis, das Sie über ein erforderliches Update für eine Amazon EC2 EC2-Instance informiert, oder andere geplante Änderungsereignisse.
- 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 auch keine öffentlichen Informationen darüber.

> **Important**
>
> Um beide Ereignistypen zu empfangen, muss Ihre Regel den `"source": [ "aws.health"]` Wert verwenden. Platzhalter, z. B. stimmen `"source": [ "aws.health*"]` nicht mit dem Muster überein, nach dem nach Ereignissen gesucht werden soll.

Wenn Sie öffentliche Ereignisse von 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 eine Backup-Region gesendet. Es wird empfohlen, AWS Health Ereignisse mithilfe von EventARN und CommunicationID zu deduplizieren, da diese für AWS Health Nachrichten, die an die Backup-Region gesendet werden, konsistent bleiben.

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

Beispiel: Öffentliche Veranstaltungen für Amazon Elastic Compute Cloud

Das folgende Ereignis zeigt ein Betriebsproblem für Amazon EC2 in der Region USA Ost (Nord-Virginia).


```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [
            {
                "latestDescription": "We are investigating increased API Error rates
 and Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
                "language": "en_US"
            }
        ],
        "page": "1",
        "totalPages": "1",
```

```
        "affectedAccount":"123456789012",

    }
}
```

Event-Prozessor für AWS Health

Wenn Sie AWS Incident Detection and Response für Ihr Konto verwenden, müssen Sie die `AWSServiceRoleForHealth_EventProcessor` dienstbezogene Rolle in Ihrem Konto installieren.

Diese Rolle vertraut darauf, dass der `event-processor.health.amazonaws.com` Dienstprinzipal die Rolle übernimmt. Dieser Rolle ist die `AWSHealth_EventProcessorServiceRolePolicy` AWS verwaltete Richtlinie zugeordnet. In dieser Richtlinie sind die Berechtigungen aufgeführt, die die Rolle ausführen kann, z. B. das Anrufen anderer Benutzer AWS-Services für Sie.

Diese Rolle erstellt dann eine von Amazon EventBridge verwaltete Regel in Ihrem Konto. Die Regel ist benannt`AWSHealthEventProcessor-DO-NOT-DELETE`. Bei dieser Regel handelt es sich um die erforderliche Infrastruktur für Ihr Konto, EventBridge sodass Informationen zur Änderung des Alarmstatus von Ihrem Konto aus übermittelt werden können AWS Health.

Ähnliche Informationen

Für weitere Informationen schauen Sie in den folgenden Themen:

- Verwenden von serviceverknüpften Rollen für AWS Health
- AWS verwaltete Richtlinie: AWSHealth_EventProcessorServiceRolePolicy

Eine EventBridge Regel erstellen für AWS Health

Sie können eine EventBridge Regel erstellen, um über AWS Health Ereignisse in Ihrem Konto benachrichtigt zu werden. Bevor Sie Veranstaltungsregeln für erstellen AWS Health, gehen Sie wie folgt vor:

- Machen Sie sich mit Ereignissen, Regeln und Zielen in vertraut EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch und Neu EventBridge — Änderungen an Ihren AWS Ressourcen nachverfolgen und darauf reagieren.
- Erstellen Sie die Ziele für die Ereignisregeln.

Um eine EventBridge Regel zu erstellen für AWS Health

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite. Wählen Sie die Region aus, in der Sie Ereignisse verfolgen möchten. AWS Health
3. Wählen Sie im Navigationsbereich Rules aus.
4. Wählen Sie Regel erstellen aus.
5. Geben Sie auf der Seite Define rule detail (Regeldetail festlegen) einen Namen und eine Beschreibung für Ihre Regel ein.
6. Behalten Sie die Standardwerte für Event Bus und Regeltyp bei und wählen Sie dann Weiter aus.
7. Wählen Sie auf der Seite „Event-Pattern erstellen“ für Event-Quelle die Optionen AWS Events und EventBridge Partnerevents aus.
8. Wählen Sie unter Ereignismuster für Ereignisquelle die Option aus AWS-Services.
9. Wählen Sie unter Ereignismuster für AWS-Servicedie Option Health aus.
10. Wählen Sie für Ereignistyp eine der folgenden Optionen aus.
    - Spezifische Ereignisse wegen Gesundheitsmissbrauchs — Erstellen Sie eine Regel für AWS Health Ereignisse, bei denen das Wort `Abuse` im Namen des Ereignistyps vorkommt.
    - Spezifische Gesundheitsereignisse — Erstellen Sie eine Regel für Ereignisse für ein bestimmtes AWS-Service Ereignis, z. B. Amazon EC2.
11. Sie können „Beliebiger Service“ oder „Spezifische Services“ wählen. Wenn Sie sich für einen bestimmten Dienst entschieden haben, wählen Sie eine der folgenden Optionen:
    - Wählen Sie Beliebige Ereignistypkategorie, um eine Regel zu erstellen, die für alle Ereignistypkategorien gilt.
    - Wählen Sie Bestimmte Ereignistypkategorie (n) und wählen Sie dann einen Wert aus der Liste aus, z. B. Problem, AccountNotification oder scheduledChange.

> **Tip**
>
> - Um alle AWS Health Ereignisse für einen bestimmten Service zu überwachen, empfehlen wir, dass Sie die Kategorie Beliebiger Ereignistyp und Beliebige Ressource auswählen. Dadurch wird sichergestellt, dass Ihre Regel alle AWS Health Ereignisse, einschließlich neuer Ereignistypcodes, für den angegebenen Dienst überwacht. Eine Beispielregel finden Sie unter Alle Amazon EC2 EC2-Ereignisse.

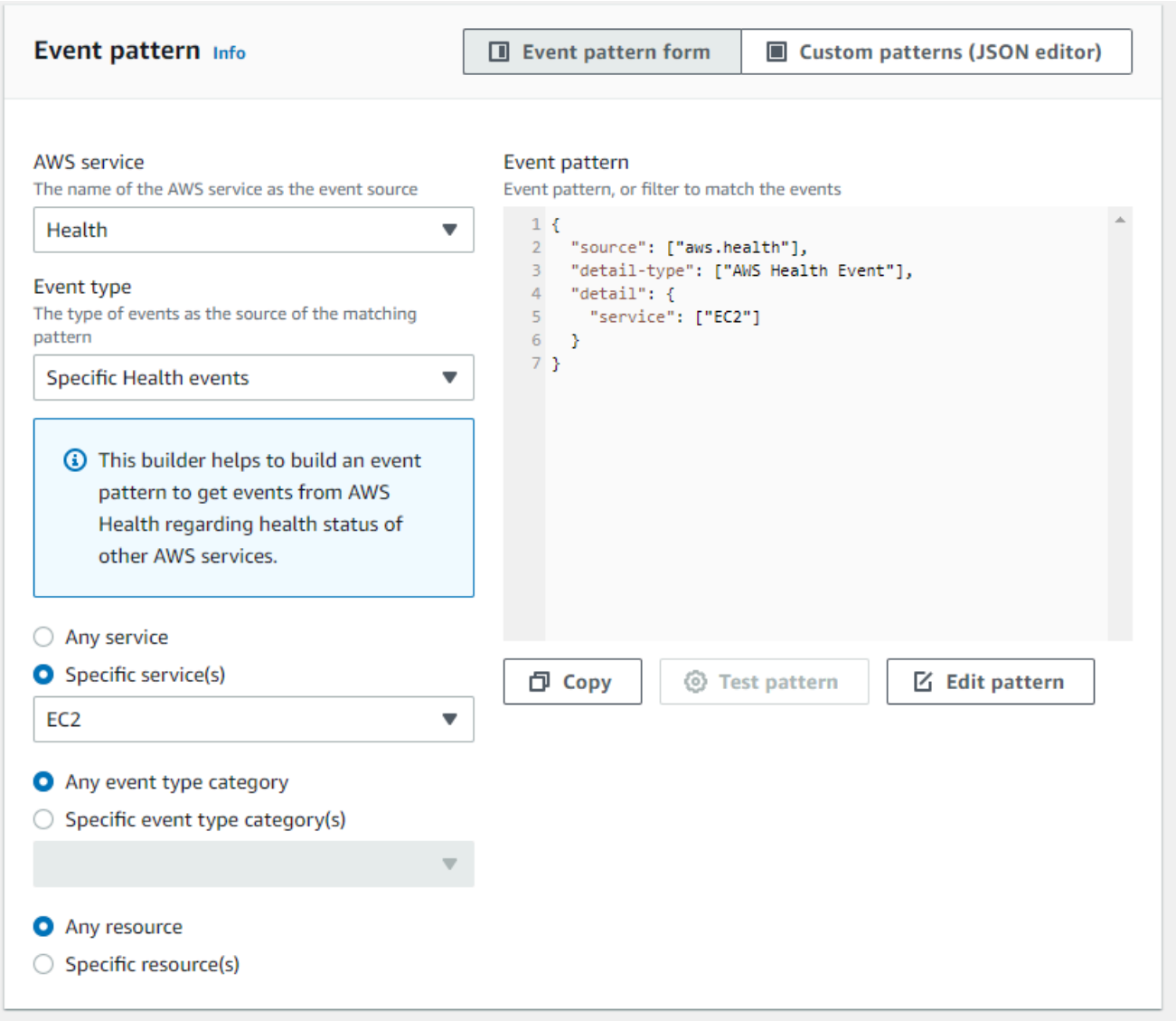
- Sie können eine Regel erstellen, um mehr als eine Service- oder Ereignistypkategorie zu überwachen. Dazu müssen Sie das Ereignismuster für die Regel manuell aktualisieren. Weitere Informationen finden Sie unter Eine Regel für mehrere Dienste und Kategorien erstellen.

12. Wenn Sie eine bestimmte Service- und Ereignistypkategorie ausgewählt haben, wählen Sie eine der folgenden Optionen für Ereignistypcodes.
    - Wählen Sie Beliebiger Ereignistypcode, um eine Regel zu erstellen, die für alle Ereignistypcodes gilt.
    - Wählen Sie Spezifische Codes für Ereignistypen und wählen Sie dann einen oder mehrere Werte aus der Liste aus. Dadurch wird eine Regel erstellt, die nur für bestimmte Ereignistypcodes gilt. Wenn Sie beispielsweise **`AWS_EC2_INSTANCE_STOP_SCHEDULED`**und wählen **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**, gilt Ihre Regel nur für diese Ereignisse, wenn sie in Ihrem Konto auftreten.
13. Wählen Sie eine der folgenden Optionen für die betroffenen Ressourcen.
    - Wählen Sie Beliebige Ressource, um eine Regel zu erstellen, die für alle Ressourcen gilt.
    - Wählen Sie Bestimmte Ressource (n) und geben Sie die IDs einer oder mehrerer Ressourcen ein. Sie können beispielsweise eine Amazon EC2 EC2-Instance-ID wie *`I-exampleA1B2C3DE4 angeben, um nach Ereignissen`* zu suchen, die nur diese Ressource betreffen.
14. Überprüfen Sie Ihre Regeleinrichtung, sodass sie Ihren Anforderungen an die Ereignisüberwachung entspricht.
15. Wählen Sie Weiter aus.
16. Wählen Sie auf der Seite Ziel (e) auswählen den Zieltyp aus, den Sie für diese Regel erstellt haben, und konfigurieren Sie dann alle zusätzlichen Optionen, die für diesen Typ erforderlich sind. Beispielsweise können Sie das Ereignis an eine Amazon-SQS-Warteschlange oder ein Amazon-SNS-Thema senden.
17. Wählen Sie Weiter aus.
18. (Optional) Fügen Sie auf der Seite Configure tags (Tags konfigurieren) beliebige Tags hinzu und wählen Sie Next (Weiter).
    - Hinweis: Tags werden derzeit nicht von der aws.health-Quelle in gesendet. EventBridge

19. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die eingerichteten Regeln, um sicherzustellen, dass sie den Anforderungen Ihrer Ereignisüberwachung entsprechen.
20. Wählen Sie Regel erstellen aus.

Example : Regel für alle Amazon EC2 EC2-Ereignisse

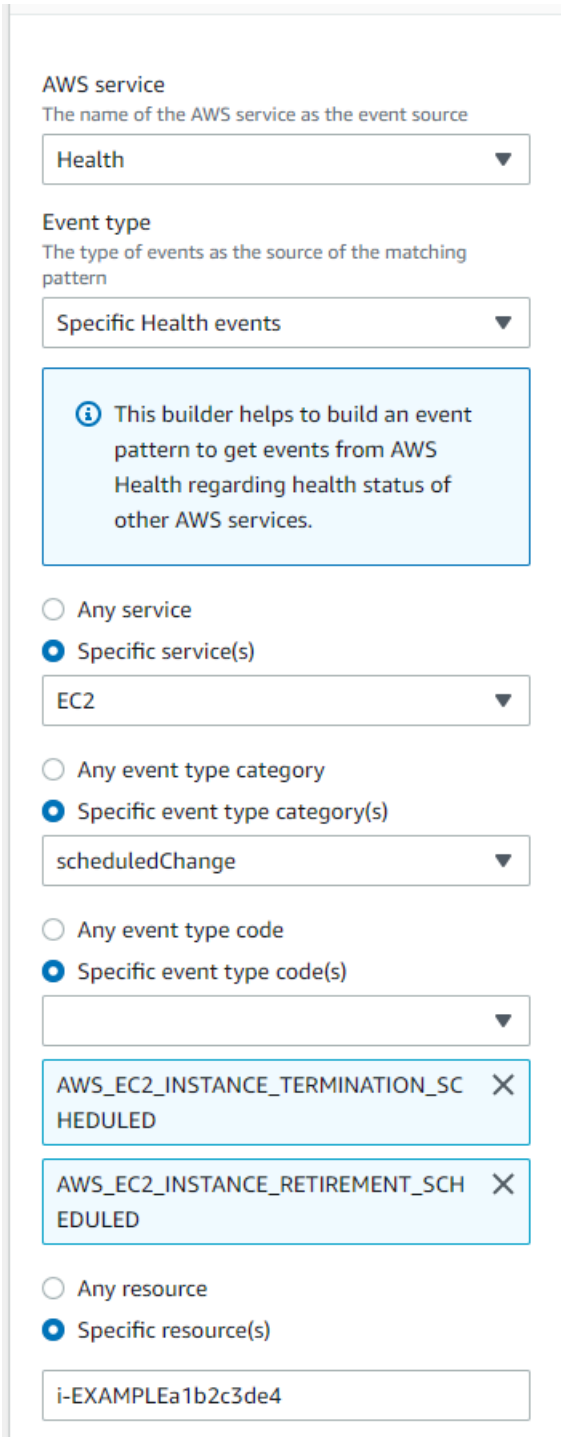
Im folgenden Beispiel wird eine Regel erstellt, sodass alle Amazon EC2 EC2-Ereignisse EventBridge überwacht werden, einschließlich der Ereignistypkategorien, Ereigniscodes und Ressourcen.



Example : Regel für bestimmte Amazon EC2 EC2-Ereignisse

Im folgenden Beispiel wird eine Regel erstellt, die Folgendes EventBridge überwacht:

- Der Amazon EC2-Service
- Die Kategorie ScheduledChange-Ereignistyp
- Der Ereignistyp kodiert für und `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- Die Instanz mit der ID `i-EXAMPLEa1b2c3de4`



Eine Regel für mehrere Dienste und Kategorien erstellen

Die Beispiele im vorherigen Verfahren zeigen Ihnen, wie Sie eine Regel für eine einzelne Service- und Ereignistypkategorie erstellen. Sie können auch eine Regel für mehrere Kategorien von Diensten und Ereignistypen erstellen. Das bedeutet, dass Sie nicht für jeden Dienst und jede Kategorie, die Sie

überwachen möchten, eine separate Regel erstellen müssen. Dazu müssen Sie das Ereignismuster bearbeiten und dann Ihre Änderungen manuell eingeben.

Verwenden Sie eine der folgenden Optionen.

Um Dienste und Kategorien für eine bestehende Regel hinzuzufügen

1. Wählen Sie in der EventBridge Konsole auf der Seite Regeln den Regelnamen aus.
2. Wählen Sie rechts oben die Option Edit (Bearbeiten) aus.
3. Wählen Sie Weiter aus.
4. Wählen Sie für Event-Muster die Option Muster bearbeiten aus und geben Sie dann Ihre Änderungen in das Textfeld ein.
5. Wählen Sie Weiter, bis Sie zur Seite „Überprüfen und aktualisieren“ gelangen.
6. Wählen Sie Regel aktualisieren, um Ihre Änderungen zu speichern.

Um Dienste und Kategorien für eine neue Regel hinzuzufügen

1. Folgen Sie den Anweisungen in Eine EventBridge Regel erstellen für AWS Health Schritt 9.
2. Anstatt einen einzelnen Dienst oder eine Kategorie aus den Listen auszuwählen, wählen Sie für Ereignismuster die Option Muster bearbeiten aus.
3. Geben Sie Ihre Änderungen in das Textfeld ein. Sehen Sie sich das folgende Beispielmuster als Modell für die Erstellung Ihres eigenen Ereignismusters an.
4. Überprüfen Sie Ihr Ereignismuster, und folgen Sie dann den weiteren Anweisungen unter Eine EventBridge Regel erstellen für AWS Health So erstellen Sie Ihre Regel.

Verwenden Sie die API oder AWS Command Line Interface (AWS CLI)

Verwenden Sie für eine neue oder bestehende Regel den PutRuleAPI-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: Mehrere Kategorien von Diensten und Ereignistypen

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

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

AWS Health Schema der Ereignisse Amazon EventBridge

Das Folgende ist das Schema für AWS Health Ereignisse. Änderungen oder Ergänzungen zur vorherigen Version des Schemas werden als „Neu“ gekennzeichnet. Nach dem Schema wird eine Beispielnutzlast bereitgestellt.

AWS Health Schema des Ereignisses

AWS Health Schema des Ereignisses

Parameter	Beschreibung	Erforderlich
Version	EventBridge Version, derzeit „0"	Ja
id	Der uniqueEventBridge Bezeichne	Ja

Parameter	Beschreibung	Erforderlich
	r für das Ereignis	
Detailtyp	Beschreibt den Detailtyp. Für AWS Health Veranstaltungen wird dies &AWS Health Event oder sein AWS Health Abuse Event	Ja
source	Die Event-Bus-Quelle. Für AWS Health Veranstaltungen wird dies sein aws.health	Ja

Parameter	Beschreibung	Erforderlich
Konto	Die accountId, an die das AWS Health Ereignis gesendet wurde. **Note** Aus organisatorischer Sicht unterscheidet sich dieser Wert von dem AffectedAccount, wenn er im Verwaltungs- oder delegierten Administratorkonto eingegangen ist.	Ja

Parameter	Beschreibung	Erforderlich
variieren	Uhrzeit, an die die Benachrichtigung gesendet wurde. EventBridge Format:`yyyy-mm-ddThh:mm:ssZ` .	Ja

Parameter	Beschreibung	Erforderlich
Region	Identifiziert den AWS-Region , an den die Benachrichtigung zugestellt wurde. **Note** Dieses Feld gibt nicht die betroffene Region für dieses AWS Health Ereignis an. Dies wird von „detail.eventRegion“ bereitgestellt.	Ja

Parameter	Beschreibung	Erforderlich
Ressourcen	Beschreibt die Liste der betroffenen Ressourcen innerhalb eines Kontos, falls es betroffene Ressourcen gibt. **Note** Dieses Feld kann leer sein, wenn keine Ressourcen referenziert werden.	Nein

Parameter	Beschreibung	Erforderlich
Detail	Dieser Abschnitt enthält alle Details der AWS Health Veranstaltung, wie unten aufgeführt.	Ja

Parameter		Beschreibung	Erforderlich
	EventARN	Eindeutiger Bezeichner für das AWS Health Ereignis für die spezifische Region, einschließlich Region und Ereignis-ID. **Note** Ein EventARN ist nicht eindeutig für ein bestimmtes Kundenkonto oder eine Region bestimmt.	Ja

Parameter		Beschreibung	Erforderlich
	Service nicht zulässig	Die von dem AWS Health Ereignis AWS-Service betroffenen Personen. Zum Beispiel Amazon EC2, Amazon Simple Storage Service, Amazon Redshift oder Amazon Relational Database Service.	Ja

Parameter		Beschreibung	Erforderlich
	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 etwa zwei Wochen vor der StartTime veröffentlicht. **Note** Alle neuen geplanten Lebenszyklusereign	Ja

Parameter		Beschreibung	Erforderlich
		isse haben den Ereignist ypAWS_{S ICE}_PLA NED_LIFE YCLE_EVE T .	
	eventTypeCategory	Der Kategorie -Code des Ereigniss es. Die möglichen Werte sind `issue`, `accountNo tificatio n` , `investiga tion` .und `scheduled Change` .	Ja

Parameter		Beschreibung	Erforderlich
	eventScopeCode	Gibt an, ob das AWS Health Ereignis kontospezifisch oder öffentlich ist. Die möglichen Wert sind `ACCOUNT_SPECIFIC` oder `PUBLIC`.	Ja

Parameter		Beschreibung	Erforderlich
	Kommunikations-ID (neu)	Eine eindeutige Kennung für diese Kommunikation für das AWS Health Ereignis. Nachrichten mit derselben CommunicationID sind mögliche Backup-Nachrichten oder Seiten eines einzelnen AWS Health Ereignisses. Diese Kennung kann zusammen mit der accountId verwendet werden, um Nachrichten zu deduplizieren.	Ja

Parameter	Beschreibung	Erforderlich
	Note In der Version der Paginierungsfunktion enthält CommunicationID die Seitenzahl, sodass die CommunicationID seitenübergreifend eindeutig bleibt, z. B. 12345678 10-1. Weitere Informationen finden Sie unter Paginierung der Ereigniss	

Parameter		Beschreibung	Erforderlich
		e auf AWS Health EventBridge.	
	startTime	Die Startzeit des Ereignisses im Format:. AWS Health `DoW, DD, MMM, YYYY, HH:MM:SS TZ` **Note** Die Startzeit für geplante Veranstaltungen kann in der future liegen.	Ja

Parameter		Beschreibung	Erforderlich
	endTime	Die Endzeit der AWS Health Veranstaltung im Format:`DoW, DD MMM YYYY HH:MM:SS TZ`. **Note** EndTime wird möglicherweise nicht für Ereignisse bereitgestellt, die in der future festgelegt werden.	Nein

Parameter		Beschreibung	Erforderlich
	lastUpdatedTime	Die letzte Aktualisierungszeit für das AWS Health Ereignis im Format:`DoW, DD MMM YYYY HH:MM:SS TZ`.	Ja

Parameter		Beschreibung	Erforderlich
	statusCode	Status des AWS Health Ereignisses. Typkategorien haben unterschiedliche Status. Die möglichen Werte für `Issue` Ereigniskategorien sind `open`, `closed` oder `upcoming` `scheduledChanges` Ereigniskategorien haben unterschiedliche Status: `Upcoming` oder `Complete`. `AccountNotifications` Ereigniskategorien haben keinen Status und	Ja

Parameter		Beschreibung	Erforderlich
		sind auf "-" gesetzt.	
	EventRegion	Die betroffene Region, die von diesem AWS Health Ereignis beschrieben wurde.	Ja
	Beschreibung des Ereignisses	Ein Abschnitt, der das AWS Health Ereignis beschreibt. Dazu gehören Felder für Sprache und Text zur Beschreibung des Ereignisses.	Ja

Parameter			Beschreibung	Erforderlich
		language	In der AWS Health Veranstaltung verwendete Sprache. Dies hängt in der Regel von der Region ab, in der die Veranstaltung veröffentlicht wird. Für die Region us-east-1 ist dies in der Regel „en_US“.	Ja

Parameter			Beschreibung	Erforderlich
		Letzte Beschreibung	Beschreibt das AWS Health Ereignis so, 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 gesamten Verlauf des	Ja

Parameter		Beschreibung	Erforderlich
		Ereignisses.	
	Event-Metadaten	Zusätzliche Event-Metadaten, die für das AWS Health Ereignis bereitgestellt werden können.	Nein

Parameter			Beschreibung	Erforderlich
		<metadata key 1>	Metadaten schlüssel, Wertzeich enfolgen „keystring1": „keyvalue1" **Note** Die Schlüssel - Wert- Paa re für Ereignism etadaten werden durch den Dienst bestimmt, der das Ereignis gesendet hat. AWS Health	Nein

Parameter			Beschreibung	Erforderlich
	Betroffene Identitäten		Ein Array, das den Ressourcenwert und den Status der betroffenen Ressourcen innerhalb dieses Ereignisses beschreibt. AWS Health	Nein
		EntityValue	Die Ressource-/Entitäts-ID	Nein
		Uhrzeit der letzten Aktualisierung (neu)	Der Zeitpunkt, zu dem dieser Ressource-/Entitätsstatus zuletzt aktualisiert wurde, im folgenden Format: `DoW, DD MMM YYYY HH:MM:SS TZ`	Nein

Parameter			Beschreibung	Erforderlich
		Status (neu)	Der Status der betroffenen Ressource/Entität. Mögliche Werte sind`IMPAIRED`, `D ,PENDING`. `RESOLVED` `UNKNOWN`	Nein

Parameter		Beschreibung	Erforderlich
	Seite (Neu)	Die Seite, für die diese Nachricht steht. Weitere Informationen finden Sie unter Paginierung der Ereignisse auf AWS Health EventBridge. **Note** Die Paginierung erfolgt nur für Ressourcen. Andere Ursachen für die Verletzung der Größenbeschränkung von 256 KB führen	Ja

Parameter		Beschreibung	Erforderlich
		dazu, dass die Kommunil tion fehlschlägt.	

Parameter		Beschreibung	Erforderlich
	Seiten insgesamt (neu)	Die Gesamtzahl der Seiten für dieses Gesundheitsereignis. Weitere Informationen finden Sie unter Paginierung der Ereignisse auf AWS Health EventBridge. **Note** Sie können damit feststellen, ob Sie alle Seiten einer mehrseitigen Mitteilung für ein Konto	Ja

Parameter	Beschreibung	Erforderlich
	erhalten haben.	

Parameter		Beschreibung	Erforderlich
	Betroffenes Konto (neu)	Dies ist die accountId des betroffen en Kontos. Note Dies kann sich vom Feld „Konto“ unterschie iden, wenn dieses Integritä tsereigni s an ein Konto gesendet wird, das Teil eines Kontos ist, AWS Organizat ions und dieses im	Ja

Parameter		Beschreibung	Erforderlich
		Verwaltungs- oder delegierten Administratorkonto empfangen wird.	

Veranstaltung im Bereich der öffentlichen Health — 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",
            "affectedAccount": "123456789012",
          }
        }
```

Kontospezifisches 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",
            "affectedAccount": "123456789012",
          }
        }
```

Kontospezifisches AWS Health Ereignis — Leistung des Amazon EC2 Instance Store-Laufwerks beeinträchtigt

```
        {
          "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-west-2::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-west-2",
            "eventDescription": [{
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }],
            "affectedEntities": [{
```

```
            "entityValue": "i-abcd1111",
          }],
          "page": "1",
          "totalPages": "1",
          "affectedAccount": "123456789012",
        }
      }
```

Paginierung der Ereignisse auf AWS Health EventBridge

AWS Health unterstützt die Paginierung von AWS Health Ereignissen, wenn die Liste der „Ressourcen“ oder „AffectedEntities“ dazu führt, dass die Nachrichtengröße die Nachrichtengrößenbeschränkung von 256 KB überschreitet EventBridge. Bisher wurde bei Überschreitung dieses Grenzwerts AWS Health nicht die vollständige Liste der Ressourcen mit Ereignissen übermittelt.

AWS Health schließt jetzt alle „Ressourcen“ und „Detail.AffectedEntities“ in die Nachricht ein. Wenn diese Liste mit „Ressourcen“ und „Detail.AffectedEntities“ 256 KB überschreitet, wird das Gesundheitsereignis in mehrere Seiten aufgeteilt und diese Seiten als AWS Health einzelne Nachrichten veröffentlicht. EventBridge Jede Seite behält den gleichen EventARN und die gleiche CommunicationID bei, sodass die Liste der „Ressourcen“ oder „Detail.AffectedEntities“ nach dem Empfang aller Seiten neu kombiniert werden kann.

Diese zusätzlichen Nachrichten können zu unnötigen Nachrichten führen, z. B. wenn die EventBridge Regel an eine für Menschen lesbare Schnittstelle wie E-Mail oder Chat gerichtet ist. Kunden mit menschenlesbaren Benachrichtigungen können einen Filter für das Feld „detail.page“ hinzufügen, um nur die erste Seite zu verarbeiten. Dadurch werden unnötige Nachrichten aus nachfolgenden Seiten entfernt.

Es sind mehrere Schemaänderungen enthalten, um den Start der Paginierung zu unterstützen. Jede CommunicationID enthält jetzt die Seitenzahl mit Bindestrich hinter der CommunicationID, auch wenn es nur eine Seite gibt. Außerdem gibt es zwei neue Felder, detail.page und detail.totalPages, die die aktuelle Seitennummer und die Gesamtzahl der Seiten für das Ereignis beschreiben. AWS Health Die in jeder paginierten Nachricht enthaltenen Informationen sind dieselben, mit Ausnahme der Liste „detail.affectedEntities“ oder „resources“. Diese Listen können rekonstruiert werden, nachdem alle Seiten empfangen wurden. Die Seiten der betroffenen Ressourcen und Entitäten sind unabhängig von der Reihenfolge.

Zusammenfassen von AWS Health Ereignissen mithilfe der Organisationsansicht und des delegierten Administratorzugriffs

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

Diese Funktion wurde entwickelt, um eine zentrale Ansicht bereitzustellen, mit der Sie AWS Health Ereignisse in Ihrer gesamten Organisation verwalten können. Durch das Einrichten einer Organisationsansicht und einer EventBridge Regel im Verwaltungskonto werden EventBridge Regeln für andere Konten in Ihrer Organisation nicht deaktiviert.

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

Empfangen von Ereignissen AWS Health mit AWS Chatbot

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 bei Ihrem AWS Health Dashboard anmelden, um mehr über das Update zu erfahren. Wenn du zum Beispiel den `AWS_EC2_INSTANCE_STOP_SCHEDULED` Ereignistyp in deinem AWS Konto beobachtest, kann das AWS Health Ereignis direkt in deinem Slack-Kanal erscheinen.

Voraussetzungen

Bevor du loslegst, musst du über Folgendes verfügen:

- Ein Chat-Client, der mit konfiguriert ist AWS Chatbot. Sie können Amazon Chime und Slack konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit AWS Chatbot im AWS Chatbot Administratorhandbuch.
- Ein Amazon SNS 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 AWS Health Ereignisse zu empfangen mit AWS Chatbot

1. Gehen Sie wie in Schritt Eine EventBridge Regel erstellen für AWS Health 13 beschrieben vor.

   a. Wenn Sie mit der Einrichtung des Ereignismusters in Schritt 13 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 Paginierung der Ereignisse auf AWS Health EventBridge.

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

   b. Wenn Sie in Schritt 14 das Ziel ausgewählt haben, wählen Sie ein SNS-Thema aus. Sie werden dasselbe SNS-Thema in der AWS Chatbot Konsole verwenden.

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

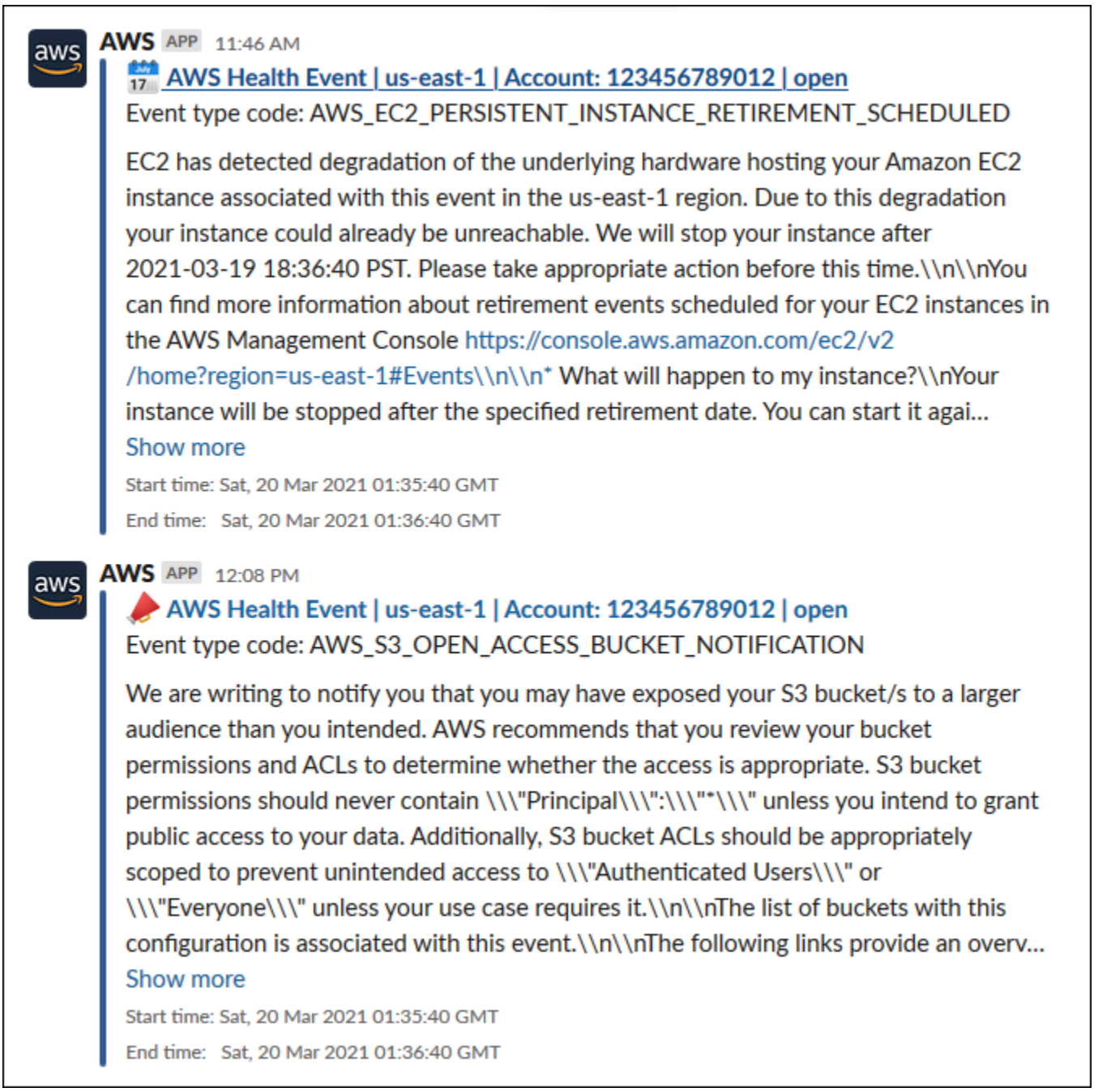
2. Navigieren Sie zur AWS Chatbot -Konsole.
3. Wähle deinen Chat-Client, z. B. den Namen deines Slack-Kanals, und wähle dann Bearbeiten.
4. Wähle im Abschnitt Benachrichtigungen — optional für Themen dasselbe SNS-Thema aus, das du in Schritt 1 angegeben hast.
5. Wählen Sie Speichern.

   Wenn AWS Health Sie ein Ereignis an senden EventBridge , das Ihrer Regel entspricht, wird das AWS Health Ereignis in Ihrem Chat-Client angezeigt.

6. Wählen Sie den Namen der Veranstaltung, um weitere Informationen in Ihrem AWS Health Dashboard zu sehen.

Example : AWS Health Ereignisse, die an Slack gesendet wurden

Im Folgenden finden Sie 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-Channel erscheinen.



Automatisieren von Aktionen für Amazon EC2 EC2-Instances

Sie können Aktionen automatisieren, die auf geplante Ereignisse für Ihre Amazon EC2 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 EC2-Instance für eine von 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 EC2-Instances zu automatisieren, müssen die Instances von Systems Manager verwaltet werden.

Weitere Informationen finden Sie unter Automating Amazon EC2 with EventBridge im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Voraussetzungen

Sie müssen eine AWS Identity and Access Management (IAM-) Richtlinie und 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 erteilt der Rolle die Erlaubnis, Aktionen in Ihrem Namen durchzuführen. Dieses Verfahren verwendet den JSON-Richtlinieneditor in der IAM-Konsole.

So erstellen Sie eine IAM-Richtlinie

1. Melden Sie sich bei der an AWS Management Console 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.

```
{
  "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 den Rollennamen auch ersetzen oder den Standardnamen verwenden. In diesem Beispiel wird *AutomationEVRole* verwendet.

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 wie ***AutomationEV RolePolicy*** und optional eine Beschreibung ein.
10. Auf der Übersichtsseite finden Sie Informationen zu den Berechtigungen, die 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 AWS Dienst zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (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 diese Rolle zuweisen möchten.
5. Wählen Sie Weiter: Berechtigungen aus.
6. Geben Sie den von Ihnen erstellten Richtliniennamen ein, z. B. *AutomationEV RolePolicy*, und aktivieren Sie dann das Kontrollkästchen neben der Richtlinie.
7. Wählen Sie Weiter: Markierungen.
8. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Rolle Metadaten hinzuzufügen.
9. Wählen Sie Weiter: Prüfen aus.

10. *Geben Sie* ***als Rollenname AutomationEVRole*** *ein.* Dieser Name muss derselbe Name sein, 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 Eine Rolle für einen AWS Dienst erstellen.

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 Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen aus.
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 Policy Document die folgende JSON-Datei, entfernen Sie die Standardrichtlinie und fügen Sie die kopierte JSON-Datei an ihrer Stelle ein.

```
{
    "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 eine Regel in der EventBridge Konsole zu erstellen, sodass Sie das Stoppen und Starten von EC2-Instances, deren Stilllegung geplant ist, automatisieren können.

So erstellen Sie eine Regel EventBridge für automatisierte 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 Define pattern (Muster definieren) die Option Event pattern (Ereignismuster) und dann Pre-defined pattern (Vordefiniertes Muster) 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 Bestimmte Ereignistyp-Kategorie (n) und anschließend scheduledChange aus.
10. Wählen Sie Code (s) für bestimmte Ereignistypen und dann den Ereignistypcode aus.

    Wählen Sie beispielsweise für Amazon EC2 EBS-gestützte Instances. **`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`** Wählen Sie für Store-Backed-Instances von Amazon EC2 Instances. **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**
11. Wählen Sie Irgendeine Ressource.

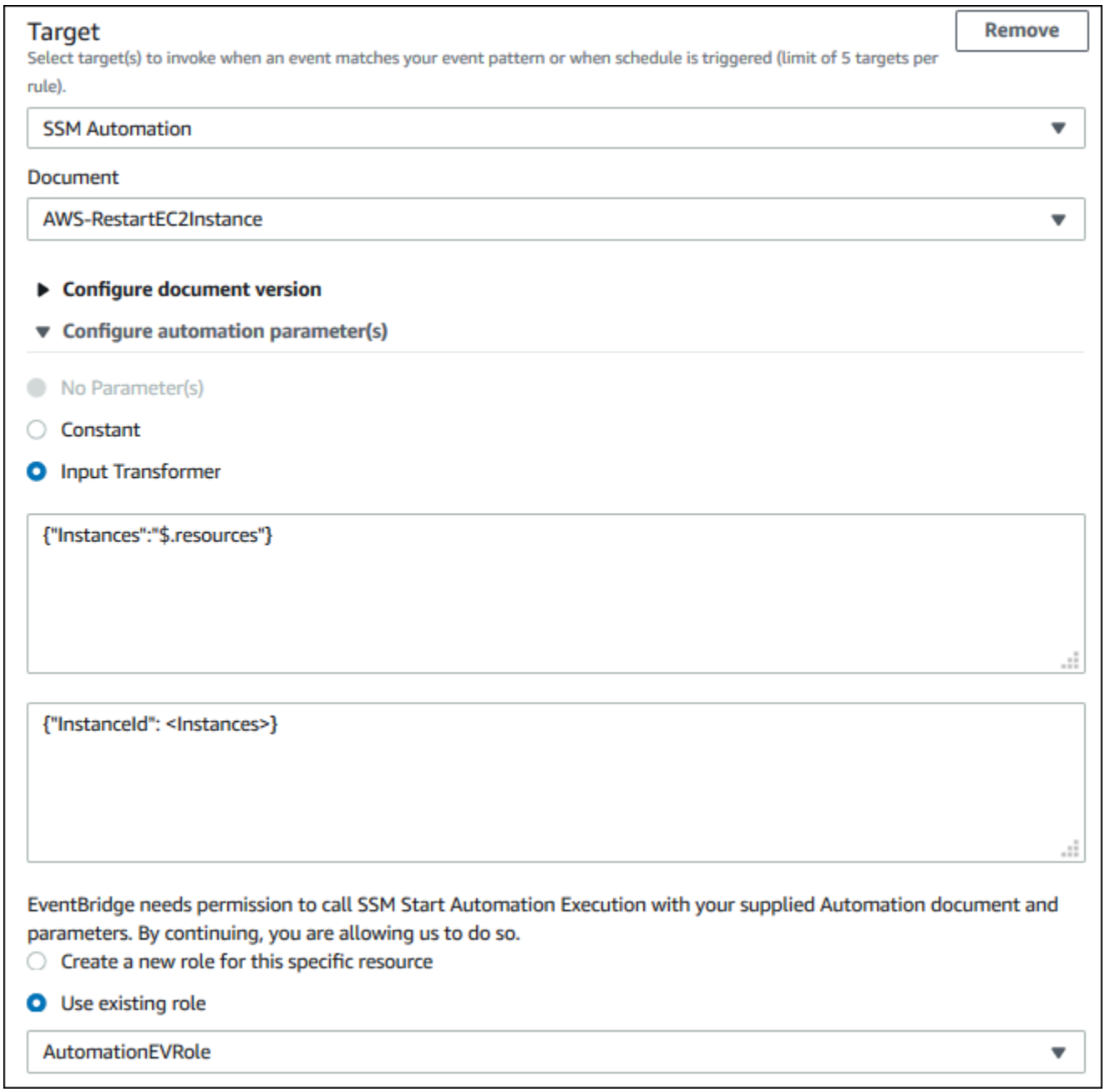
    Ihr Event-Muster wird dem folgenden Beispiel ähneln.

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 die Option Automatisierungsparameter konfigurieren und wählen Sie dann Input Transformer aus.
15. Geben Sie in das Feld Eingabepfad ein**`{"Instances":"$.resources"}`**.
16. Geben Sie für das zweite Feld ein**`{"InstanceId": <Instances>}`**.
17. Wählen Sie Bestehende Rolle verwenden 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 nicht über eine bestehende IAM-Rolle mit den erforderlichen EC2- und Systems Manager Manager-Berechtigungen und einer vertrauenswürdigen Beziehung verfügen, wird Ihre Rolle nicht in der Liste angezeigt. Weitere Informationen finden Sie unter Voraussetzungen.

18. Wählen Sie Erstellen.

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

Konfigurieren Sie SMC-Konnektoren für AWS Health

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 Integritätsereignisse verwalten. ServiceNow Die SMC-Integration mit AWS Health kann gesendete Health-Ereignisse verwenden, EventBridge um JIRA-Tickets und -Incidents automatisch zu erstellen, zuzuordnen und ServiceNow zu aktualisieren.

Sie können die Organisationsansicht und den delegierten Administratorzugriff verwenden, um Gesundheitsereignisse im gesamten Unternehmen einfach in JIRA zu verwalten und ServiceNow AWS Health Informationen direkt in den Arbeitsablauf Ihres Teams zu integrieren.

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

Weitere Informationen zur JIRA Management Cloud-Integration mithilfe des SMC finden AWS Health Sie unter in JIRA.

Überwachung 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 können, 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 beispielsweise ein Ereignis über Ihre Amazon EC2 EC2-Instances AWS Health veröffentlicht wird, können Sie diese Benachrichtigungen verwenden, um Maßnahmen zu ergreifen und Ihre Ressourcen nach Bedarf zu aktualisieren oder zu ersetzen. Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen EventBridge.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

- AWS Health API-Aufrufe protokollieren mit AWS CloudTrail

AWS Health API-Aufrufe protokollieren mit AWS CloudTrail

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

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

Weitere Informationen darüber 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 unterstützte Ereignisaktivitäten in auftreten AWS Health, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf 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 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 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 in dieser dokumentiert. Beispielsweise generieren Aufrufe der `DescribeAffectedEntities` Operationen `DescribeEventsDescribeEventDetails`, und Einträge in den CloudTrail Protokolldateien.

AWS Health unterstützt die Protokollierung 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 dem CloudTrail UserIdentity-Element.

Sie können Ihre Protokolldateien so lange in Ihrem Amazon S3 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 SNS-Benachrichtigungen veröffentlicht werden, wenn neue Protokolldateien zugestellt werden. Weitere Informationen finden Sie unter Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail.

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

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

Beispiel: Einträge in AWS Health Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 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 Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den DescribeEntityAggregatesVorgang 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"
   }
   ],
   ...
}
```

Dokumentenverlauf 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
Der Datenschutz für den Netzwerkverkehr wurde aus der Dokumentation zum Abschnitt AWS Health Sicherheit entfernt	Weitere Informationen finden Sie unter Sicherheit in AWS Health	27. März 2024
Zur AWS Health Dokumentation wurde das AWS Health Dashboard — Servicestatus und geplante Lebenszyklusereignisse aktualisiert.	Weitere Informationen finden Sie unter AWS Health Dashboard — Servicestatus und Geplante Lebenszyklusereignisse für AWS Health.	15. Februar 2024
Ein doppelter Aufzählungspunkt beim Erstellen einer EventBridge Regel für wurde entfernt AWS Health	Ein doppelter Aufzählungspunkt unter EventBridge Regel erstellen für wurde entfernt AWS Health.	4. Dezember 2023
Dokumentation für geplante Lebenszyklusereignisse 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	16. Oktober 2023

	(US) Regions. Siehe AWS Verwaltete Richtlinien für AWS Health.	
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 aggregieren wurde die 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: OrganizationsServiceRolePolicy Health_. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Health.	19. Juli 2023
AWS Health Schema unterstützt jetzt Event-Metadaten	Sie können jetzt Ereignismetadaten von AWS Health Ereignissen empfangen . Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen EventBridge.	20. Juni 2023

Aktualisierte Dokumentation für Amazon EventBridge	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 überwachen EventBridge.	2. Mai 2023
Dokumentation für AWS verwaltete Richtlinien hinzugefügt	Dokumentation zu den AWS verwalteten Richtlinien für AWS Health und zur Verwendung von serviceverknüpften Rollen für AWS Health hinzugefügt.	18. Januar 2023
Dokumentation zur Zeitzoneneinstellung 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 — Dienststatus.	21. September 2022
Aktualisierte Dokumentation	Dokumentation für AWS Health Aware hinzugefügt. Weitere Informationen finden Sie unter AWS Health Aware.	25. Mai 2022

Aktualisierte Dokumentation	Die Service Health Dashboard und die 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 unter AWS Health Dashboard — Dienststatus.	28. Februar 2022
Aktualisierte Dokumentation für Amazon EventBridge	Neues Thema für die AWS Health Nutzung von Amazon EventBridge zur Überwachung von Gesundheitsereignissen. Weitere Informationen finden Sie unter AWS Health Ereignisse mit Amazon überwachen 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 Ereignisse wurde aktualisiert	Es wurde ein Abschnitt zum Erstellen einer Regel für mehrere Dienste und Ereignistypkategorien hinzugefügt. Weitere Informationen finden Sie unter Eine Regel für mehrere Dienste und Kategorien erstellen.	7. Mai 2021
Die Dokumentation für CloudWatch Ereignisse wurde aktualisiert	Der Abschnitt zur Automatisierung von AWS Systems Manager Aktionen für Amazon CloudWatch Events-Regeln wurde aktualisiert. Weitere Informationen finden Sie unter Automatisieren von Aktionen für Amazon EC2 EC2-Instances.	28. April 2021
Die Dokumentation für CloudWatch Ereignisse wurde aktualisiert	Es wurde ein Bereich hinzugefügt, in dem Sie AWS Health Ereignisse in Ihrem Chat-Client empfangen können. Weitere Informationen finden Sie unter Empfangen von AWS Health Ereignissen mit AWS Chatbot.	16. März 2021

Aktualisierte Dokumentation	Die folgenden Themen werden aktualisiert: • Das Thema AWS Health Ereignisse aggregieren wurde aktualisiert • Das Thema „Monitor für AWS Health Ereignisse mit Amazon CloudWatch Events“ wurde neu organisiert und aktualisiert • Der Abschnitt „Ressourcen- und aktionsbasierte Bedingungen“ wurde aktualisiert	29. Januar 2021
Das AWS Health Dashboard für die Organisationsansicht wurde in der AWS Health Konsole hinzugefügt	Sie können die AWS Health Konsole verwenden, um die Funktion zur Organisationsansicht zu aktivieren. Sie können dann Gesundheitsereignisse für Mitgliedskonten in Ihrer AWS Organisation anzeigen.	14. Dezember 2020
Demo für Endgeräte mit hoher Verfügbarkeit	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	Die Organisation aktualisiert und hat einen RSS-Feed hinzugefügt, sodass Sie die neuesten Aktualisierungen der AWS Health Dokumentation abonnieren können.	28. August 2020

Frühere Aktualisierungen

Änderung	Beschreibung	Datum
Das Thema der Organisat ionsansicht wurde aktualisiert, damit Beispiele enthalten sind.	Siehe Aggregieren von AWS Health-Ereignissen über Konten mit Organisationsansic ht.	3. Juni 2020
Sicherheit und AWS Health	Es wurden Informationen zu Sicherheitsüberlegungen bei der Verwendung von AWS Health hinzugefügt. Siehe Sicherheit in 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 von AWS Health-Ereignissen über Konten mit Organisationsansic ht.	18. Dezember 2019
Es wurde ein neuer Abschnitt „Ressourcen- und aktionsba sierte Bedingungen“ hinzugefü gt, in dem die von der API gewährten Einschränkungen für Ereignisse erläutert werden. AWS Health	Siehe Identity and Access Management für AWS Health.	2. August 2018
Ein Hinweis zur Sichtbark eit von Informationen wurde hinzugefügt. AWS Health	Siehe Identity and Access Management für AWS Health.	16. August 2017
Service-Veröffentlichung.	AWS Health veröffentlicht.	1. Dezember 2016

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.