Entwicklerhandbuch

AWS IoT Events

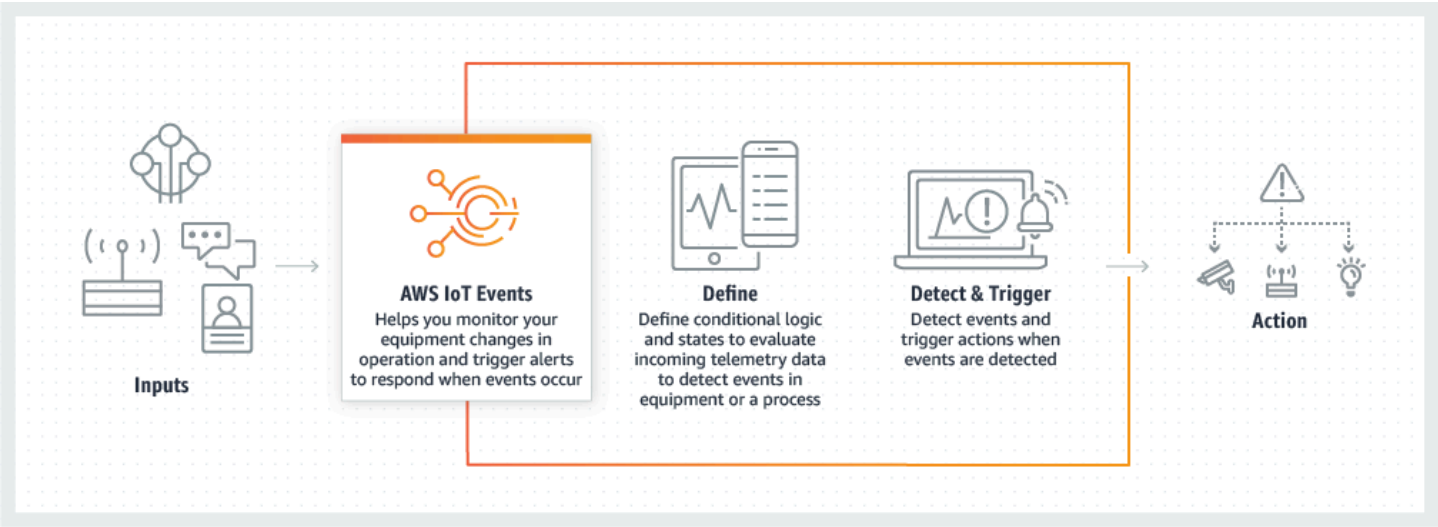
AWS IoT Events: Entwicklerhandbuch

Table of Contents

Was ist AWS IoT Events?

AWS IoT Events ermöglicht es Ihnen, Ihre Geräte oder Geräteflotten auf Ausfälle oder Betriebsänderungen zu überwachen und bei Auftreten solcher Ereignisse Maßnahmen auszulösen. AWS IoT Events überwacht kontinuierlich IoT-Sensordaten von Geräten, Prozessen, Anwendungen und anderen AWS Diensten, um wichtige Ereignisse zu identifizieren, damit Sie Maßnahmen ergreifen können.

Verwenden Sie diese Option AWS IoT Events , um komplexe Anwendungen zur Ereignisüberwachung in der AWS Cloud zu erstellen, auf die Sie über die AWS IoT Events Konsole oder zugreifen könnenAPIs.



Themen

- Vorteile und Funktionen
- Anwendungsfälle

Vorteile und Funktionen

Akzeptieren Sie Eingaben aus mehreren Quellen

AWS IoT Events akzeptiert Eingaben aus vielen IoT-Telemetriedatenquellen. Dazu gehören Sensorgeräte, Verwaltungsanwendungen und andere AWS IoT Dienste wie AWS IoT Core und AWS IoT Analytics. Sie können alle eingegebenen Telemetriedaten über eine API Standardschnittstelle (`BatchPutMessage`API) oder die AWS IoT Events Konsole AWS IoT Events per Push übertragen.

Weitere Informationen zu den ersten Schritten mit finden Sie AWS IoT Events unterErste Schritte mit der AWS IoT Events Konsole.

Verwenden Sie einfache logische Ausdrücke, um komplexe Ereignismuster zu erkennen

AWS IoT Events kann Muster von Ereignissen erkennen, die mehrere Eingaben von einem einzelnen IoT-Gerät oder einer einzelnen IoT-Anwendung oder von verschiedenen Geräten und vielen unabhängigen Sensoren beinhalten. Dies ist besonders nützlich, da jeder Sensor und jede Anwendung wichtige Informationen liefert. Aber nur durch die Kombination verschiedener Sensor- und Anwendungsdaten können Sie sich ein vollständiges Bild von der Leistung und Qualität der Abläufe machen. Sie können AWS IoT Events Melder so konfigurieren, dass sie diese Ereignisse mithilfe einfacher logischer Ausdrücke anstelle von komplexem Code erkennen.

Weitere Hinweise zu logischen Ausdrücken finden Sie unterAusdrücke zum Filtern, Transformieren und Verarbeiten von Ereignisdaten.

Auf Ereignissen basierende Aktionen auslösen

AWS IoT Events ermöglicht es Ihnen, Aktionen in Amazon Simple Notification Service (AmazonSNS), Lambda AWS IoT Core, Amazon SQS und Amazon Kinesis Firehose direkt auszulösen. Sie können eine AWS Lambda Funktion auch mithilfe der AWS IoT Regel-Engine auslösen, sodass Sie Aktionen mithilfe anderer Dienste wie Amazon Connect oder Ihrer eigenen Enterprise Resource Planning (ERP) -Anwendungen ausführen können.

AWS IoT Events enthält eine vorgefertigte Bibliothek mit Aktionen, die Sie ausführen können, und ermöglicht es Ihnen auch, Ihre eigenen zu definieren.

Weitere Informationen zum Auslösen von Aktionen auf der Grundlage von Ereignissen finden Sie unter. Unterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen

Automatisch skalieren, um den Anforderungen Ihrer Flotte gerecht zu werden

AWS IoT Events skaliert automatisch, wenn Sie homogene Geräte anschließen. Sie können einen Detektor einmal für einen bestimmten Gerätetyp definieren, und der Dienst skaliert und verwaltet automatisch alle Instanzen dieses Geräts, mit denen eine Verbindung hergestellt wird AWS IoT Events.

Beispiele für Detektormodelle finden Sie unterAWS IoT Events Beispiele für Detektormodelle.

Anwendungsfälle

AWS IoT Events hat viele Verwendungsmöglichkeiten. Hier sind ein paar Beispiele für Anwendungsfälle.

Überwachen und warten Sie Remote-Geräte

Die Überwachung einer Flotte von ferngesteuerten Maschinen kann eine Herausforderung sein, insbesondere wenn eine Fehlfunktion ohne klaren Kontext auftritt. Wenn eine Maschine nicht mehr funktioniert, kann dies bedeuten, dass die gesamte Verarbeitungseinheit oder Maschine ausgetauscht werden muss. Aber das ist nicht nachhaltig. Damit können AWS IoT Events Sie Nachrichten von mehreren Sensoren auf jedem Gerät empfangen, um bestimmte Probleme im Laufe der Zeit zu diagnostizieren. Anstatt die gesamte Einheit auszutauschen, verfügen Sie jetzt über die erforderlichen Informationen, um einen Techniker mit dem genauen Teil zu beauftragen, der ausgetauscht werden muss. Bei Millionen von Maschinen können sich die Einsparungen auf Millionen von Dollar summieren, wodurch Ihre Gesamtkosten für den Besitz oder die Wartung jeder Maschine sinken.

Industrieroboter verwalten

Der Einsatz von Robotern in Ihren Einrichtungen zur Automatisierung der Paketbewegung kann die Effizienz erheblich steigern. Um die Kosten zu minimieren, können Roboter mit einfachen, kostengünstigen Sensoren ausgestattet werden, die Daten an die Cloud melden. Bei Dutzenden von Sensoren und Hunderten von Betriebsmodi kann es jedoch schwierig sein, Probleme in Echtzeit zu erkennen. Damit können Sie ein Expertensystem aufbauen AWS IoT Events, das diese Sensordaten in der Cloud verarbeitet und Warnmeldungen erstellt, um das technische Personal automatisch zu benachrichtigen, wenn ein Ausfall unmittelbar bevorsteht.

Verfolgen Sie Gebäudeautomationssysteme

In Rechenzentren trägt die Überwachung auf hohe Temperaturen und niedrige Luftfeuchtigkeit dazu bei, Geräteausfälle zu verhindern. Sensoren werden häufig von vielen Herstellern gekauft und jeder Typ wird mit einer eigenen Verwaltungssoftware geliefert. Verwaltungssoftware verschiedener Anbieter ist jedoch manchmal nicht kompatibel, was die Erkennung von Problemen erschwert. Mithilfe dieser Funktion können Sie Warnmeldungen einrichten AWS IoT Events, um Ihre Betriebsanalysten rechtzeitig vor einem Ausfall über Probleme mit Ihren Heiz- und Kühlsystemen zu informieren. Auf diese Weise können Sie eine ungeplante Abschaltung des Rechenzentrums verhindern, die Tausende von Dollar für den Austausch von Geräten und potenzielle Umsatzeinbußen kosten würde.

Einrichten AWS IoT Events

Dieser Abschnitt enthält eine Anleitung zur Einrichtung AWS IoT Events, einschließlich der Erstellung eines AWS Kontos, der Konfiguration der erforderlichen Berechtigungen und der Einrichtung von Rollen für die Verwaltung des Zugriffs auf Ressourcen.

Themen

Einrichtung eines AWS-Konto

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS -Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer.

   Anweisungen finden Sie im Benutzerhandbuch unter Aktivieren eines virtuellen MFA Geräts für Ihren AWS-Konto IAM Root-Benutzer (Konsole).

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, URL die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugangsportal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Berechtigungen einrichten für AWS IoT Events

In diesem Abschnitt werden die Berechtigungen beschrieben, die für die Nutzung einiger Funktionen von erforderlich sind AWS IoT Events. Sie können AWS CLI Befehle oder die Konsole AWS Identity and Access Management (IAM) verwenden, um Rollen und zugehörige Berechtigungsrichtlinien für den Zugriff auf Ressourcen oder die Ausführung bestimmter Funktionen in zu erstellen AWS IoT Events.

Das IAMBenutzerhandbuch enthält detailliertere Informationen zur sicheren Steuerung von Zugriffsberechtigungen für AWS Ressourcen. Spezifische Informationen zu AWS IoT Events finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS IoT Events.

Informationen zur Verwendung der IAM Konsole zum Erstellen und Verwalten von Rollen und Berechtigungen finden Sie im IAMTutorial: AWS Kontoübergreifendes Delegieren des Zugriffs mithilfe von IAM Rollen.

> **Note**
>
> Schlüssel können zwischen 1 und 128 Zeichen lang sein und Folgendes beinhalten:
>
> - Groß- oder Kleinbuchstaben a-z
> - Zahlen 0-9
> - Sonderzeichen -, _ oder:.

Aktionsberechtigungen für AWS IoT Events

AWS IoT Events ermöglicht es Ihnen, Aktionen auszulösen, die andere AWS Dienste verwenden. Dazu müssen Sie die AWS IoT Events Erlaubnis erteilen, diese Aktionen in Ihrem Namen durchzuführen. Dieser Abschnitt enthält eine Liste der Aktionen und eine Beispielrichtlinie, die die Erlaubnis erteilt, all diese Aktionen mit Ihren Ressourcen durchzuführen. Ändern Sie die *region* and *account-id* Referenzen nach Bedarf. Wenn möglich, sollten Sie auch die Platzhalter (*) so ändern, dass sie sich auf bestimmte Ressourcen beziehen, auf die zugegriffen wird. Sie können die IAM Konsole verwenden, um die Erlaubnis AWS IoT Events zum Senden einer von Ihnen definierten SNS Amazon-Warnung zu erteilen.

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie einen Timer verwenden oder eine Variable festlegen können:

- `setTimer`um einen Timer zu erstellen.
- `resetTimer`um den Timer zurückzusetzen.
- `clearTimer`um den Timer zu löschen.
- `setVariable`um eine Variable zu erstellen.

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie mit AWS Diensten arbeiten können:

- `iotTopicPublish`um eine Nachricht zu einem MQTT Thema zu veröffentlichen.
- `iotEvents`um Daten AWS IoT Events als Eingabewert an zu senden.
- `iotSiteWise` zum Senden von Daten an eine Komponenteneigenschaft in AWS IoT SiteWise
- `dynamoDB`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `dynamoDBv2`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `firehose`um Daten an einen Amazon Data Firehose-Stream zu senden.
- `lambda`um eine Funktion aufzurufen. AWS Lambda
- `sns`um Daten als Push-Benachrichtigung zu senden.
- `sqs`um Daten an eine SQS Amazon-Warteschlange zu senden.

Example Richtlinie

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "iot:Publish",
        "Resource": "arn:aws:iot:<region>:<account_id>:topic/*"
      },
      {
        "Effect": "Allow",
        "Action": "iotevents:BatchPutMessage",
        "Resource": "arn:aws:iotevents:<region>:<account_id>:input/*"
      },
      {
        "Effect": "Allow",
        "Action": "iotsitewise:BatchPutAssetPropertyValue",
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": "dynamodb:PutItem",
        "Resource": "arn:aws:dynamodb:<region>:<account_id>:table/*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "firehose:PutRecord",
          "firehose:PutRecordBatch"
        ],
        "Resource": "arn:aws:firehose:<region>:<account_id>:deliverystream/*"
      },
      {
        "Effect": "Allow",
        "Action": "lambda:InvokeFunction",
        "Resource": "arn:aws:lambda:<region>:<account_id>:function:*"
      },
      {
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "arn:aws:sns:<region>:<account_id>:*"
      },
      {
        "Effect": "Allow",
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:<region>:<account_id>:*"
```

```
      }
    ]
}
```

Sicherung der Eingabedaten in AWS IoT Events

Es ist wichtig zu berücksichtigen, wer Zugriff auf Eingabedaten für die Verwendung in einem Detektormodell gewähren kann. Wenn Sie einen Benutzer oder eine Entität haben, deren Gesamtberechtigungen Sie einschränken möchten, die jedoch berechtigt sind, ein Detektormodell zu erstellen oder zu aktualisieren, müssen Sie diesem Benutzer oder dieser Entität auch die Erlaubnis erteilen, das Eingangs-Routing zu aktualisieren. Das bedeutet, dass Sie nicht nur die Erlaubnis für `iotevents:CreateDetectorModel` und erteilen müssen`iotevents:UpdateDetectorModel`, sondern auch die Erlaubnis für`iotevents:UpdateInputRouting`.

Example

Die folgende Richtlinie fügt die Erlaubnis für hinzu`iotevents:UpdateInputRouting`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "updateRoutingPolicy",
            "Effect": "Allow",
            "Action": [
                "iotevents:UpdateInputRouting"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können anstelle des Platzhalters "`*`" eine Liste mit eingegebenen Amazon-Ressourcennamen (ARNs) angeben, um diese Berechtigung auf bestimmte Eingaben zu beschränken. `Resource` Auf diese Weise können Sie den Zugriff auf die Eingabedaten einschränken, die von Detektormodellen verwendet werden, die vom Benutzer oder der Entität erstellt oder aktualisiert wurden.

Rollenrichtlinie für CloudWatch Amazon-Protokollierung

Die folgenden Richtliniendokumente enthalten die Rollen- und Vertrauensrichtlinien, anhand AWS IoT Events derer Sie Protokolle in CloudWatch Ihrem Namen einreichen können.

Rollenrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutMetricFilter",
                "logs:PutRetentionPolicy",
                "logs:GetLogEvents",
                "logs:DeleteLogStream"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        }
    ]
}
```

Vertrauensrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [

          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Sie benötigen außerdem eine dem Benutzer zugeordnete IAM Berechtigungsrichtlinie, die es dem Benutzer ermöglicht, Rollen zu übergeben, und zwar wie folgt. Weitere Informationen finden Sie im

Benutzerhandbuch unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS Dienst. IAM

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
          "iam:GetRole",
          "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::<account-id>:role/Role_To_Pass"
    }
  ]
}
```

Sie können den folgenden Befehl verwenden, um die Ressourcenrichtlinie für CloudWatch Protokolle festzulegen. Dies ermöglicht AWS IoT Events das Einfügen von Protokollereignissen in CloudWatch Streams.

```
aws logs put-resource-policy --policy-name ioteventsLoggingPolicy --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
 \"IoTEventsToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service\":
 [ \"iotevents.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource\": \"*
\" } ] }"
```

Verwenden Sie den folgenden Befehl, um Protokollierungsoptionen festzulegen. Ersetzen Sie das `roleArn` durch die Protokollierungsrolle, die Sie erstellt haben.

```
aws iotevents put-logging-options --cli-input-json "{ \"loggingOptions\": {\"roleArn\":
 \"arn:aws:iam::123456789012:role/testLoggingRole\", \"level\": \"INFO\", \"enabled\":
 true } }"
```

Rollenrichtlinie für Amazon SNS Messaging

Die folgenden Richtliniendokumente enthalten die Rollen- und Vertrauensrichtlinien, die das Senden von SNS Nachrichten AWS IoT Events ermöglichen.

Rollenrichtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sns:*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:sns:us-east-1:123456789012:testAction"
        }
    ]
}
```

Vertrauensrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Erste Schritte mit der AWS IoT Events Konsole

In diesem Abschnitt erfahren Sie, wie Sie mit der AWS IoT Events Konsole ein Eingabe- und ein Detektormodell erstellen. Sie modellieren zwei Zustände eines Motors: einen Normalzustand und einen Überdruckzustand. Wenn der gemessene Druck im Motor einen bestimmten Schwellenwert überschreitet, geht das Modell vom Normalzustand in den Überdruckzustand über. Dann sendet es eine SNS Amazon-Nachricht, um einen Techniker über den Zustand zu informieren. Wenn der Druck bei drei aufeinanderfolgenden Druckmessungen wieder unter den Schwellenwert fällt, kehrt das Modell in den Normalzustand zurück und sendet eine weitere SNS Amazon-Nachricht als Bestätigung.

Wir prüfen, ob drei aufeinanderfolgende Messwerte unter dem Druckschwellenwert liegen, um ein mögliches Stottern bei Überdruck oder normalen Meldungen im Falle einer nichtlinearen Erholungsphase oder einer anomalen Druckmessung zu vermeiden.

Auf der Konsole finden Sie auch mehrere vorgefertigte Modellvorlagen für Melder, die Sie anpassen können. Sie können die Konsole auch verwenden, um Meldermodelle zu importieren, die von anderen geschrieben wurden, oder um Ihre Meldermodelle zu exportieren und sie in verschiedenen AWS Regionen zu verwenden. Wenn Sie ein Meldermodell importieren, stellen Sie sicher, dass Sie die erforderlichen Eingaben erstellen oder sie für die neue Region neu erstellen, und aktualisieren Sie alle ARNs verwendeten Rollen.

Verwenden Sie die AWS IoT Events Konsole, um mehr über Folgendes zu erfahren.

Definieren Sie Eingaben

Um Ihre Geräte und Prozesse zu überwachen, müssen sie über eine Möglichkeit verfügen, Telemetriedaten in AWS IoT Events zu übertragen. Dies geschieht, indem Nachrichten als Eingaben an gesendet AWS IoT Events werden. Hierfür gibt es mehrere Möglichkeiten:

- Benutze die BatchPutMessageOperation.
- Schreiben Sie in AWS IoT Core eine AWS IoT Events Aktionsregel für die AWS IoT Regel-Engine, die Ihre Nachrichtendaten weiterleitet. AWS IoT Events Sie müssen die Eingabe anhand des Namens identifizieren.
- Verwenden Sie in AWS IoT Analytics die CreateDatasetOperation, um einen Datensatz mit zu erstellen`contentDeliveryRules`. Diese Regeln spezifizieren die AWS IoT Events Eingabe, an die der Inhalt des Datensatzes automatisch gesendet wird.

Bevor Ihre Geräte Daten auf diese Weise senden können, müssen Sie einen oder mehrere Eingänge definieren. Geben Sie dazu jeder Eingabe einen Namen und geben Sie an, welche Felder in den eingehenden Nachrichtendaten von der Eingabe überwacht werden.

Erstellen Sie ein Detektormodell

Definieren Sie mithilfe von Zuständen ein Detektormodell (ein Modell Ihrer Ausrüstung oder Ihres Prozesses). Definieren Sie für jeden Status eine bedingte (boolesche) Logik, die die eingehenden Eingaben auswertet, um signifikante Ereignisse zu erkennen. Wenn das Detektormodell ein Ereignis erkennt, kann es den Status ändern oder mithilfe anderer Dienste benutzerdefinierte oder vordefinierte Aktionen auslösen. AWS Sie können zusätzliche Ereignisse definieren, die Aktionen auslösen, wenn Sie einen Status betreten oder verlassen und optional, wenn eine Bedingung erfüllt ist.

In diesem Tutorial senden Sie eine SNS Amazon-Nachricht als Aktion, wenn das Modell in einen bestimmten Status eintritt oder diesen verlässt.

Überwachen Sie ein Gerät oder einen Prozess

Wenn Sie mehrere Geräte oder Prozesse überwachen, geben Sie in jeder Eingabe ein Feld an, das das jeweilige Gerät oder den Prozess identifiziert, von dem die Eingabe stammt. Das `key` Feld finden Sie in`CreateDetectorModel`. Wenn das von identifizierte Eingabefeld einen neuen Wert `key` erkennt, wird ein neues Gerät identifiziert und ein Detektor erstellt. Jeder Detektor ist ein Exemplar des Detektormodells. Der neue Detektor reagiert weiterhin auf Eingaben von diesem Gerät, bis sein Detektormodell aktualisiert oder gelöscht wird.

Wenn Sie einen einzelnen Prozess überwachen (auch wenn mehrere Geräte oder Unterprozesse Eingaben senden), geben Sie kein eindeutiges `key` Identifikationsfeld an. In diesem Fall erzeugt das Modell einen einzelnen Detektor (Instanz), wenn die erste Eingabe eingeht.

Senden Sie Nachrichten als Eingaben an Ihr Detektormodell

Es gibt mehrere Möglichkeiten, eine Nachricht von einem Gerät oder Prozess als Eingabe in einen AWS IoT Events Detektor zu senden, ohne dass Sie die Nachricht zusätzlich formatieren müssen. In diesem Tutorial verwenden Sie die AWS IoT Konsole, um eine AWS IoT Events Aktionsregel für die AWS IoT Regel-Engine zu schreiben, in AWS IoT Events die Ihre Nachrichtendaten weitergeleitet werden.

Identifizieren Sie dazu die Eingabe anhand des Namens und verwenden Sie weiterhin die AWS IoT Konsole, um Nachrichten zu generieren, an die sie als Eingaben weitergeleitet AWS IoT Events werden.

> **Note**
>
> In diesem Tutorial wird die Konsole verwendet, um dasselbe `input` zu erstellen. Dies `detector model` wird im Beispiel unter gezeigtTutorials für AWS IoT Events Anwendungsfälle. Sie können dieses JSON Beispiel verwenden, um dem Tutorial zu folgen.

Themen

Voraussetzungen für den Einstieg AWS IoT Events

Wenn Sie noch kein AWS Konto haben, erstellen Sie eines.

1. Folgen Sie den Anweisungen inEinrichten AWS IoT Events, um sicherzustellen, dass das Konto ordnungsgemäß eingerichtet und die erforderlichen Berechtigungen erteilt wurden.
2. Erstellen Sie zwei Amazon Simple Notification Service (AmazonSNS) -Themen.

   In diesem Tutorial (und dem entsprechenden Beispiel) wird davon ausgegangen, dass Sie zwei SNS Amazon-Themen erstellt haben. Die ARNs dieser Themen werden wie folgt angezeigt: `arn:aws:sns:us-east-1:123456789012:underPressureAction` und`arn:aws:sns:us-east-1:123456789012:pressureClearedAction`. Ersetzen Sie diese Werte durch die ARNs von Ihnen SNS erstellten Amazon-Themen. Weitere Informationen finden Sie im Amazon Simple Notification Service-Entwicklerhandbuch.

   Als Alternative zur Veröffentlichung von Benachrichtigungen zu SNS Amazon-Themen können Sie festlegen, dass die Melder MQTT Nachrichten mit einem von Ihnen angegebenen Thema senden. Mit dieser Option können Sie überprüfen, ob Ihr Detektormodell Instances erstellt und ob diese Instances Benachrichtigungen senden, indem Sie die AWS IoT Core-Konsole verwenden, um Nachrichten zu diesen MQTT Themen zu abonnieren und zu überwachen. Sie können den MQTT Themennamen auch dynamisch zur Laufzeit definieren, indem Sie eine Eingabe oder Variable verwenden, die im Detektormodell erstellt wurde.

3. Wählen Sie einen AWS-Region , der unterstützt AWS IoT Events. Weitere Informationen finden Sie unter AWS IoT Events im Allgemeine AWS-Referenz. Hilfe finden Sie unter Arbeiten mit dem AWS Management Console im Abschnitt Erste Schritte mit dem AWS Management Console.

Erstellen Sie eine Eingabe für Modelle

Wir empfehlen, bei der Erstellung der Eingaben für Ihre Modelle Dateien zusammenzustellen, die Beispielnachrichten enthalten, die Ihre Geräte oder Prozesse zur Meldung ihres Zustands senden. Diese Dateien helfen Ihnen dabei, die erforderlichen Eingaben zu definieren.

Sie können eine Eingabe mit mehreren Methoden erstellen, die in diesem Abschnitt beschrieben werden.

Erstellen Sie eine JSON Eingabedatei

1. Erstellen Sie zunächst eine Datei mit dem Namen `input.json` auf Ihrem lokalen Dateisystem mit dem folgenden Inhalt:

```
{
  "motorid": "Fulton-A32",
  "sensorData": {
    "pressure": 23,
    "temperature": 47
  }
}
```

2. Jetzt, da Sie diese `input.json` Starterdatei haben, können Sie eine Eingabe erstellen. Es gibt zwei Möglichkeiten, eine Eingabe zu erstellen. Sie können eine Eingabe mithilfe des Navigationsbereichs in der AWS IoT Events Konsole erstellen. Sie können auch eine Eingabe innerhalb des Detektormodells erstellen, nachdem es erstellt wurde.

Erstellen und konfigurieren Sie eine Eingabe

Erfahren Sie, wie Sie eine Eingabe für ein Alarmmodell oder ein Meldermodell erstellen.

1. Loggen Sie sich in die AWS IoT Events Konsole ein oder wählen Sie die Option Neues AWS IoT Events Konto erstellen.

2. Wählen Sie in der AWS IoT Events Konsole in der oberen linken Ecke den Navigationsbereich aus und erweitern Sie ihn.
3. Wählen Sie im linken Navigationsbereich Eingaben aus.
4. Wählen Sie in der rechten Ecke der Konsole die Option Eingabe erstellen aus.
5. Geben Sie ein Unikat an InputName.
6. Optional — geben Sie eine Beschreibung für Ihre Eingabe ein.
7. Um eine JSON Datei hochzuladen, wählen Sie die `input.json` Datei aus, die Sie in der Übersicht für erstellt habenErstellen Sie eine JSON Eingabedatei. Die Option Eingabeattribute auswählen wird mit einer Liste der von Ihnen eingegebenen Attribute angezeigt.
8. Wählen Sie unter Eingabeattribute auswählen die zu verwendenden Attribute aus und klicken Sie auf Erstellen. In diesem Beispiel wählen wir motorid und sensorData.pressure aus.
9. Optional — Fügen Sie der Eingabe relevante Tags hinzu.

> **Note**
>
> Sie können auch zusätzliche Eingaben innerhalb des Meldermodells in der AWS IoT Events Konsole erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Eingabe innerhalb des Detektormodells.

Erstellen Sie eine Eingabe innerhalb des Detektormodells

In diesem Abschnitt wird gezeigt, wie ein Eingang für ein Detektormodell zum Empfang von Telemetriedaten oder Nachrichten definiert wird.

1. Öffnen Sie die AWS IoT Events -Konsole.
2. Wählen Sie in der AWS IoT Events Konsole die Option Meldermodell erstellen aus.
3. Wählen Sie Neu erstellen.
4. Wählen Sie Create input (Eingabe erstellen).
5. Geben Sie für die Eingabe eine InputNameoptionale Beschreibung ein und wählen Sie Datei hochladen. Wählen Sie im daraufhin angezeigten Dialogfeld die `input.json` Datei aus, für die Sie in der Übersicht erstellt habenErstellen Sie eine JSON Eingabedatei.
6. Wählen Sie unter Eingabeattribute auswählen die zu verwendenden Attribute aus und klicken Sie auf Erstellen. In diesem Beispiel wählen wir motorIdund sensorData.pressure aus.

Erstellen Sie ein Detektormodell

In diesem Thema definieren Sie mithilfe von Zuständen ein Detektormodell (ein Modell Ihrer Ausrüstung oder Ihres Prozesses).

Für jeden Status definieren Sie eine bedingte (boolesche) Logik, die die eingehenden Eingaben auswertet, um ein signifikantes Ereignis zu erkennen. Wenn ein Ereignis erkannt wird, ändert es den Status und kann zusätzliche Aktionen einleiten. Diese Ereignisse werden als Übergangsereignisse bezeichnet.

In Ihren Zuständen definieren Sie auch Ereignisse, die Aktionen ausführen können, wenn der Melder in diesen Zustand eintritt oder ihn verlässt oder wenn eine Eingabe eingeht (diese Ereignisse werden als `OnEnter` `OnInput` AND-Ereignisse bezeichnet). `OnExit` Die Aktionen werden nur ausgeführt, wenn die Bedingungslogik des Ereignisses Folgendes ergibt. `true`

Um ein Detektormodell zu erstellen

1. Der erste Detektorstatus wurde für Sie erstellt. Um ihn zu ändern, wählen Sie den Kreis mit der Bezeichnung State_1 im Hauptbearbeitungsbereich aus.
2. Geben Sie im Bereich „Status“ den Namen des Bundesstaates ein und wählen Sie „OnEnterEreignis hinzufügen“.
3. Geben Sie auf der Seite „ OnEnter Ereignis hinzufügen“ einen Namen für das Ereignis und die Bedingung für das Ereignis ein. Geben Sie in diesem Beispiel ein, `true` um anzugeben, dass das Ereignis immer ausgelöst wird, wenn der Status eingegeben wird.
4. Wählen Sie unter Ereignisaktionen die Option Aktion hinzufügen aus.
5. Gehen Sie unter Ereignisaktionen wie folgt vor:

   a. Wählen Sie „Variable festlegen“
   b. Wählen Sie für den Variablenbetrieb die Option Wert zuweisen.
   c. Geben Sie unter Variablenname den Namen der Variablen ein, die festgelegt werden soll.
   d. Geben Sie für Variablenwert den Wert **`0`** (Null) ein.
6. Wählen Sie Save (Speichern) aus.

   Eine Variable, wie die, die Sie definiert haben, kann auf jeden Fall im Detektormodell festgelegt werden (mit einem Wert). Auf den Wert der Variablen kann erst verwiesen werden (z. B. in der bedingten Logik eines Ereignisses), wenn der Detektor einen Status erreicht hat und eine Aktion ausgeführt hat, in der er definiert oder gesetzt ist.

7. Wählen Sie im Statusbereich das X neben Status, um zur Modellpalette Detector zurückzukehren.
8. Um einen zweiten Detektorstatus zu erstellen, wählen Sie in der Modellpalette Detektor die Option Status und ziehen Sie ihn in den Hauptbearbeitungsbereich. Dadurch wird ein Zustand mit dem Titel erstelltuntitled_state_1.
9. Halten Sie im ersten Status (Normal) an. Am Rand des Bundesstaats erscheint ein Pfeil.
10. Klicken Sie auf den Pfeil und ziehen Sie ihn vom ersten Status in den zweiten Status. Eine gerichtete Linie vom ersten zum zweiten Status (mit der Bezeichnung Unbenannt) wird angezeigt.
11. Wählen Sie die Linie Ohne Titel aus. Geben Sie im Bereich „Übergangsereignis“ einen Namen für das Ereignis und eine Logik für das Ereignis ein.
12. Wählen Sie im Bereich „Übergangsereignis“ die Option Aktion hinzufügen aus.
13. Wählen Sie im Bereich „Aktionen für Übergangsereignis hinzufügen“ die Option Aktion hinzufügen aus.
14. Wählen Sie für Aktion auswählen die Option Variable festlegen aus.
    a. Wählen Sie für Variablenoperation die Option Wert zuweisen aus.
    b. Geben Sie unter Variablenname den Namen der Variablen ein.
    c. Geben Sie für Wert zuweisen einen Wert ein, z. B.: `$variable.pressureThresholdBreached + 3`
    d. Wählen Sie Save (Speichern) aus.
15. Wählen Sie den zweiten Status untitled_state_1 aus.
16. Geben Sie im Bereich „Status“ den Namen des Bundesstaates ein und wählen Sie für „Bei Eingabe“ die Option „Ereignis hinzufügen“ aus.
17. Geben Sie auf der Seite „ OnEnter Ereignis hinzufügen“ den Namen des Ereignisses und die Bedingung für das Ereignis ein. Wählen Sie Aktion hinzufügen aus.
18. Wählen Sie für Aktion auswählen die Option SNSNachricht senden aus.
    a. Geben Sie als SNSThema das Ziel ARN Ihres SNS Amazon-Themas ein.
    b. Wählen Sie Save (Speichern) aus.
19. Fahren Sie mit dem Hinzufügen der Ereignisse im Beispiel fort.
    a. Wählen Sie für OnInputEreignis hinzufügen aus und geben Sie die folgenden Ereignisinformationen ein und speichern Sie sie.

```
Event name: Overpressurized
Event condition: $input.PressureInput.sensorData.pressure > 70
Event actions:
  Set variable:
    Variable operation: Assign value
    Variable name: pressureThresholdBreached
    Assign value: 3
```

b. Wählen Sie für OnInput„Ereignis hinzufügen“ und geben Sie die folgenden Ereignisinformationen ein und speichern Sie sie.

```
Event name: Pressure Okay
Event condition: $input.PressureInput.sensorData.pressure <= 70
Event actions:
  Set variable:
    Variable operation: Decrement
    Variable name: pressureThresholdBreached
```

c. Wählen Sie „Veranstaltung hinzufügen“ und geben Sie die folgenden Veranstaltungsinformationen unter Verwendung des ARN von Ihnen erstellten SNS Amazon-Themas ein und speichern Sie sie. OnExit

```
Event name: Normal Pressure Restored
Event condition: true
Event actions:
  Send SNS message:
    Target arn: arn:aws:sns:us-east-1:123456789012:pressureClearedAction
```

20. Machen Sie eine Pause im zweiten Status (Gefährlich). Am Rand des Bundesstaats erscheint ein Pfeil
21. Klicken Sie auf den Pfeil und ziehen Sie ihn vom zweiten Status in den ersten Status. Eine gerichtete Linie mit der Bezeichnung Unbenannt wird angezeigt.
22. Wählen Sie die Zeile „Unbenannt“ und geben Sie im Bereich „Übergangsereignis“ anhand der folgenden Informationen einen Namen für das Ereignis und eine Logik für das Ereignis ein.

```
{
  Event name: BackToNormal
```

```
  Event trigger logic: $input.PressureInput.sensorData.pressure <= 70 &&
 $variable.pressureThresholdBreached <= 0
}
```

Weitere Informationen darüber, warum wir den `$input` Wert und den `$variable` Wert in der Triggerlogik testen, finden Sie im Eintrag zur Verfügbarkeit von Variablenwerten unter. Einschränkungen und Einschränkungen des Detektormodells

23. Wählen Sie den Startstatus aus. Standardmäßig wurde dieser Status erstellt, als Sie ein Detektormodell erstellt haben). Wählen Sie im Startbereich den Zielstatus aus (z. B. Normal).
24. Als Nächstes konfigurieren Sie Ihr Meldermodell so, dass es auf Eingaben wartet. Wählen Sie in der oberen rechten Ecke Veröffentlichen aus.
25. Gehen Sie auf der Seite Meldermodell veröffentlichen wie folgt vor.
    a. Geben Sie einen Modellnamen für den Detektor, eine Beschreibung und den Namen einer Rolle ein. Diese Rolle wurde für Sie erstellt.
    b. Wählen Sie für jeden eindeutigen Schlüsselwert einen Detektor erstellen aus. Um Ihre eigene Rolle zu erstellen und zu verwenden, folgen Sie den Schritten unter Berechtigungen einrichten für AWS IoT Events und geben Sie sie hier als Rolle ein.
26. Wählen Sie unter Detector creation key den Namen eines der Attribute der Eingabe, die Sie zuvor definiert haben. Das Attribut, das Sie als Schlüssel für die Erstellung des Melders wählen, muss in jeder Nachrichteneingabe vorhanden sein und für jedes Gerät, das Nachrichten sendet, eindeutig sein. In diesem Beispiel wird das motorid-Attribut verwendet.
27. Wählen Sie Save and publish (Speichern und veröffentlichen).

> **Note**
>
> Die Anzahl der eindeutigen Melder, die für ein bestimmtes Detektormodell erstellt wurden, basiert auf den gesendeten Eingangsmeldungen. Wenn ein Detektormodell erstellt wird, wird ein Schlüssel aus den Eingabeattributen ausgewählt. Dieser Schlüssel bestimmt, welche Detektorinstanz verwendet werden soll. Wenn der Schlüssel noch nie gesehen wurde (für dieses Detektormodell), wird eine neue Detektorinstanz erstellt. Wenn der Schlüssel schon einmal gesehen wurde, verwenden wir die bestehende Detektorinstanz, die diesem Schlüsselwert entspricht.

Sie können eine Sicherungskopie Ihrer Detektormodelldefinition (unJSON) erstellen, das Meldermodell neu erstellen oder aktualisieren oder es als Vorlage verwenden, um ein anderes Meldermodell zu erstellen.

Sie können dies von der Konsole aus oder mit dem folgenden CLI Befehl tun. Ändern Sie bei Bedarf den Namen des Meldermodells so, dass er dem entspricht, den Sie bei der Veröffentlichung im vorherigen Schritt verwendet haben.

```
aws iotevents describe-detector-model  --detector-model-name motorDetectorModel >
 motorDetectorModel.json
```

Dadurch wird eine Datei (`motorDetectorModel.json`) erstellt, deren Inhalt dem folgenden ähnelt.

```
{
    "detectorModel": {
        "detectorModelConfiguration": {
            "status": "ACTIVE",
            "lastUpdateTime": 1552072424.212,
            "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
            "creationTime": 1552072424.212,
            "detectorModelArn": "arn:aws:iotevents:us-
west-2:123456789012:detectorModel/motorDetectorModel",
            "key": "motorid",
            "detectorModelName": "motorDetectorModel",
            "detectorModelVersion": "1"
        },
        "detectorModelDefinition": {
            "states": [
                {
                    "onInput": {
                        "transitionEvents": [
                            {
                                "eventName": "Overpressurized",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
                                            "value":
 "$variable.pressureThresholdBreached + 3"
                                        }
                                    }
```

```
                                ],
                                "condition": "$input.PressureInput.sensorData.pressure
> 70",
                                "nextState": "Dangerous"
                            }
                        ],
                        "events": []
                    },
                    "stateName": "Normal",
                    "onEnter": {
                        "events": [
                            {
                                "eventName": "init",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
"pressureThresholdBreached",
                                            "value": "0"
                                        }
                                    }
                                ],
                                "condition": "true"
                            }
                        ]
                    },
                    "onExit": {
                        "events": []
                    }
                },
                {
                    "onInput": {
                        "transitionEvents": [
                            {
                                "eventName": "Back to Normal",
                                "actions": [],
                                "condition": "$variable.pressureThresholdBreached <= 1
&& $input.PressureInput.sensorData.pressure <= 70",
                                "nextState": "Normal"
                            }
                        ],
                        "events": [
                            {
                                "eventName": "Overpressurized",
```

```
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
                                            "value": "3"
                                        }
                                    }
                                ],
                                "condition": "$input.PressureInput.sensorData.pressure
 > 70"
                            },
                            {
                                "eventName": "Pressure Okay",
                                "actions": [
                                    {
                                        "setVariable": {
                                            "variableName":
 "pressureThresholdBreached",
                                            "value":
 "$variable.pressureThresholdBreached - 1"
                                        }
                                    }
                                ],
                                "condition": "$input.PressureInput.sensorData.pressure
 <= 70"
                            }
                        ]
                    },
                    "stateName": "Dangerous",
                    "onEnter": {
                        "events": [
                            {
                                "eventName": "Pressure Threshold Breached",
                                "actions": [
                                    {
                                        "sns": {
                                            "targetArn": "arn:aws:sns:us-
west-2:123456789012:MyIoTButtonSNSTopic"
                                        }
                                    }
                                ],
                                "condition": "$variable.pressureThresholdBreached > 1"
                            }
```

```
                        ]
                    },
                    "onExit": {
                        "events": [
                            {
                                "eventName": "Normal Pressure Restored",
                                "actions": [
                                    {
                                        "sns": {
                                            "targetArn": "arn:aws:sns:us-
west-2:123456789012:IoTVirtualButtonTopic"
                                        }
                                    }
                                ],
                                "condition": "true"
                            }
                        ]
                    }
                }
            ],
            "initialStateName": "Normal"
        }
    }
}
```

Senden Sie Eingaben, um das Detektormodell zu testen

Es gibt mehrere Möglichkeiten, Telemetriedaten zu empfangen AWS IoT Events (siehe Unterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen). In diesem Thema erfahren Sie, wie Sie in der AWS IoT Konsole eine AWS IoT Regel erstellen, die Nachrichten als Eingaben an Ihren AWS IoT Events Detektor weiterleitet. Sie können den MQTT Client der AWS IoT Konsole verwenden, um Testnachrichten zu senden. Mit dieser Methode können Sie Telemetriedaten darüber abrufen AWS IoT Events , wann Ihre Geräte MQTT Nachrichten über den AWS IoT Message Broker senden können.

Um Eingaben zu senden, um das Detektormodell zu testen

1. Öffnen Sie die AWS IoT Core -Konsole. Wählen Sie im linken Navigationsbereich unter Verwalten die Option Nachrichtenweiterleitung und anschließend Regeln aus.
2. Wählen Sie oben rechts Regel erstellen aus.

3. Führen Sie auf der Seite Regel erstellen die folgenden Schritte aus:

   1. Schritt 1. Geben Sie die Eigenschaften der Regel an. Füllen Sie die folgenden Felder aus:
      - Name der Regel. Geben Sie einen Namen für Ihre Regel ein, z. `MyIoTEventsRule` B.

        > **Note**
        > Verwenden Sie keine Leerzeichen.

      - Beschreibung der Regel. Dieser Schritt ist optional.
      - Wählen Sie Weiter.
   2. Schritt 2. SQLAnweisung konfigurieren. Füllen Sie die folgenden Felder aus:
      - SQLVersion. Wählen Sie die entsprechende Option aus der Liste aus.
      - SQLAussage. Geben Sie **`SELECT *, topic(2) as motorid FROM 'motors/+/status'`** ein.

      Wählen Sie Weiter.
   3. Schritt 3. Regelaktionen anhängen. Gehen Sie im Abschnitt Regelaktionen wie folgt vor:
      - Aktion 1. Wählen Sie IoT Events aus. Die folgenden Felder werden angezeigt:
        a. Geben Sie den Namen ein. Wählen Sie die entsprechende Option aus der Liste aus. Wenn Ihre Eingabe nicht angezeigt wird, wählen Sie Aktualisieren.

           Um eine neue Eingabe zu erstellen, wählen Sie Create IoT Events input aus. Füllen Sie die folgenden Felder aus:
           - Geben Sie den Namen ein. Geben Sie `PressureInput` ein.
           - Beschreibung. Dieser Schritt ist optional.
           - Laden Sie eine JSON Datei hoch. Laden Sie eine Kopie Ihrer JSON Datei hoch. Auf diesem Bildschirm befindet sich ein Link zu einer Beispieldatei, falls Sie keine Datei haben. Der Code beinhaltet:

```
{
  "motorid": "Fulton-A32",
  "sensorData": {
    "pressure": 23,
    "temperature": 47
  }
```

```
}
```

- Wählen Sie Eingabeattribute. Wählen Sie die entsprechende (n) Option (en) aus.
- Tags. Dieser Schritt ist optional.

Wählen Sie Create (Erstellen) aus.

Kehren Sie zum Bildschirm Regel erstellen zurück und aktualisieren Sie das Feld Eingabename. Wählen Sie die Eingabe aus, die Sie gerade erstellt haben.

b. Batch-Modus. Dieser Schritt ist optional. Wenn es sich bei der Payload um eine Reihe von Nachrichten handelt, wählen Sie diese Option.

c. Nachrichten-ID. Dies ist zwar optional, wird aber empfohlen.

d. IAMRolle. Wählen Sie die entsprechende Rolle aus der Liste aus. Wenn die Rolle nicht aufgeführt ist, wählen Sie Neue Rolle erstellen.

Geben Sie einen Rollennamen ein und wählen Sie Erstellen aus.

Um eine weitere Regel hinzuzufügen, wählen Sie Regelaktion hinzufügen

- Fehleraktion. Dieser Abschnitt ist optional. Um eine Aktion hinzuzufügen, wählen Sie Fehleraktion hinzufügen und wählen Sie die entsprechende Aktion aus der Liste aus.

  Füllen Sie die angezeigten Felder aus.

- Wählen Sie Weiter.

4. Schritt 4. Überprüfen und erstellen. Überprüfen Sie die Informationen auf dem Bildschirm und wählen Sie Erstellen.

4. Wählen Sie im linken Navigationsbereich unter Test die Option MQTTTest Client aus.

5. Wählen Sie Publish to topic (In Thema veröffentlichen) aus. Füllen Sie die folgenden Felder aus:

   - Name des Themas. Geben Sie einen Namen ein, um die Nachricht zu identifizieren, z. `motors/Fulton-A32/status` B.
   - Nutzlast der Nachricht. Geben Sie Folgendes ein:

```
{
  "messageId": 100,
  "sensorData": {
    "pressure": 39
  }
```

```
}
```

> **Note**
>
> Ändern Sie die `messageId` jedes Mal, wenn Sie eine neue Nachricht veröffentlichen.

6. Behalten Sie für Publish das gleiche Thema bei, ändern Sie das `"pressure"` in der Payload jedoch auf einen Wert, der über dem Schwellenwert liegt, den Sie im Detektormodell angegeben haben (z. B.**85**).
7. Wählen Sie Publish.

Die von Ihnen erstellte Detektor-Instance generiert und sendet Ihnen eine SNS Amazon-Nachricht. Senden Sie weiterhin Nachrichten mit Druckwerten über oder unter dem Druckgrenzwert (70 in diesem Beispiel), um zu sehen, wie der Detektor in Betrieb ist.

In diesem Beispiel müssen Sie drei Nachrichten mit Druckwerten unter dem Schwellenwert senden, um in den Normalzustand zurückzukehren und eine SNS Amazon-Nachricht zu erhalten, die darauf hinweist, dass der Überdruck behoben wurde. Sobald der Melder wieder im Normalzustand ist, wechselt der Melder durch eine Meldung mit einem Druckwert über dem Grenzwert in den Status Gefährlich und sendet eine SNS Amazon-Nachricht, die auf diesen Zustand hinweist.

Nachdem Sie nun ein einfaches Eingabe- und Meldermodell erstellt haben, versuchen Sie Folgendes.

- Weitere Beispiele (Vorlagen) für Detektormodelle finden Sie auf der Konsole.
- Folgen Sie den Schritten unterEinfaches step-by-step Beispiel, um ein Eingabe- und Detektormodell mit dem zu erstellen AWS CLI
- Erfahren Sie mehr über das, Ausdrücke zum Filtern, Transformieren und Verarbeiten von Ereignisdaten was in Ereignissen verwendet wird.
- Erfahren Sie mehr über Unterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen.
- Wenn etwas nicht funktioniert, finden Sie weitere Informationen unterProblembehebung AWS IoT Events.

Bewährte Verfahren für AWS IoT Events

Folgen Sie diesen bewährten Methoden, um den größtmöglichen Nutzen daraus zu ziehen AWS IoT Events.

Themen

Aktivieren Sie die CloudWatch Amazon-Protokollierung bei der Entwicklung von AWS IoT Events Detektormodellen

Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Damit CloudWatch erhalten Sie systemweiten Einblick in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand. Wenn Sie ein AWS IoT Events Detektormodell entwickeln oder debuggen, CloudWatch wissen Sie, was AWS IoT Events gerade passiert und welche Fehler dabei auftreten.

Um zu aktivieren CloudWatch

1. Falls Sie dies noch nicht getan haben, folgen Sie den Schritten unter Berechtigungen einrichten für AWS IoT Events So erstellen Sie eine Rolle mit einer angehängten Richtlinie, die die Berechtigung zum Erstellen und Verwalten von CloudWatch Protokollen für erteilt AWS IoT Events.
2. Rufen Sie die AWS IoT Events -Konsole auf.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen Sie auf der Seite Einstellungen die Option Bearbeiten aus.
5. Gehen Sie auf der Seite Protokollierungsoptionen bearbeiten im Abschnitt Protokollierungsoptionen wie folgt vor:

    a. Wählen Sie unter Ausführlichkeitsgrad eine Option aus.

    b. Wählen Sie unter Rolle auswählen eine Rolle aus, die über ausreichende Berechtigungen verfügt, um die von Ihnen ausgewählten Protokollierungsaktionen durchzuführen.

c. (Optional) Wenn Sie Debug als Ausführlichkeitsstufe ausgewählt haben, können Sie Debug-Ziele hinzufügen, indem Sie wie folgt vorgehen:

   i. Wählen Sie unter Debug-Ziele die Option Modelloption hinzufügen aus.

   ii. Geben Sie einen Modellnamen für den Detektor ein und (optional) KeyValue, um die Meldermodelle und spezifischen Melder (Instanzen) anzugeben, die protokolliert werden sollen.

6. Wählen Sie Aktualisieren.

Ihre Protokollierungsoptionen wurden erfolgreich aktualisiert.

Veröffentlichen Sie regelmäßig, um Ihr Meldermodell zu speichern, wenn Sie in der AWS IoT Events Konsole arbeiten

Wenn Sie die AWS IoT Events Konsole verwenden, werden Ihre laufenden Arbeiten lokal in Ihrem Browser gespeichert. Sie müssen jedoch Veröffentlichen wählen, um Ihr Meldermodell zu speichern AWS IoT Events. Nachdem Sie ein Detektormodell veröffentlicht haben, ist Ihr veröffentlichtes Werk in jedem Browser verfügbar, den Sie für den Zugriff auf Ihr Konto verwenden.

> **Note**
>
> Wenn Sie Ihr Werk nicht veröffentlichen, wird es nicht gespeichert. Nachdem Sie ein Detektormodell veröffentlicht haben, können Sie seinen Namen nicht mehr ändern. Sie können seine Definition jedoch weiter ändern.

Tutorials für AWS IoT Events Anwendungsfälle

In diesem Kapitel erfahren Sie, wie Sie:

- Holen Sie sich Hilfe bei der Entscheidung, welche Zustände in Ihr Detektormodell aufgenommen werden sollen, und bestimmen Sie, ob Sie eine oder mehrere Detektorinstanzen benötigen.
- Folgen Sie einem Beispiel, das den verwendet AWS CLI.
- Erstellen Sie einen Eingang für den Empfang von Telemetriedaten von einem Gerät und einem Detektormodell, um den Status des Geräts, das diese Daten sendet, zu überwachen und darüber zu berichten.
- Informieren Sie sich über die Einschränkungen und Einschränkungen in Bezug auf Eingänge, Meldermodelle und den AWS IoT Events Service.
- Sehen Sie sich ein komplexeres Beispiel für ein Detektormodell mit Kommentaren an.

Themen

Verwenden Sie AWS IoT Events zur Überwachung Ihrer IoT-Geräte

Sie können AWS IoT Events damit Ihre Geräte oder Prozesse überwachen und bei wichtigen Ereignissen Maßnahmen ergreifen. Gehen Sie dazu wie folgt vor:

Eingaben erstellen

Sie müssen über eine Möglichkeit verfügen, mit der Ihre Geräte und Prozesse Telemetriedaten abrufen können. AWS IoT Events Sie tun dies, indem Sie Nachrichten als Eingaben an AWS IoT Events senden. Sie können Nachrichten auf verschiedene Arten als Eingaben senden:

- Verwenden Sie die BatchPutMessageOperation.
- Definieren Sie eine `iotEvents`Regelaktion für die AWS IoT Core Regel-Engine. Die Regelaktion leitet Nachrichtendaten aus Ihrer Eingabe an. AWS IoT Events

- Verwenden Sie in die CreateDatasetOperation AWS IoT Analytics, um einen Datensatz mit zu erstellen. `contentDeliveryRules` Diese Regeln spezifizieren die AWS IoT Events Eingabe, an die der Inhalt des Datensatzes automatisch gesendet wird.
- Definieren Sie eine iotEventsAktion in einem AWS IoT Events Detektormodell `onExit` oder in einem `transitionEvents` Ereignis. `onInput` Informationen über die Instanz des Detektormodells und das Ereignis, das die Aktion ausgelöst hat, werden als Eingabe mit dem von Ihnen angegebenen Namen an das System zurückgemeldet.

Bevor Ihre Geräte Daten auf diese Weise senden, müssen Sie einen oder mehrere Eingänge definieren. Geben Sie dazu jeder Eingabe einen Namen und geben Sie an, welche Felder in den eingehenden Nachrichtendaten von der Eingabe überwacht werden. AWS IoT Events erhält seine Eingabe in Form von JSON Nutzdaten aus vielen Quellen. Jede Eingabe kann eigenständig bearbeitet oder mit anderen Eingaben kombiniert werden, um komplexere Ereignisse zu erkennen.

Erstellen Sie ein Detektormodell

Definieren Sie mithilfe von Zuständen ein Detektormodell (ein Modell Ihrer Ausrüstung oder Ihres Prozesses). Für jeden Zustand definieren Sie eine bedingte (boolesche) Logik, die die eingehenden Eingaben auswertet, um signifikante Ereignisse zu erkennen. Wenn ein Ereignis erkannt wird, kann es den Status ändern oder mithilfe anderer AWS Dienste benutzerdefinierte oder vordefinierte Aktionen auslösen. Sie können zusätzliche Ereignisse definieren, die Aktionen auslösen, wenn Sie einen Status betreten oder verlassen und optional, wenn eine Bedingung erfüllt ist.

In diesem Tutorial senden Sie eine SNS Amazon-Nachricht als Aktion, wenn das Modell in einen bestimmten Status eintritt oder diesen verlässt.

Überwachen Sie ein Gerät oder einen Prozess

Wenn Sie mehrere Geräte oder Prozesse überwachen, geben Sie in jeder Eingabe ein Feld an, das das jeweilige Gerät oder den Prozess identifiziert, von dem die Eingabe stammt. (Siehe das `key` Feld unter`CreateDetectorModel`.) Wenn ein neues Gerät identifiziert wird (ein neuer Wert wird in dem Eingabefeld angezeigt, das durch den identifiziert wird`key`), wird ein Detektor erzeugt. (Jeder Detektor ist eine Instanz des Detektormodells.) Dann reagiert der neue Detektor weiterhin auf Eingaben von diesem Gerät, bis sein Meldermodell aktualisiert oder gelöscht wird.

Wenn Sie einen einzelnen Prozess überwachen (auch wenn mehrere Geräte oder Unterprozesse Eingaben senden), geben Sie kein eindeutiges `key` Identifikationsfeld an. In diesem Fall wird ein einzelner Detektor (Instanz) erstellt, wenn die erste Eingabe eintrifft.

Senden Sie Nachrichten als Eingaben an Ihr Detektormodell

Es gibt mehrere Möglichkeiten, eine Nachricht von einem Gerät oder Prozess als Eingabe in einen AWS IoT Events Detektor zu senden, ohne dass Sie die Nachricht zusätzlich formatieren müssen. In diesem Tutorial verwenden Sie die AWS IoT Konsole, um eine AWS IoT Events Aktionsregel für die AWS IoT Core Regel-Engine zu schreiben, in AWS IoT Events die Ihre Nachrichtendaten weitergeleitet werden. Dazu identifizieren Sie die Eingabe anhand des Namens. Anschließend verwenden Sie weiterhin die AWS IoT Konsole, um einige Nachrichten zu generieren, an die Sie als Eingaben weitergeleitet werden AWS IoT Events.

Woher wissen Sie, welche Zustände Sie in einem Detektormodell benötigen?

Um zu bestimmen, welche Zustände Ihr Detektormodell haben sollte, entscheiden Sie zunächst, welche Maßnahmen Sie ergreifen können. Wenn Ihr Auto beispielsweise mit Benzin betrieben wird, schauen Sie bei Fahrtantritt auf die Tankanzeige, ob Sie tanken müssen. Hier haben Sie eine Aktion: Sagen Sie dem Fahrer, er solle „Gas holen“. Ihr Meldermodell benötigt zwei Zustände: „Auto benötigt keinen Kraftstoff“ und „Auto benötigt Kraftstoff“. Im Allgemeinen möchten Sie einen Status für jede mögliche Aktion und einen weiteren für den Fall definieren, dass keine Aktion erforderlich ist. Das funktioniert auch dann, wenn die Aktion selbst komplizierter ist. Möglicherweise möchten Sie Informationen darüber suchen, wo sich die nächstgelegene Tankstelle oder der günstigste Preis befindet, und diese Informationen hinzufügen, aber Sie tun dies, wenn Sie die Nachricht „Geh tanken“ senden.

Um zu entscheiden, welchen Status Sie als Nächstes eingeben möchten, schauen Sie sich die Eingaben an. Die Eingaben enthalten die Informationen, die Sie benötigen, um zu entscheiden, in welchem Zustand Sie sich befinden sollten. Um eine Eingabe zu erstellen, wählen Sie eines oder mehrere Felder in einer von Ihrem Gerät oder Prozess gesendeten Nachricht aus, die Ihnen bei der Entscheidung helfen. In diesem Beispiel benötigen Sie eine Eingabe, die Ihnen den aktuellen Kraftstoffstand („Prozent voll“) anzeigt. Vielleicht sendet Ihnen Ihr Auto mehrere verschiedene Nachrichten mit jeweils unterschiedlichen Feldern. Um diese Eingabe zu erstellen, müssen Sie die Nachricht und das Feld auswählen, das den aktuellen Füllstand der Gasanzeige anzeigt. Die Länge der Reise, die Sie unternehmen werden („Entfernung zum Ziel“), kann aus Gründen der Übersichtlichkeit fest codiert werden. Sie können Ihre durchschnittliche Reisedauer verwenden. Auf der Grundlage der Eingabe führen Sie einige Berechnungen durch (wie viele Gallonen entspricht dieser volle Prozentsatz? ist die durchschnittliche Reisedauer größer als die Meilen, die Sie zurücklegen können, wenn man die Gallonen berücksichtigt, die Sie haben, und Ihren

durchschnittlichen „Meilen pro Gallone“. Sie führen diese Berechnungen durch und senden bei Ereignissen Nachrichten.

Bisher haben Sie zwei Zustände und eine Eingabe. Sie benötigen ein Ereignis im ersten Status, das die Berechnungen auf der Grundlage der Eingabe durchführt und entscheidet, ob in den zweiten Status übergegangen werden soll. Das ist ein Übergangsereignis. (`transitionEvents`befinden sich in der `onInput` Ereignisliste eines Bundesstaates. Beim Empfang einer Eingabe in diesem ersten Zustand wechselt das Ereignis in den zweiten Status, sofern der Zustand des Ereignisses erfüllt `condition` ist.) Wenn Sie den zweiten Status erreichen, senden Sie die Nachricht, sobald Sie den Status betreten. (Sie verwenden ein `onEnter` Ereignis. Beim Eintritt in den zweiten Status sendet dieses Ereignis die Nachricht. Sie müssen nicht warten, bis eine weitere Eingabe eintrifft.) Es gibt auch andere Arten von Ereignissen, aber das ist alles, was Sie für ein einfaches Beispiel benötigen.

Die anderen Arten von Ereignissen sind `onExit` und`onInput`. Sobald eine Eingabe eingeht und die Bedingung erfüllt ist, führt ein `onInput` Ereignis die angegebenen Aktionen aus. Wenn ein Vorgang seinen aktuellen Status verlässt und die Bedingung erfüllt ist, führt das `onExit` Ereignis die angegebenen Aktionen aus.

Fehlt dir etwas? Ja, wie kehrt man zum ersten Zustand „Auto braucht keinen Kraftstoff“ zurück? Nachdem Sie Ihren Benzintank gefüllt haben, zeigt der Eingang an, dass der Tank voll ist. In Ihrem zweiten Zustand benötigen Sie ein Übergangsereignis, das zum ersten Zustand zurückkehrt. Dieses Ereignis tritt ein, wenn die Eingabe empfangen wird (in den `onInput:` Ereignissen des zweiten Zustands). Es sollte in den ersten Zustand zurückkehren, wenn die Berechnungen ergeben, dass Sie jetzt genug Benzin haben, um dorthin zu gelangen, wo Sie hin möchten.

Das sind die Grundlagen. Einige Detektormodelle werden komplexer, wenn sie Zustände hinzufügen, die wichtige Eingaben widerspiegeln, nicht nur mögliche Aktionen. In einem Detektormodell, das die Temperatur erfasst, könnten beispielsweise drei Zustände vorliegen: ein „normaler“ Zustand, ein „zu heißer“ Zustand und ein Zustand mit „potenziellem Problem“. Sie gehen in den potenziellen Problemzustand über, wenn die Temperatur über ein bestimmtes Niveau steigt, aber noch nicht zu heiß geworden ist. Sie möchten keinen Alarm senden, es sei denn, die Temperatur bleibt länger als 15 Minuten bei dieser Temperatur. Wenn sich die Temperatur vorher wieder normalisiert hat, geht der Melder wieder in den Normalzustand über. Wenn der Timer abläuft, wechselt der Melder in den zu heißen Zustand und sendet einen Alarm, nur um vorsichtig zu sein. Sie könnten dasselbe tun, indem Sie Variablen und einen komplexeren Satz von Ereignisbedingungen verwenden. Oft ist es jedoch einfacher, einen anderen Status zu verwenden, um die Ergebnisse Ihrer Berechnungen tatsächlich zu speichern.

Woher wissen Sie, ob Sie eine oder mehrere Instanzen eines Detektors benötigen?

Um zu entscheiden, wie viele Instanzen Sie benötigen, fragen Sie sich: „Was möchten Sie wissen?“ Nehmen wir an, Sie möchten wissen, wie das Wetter heute ist. Regnet es (Bundesstaat)? Müssen Sie einen Regenschirm mitnehmen (Aktion)? Sie können einen Sensor verwenden, der die Temperatur meldet, einen anderen, der die Luftfeuchtigkeit meldet, und andere, die den Luftdruck, die Windgeschwindigkeit und -richtung sowie den Niederschlag melden. Sie müssen jedoch alle diese Sensoren gemeinsam überwachen, um den Wetterzustand (Regen, Schnee, Bewölkung, Sonne) und die entsprechenden Maßnahmen zu ermitteln (nehmen Sie sich einen Regenschirm oder tragen Sie Sonnencreme auf). Trotz der Anzahl der Sensoren möchten Sie, dass eine Melderinstanz den Wetterstatus überwacht und Sie darüber informiert, welche Maßnahmen zu ergreifen sind.

Wenn Sie jedoch für die Wettervorhersage in Ihrer Region verantwortlich sind, verfügen Sie möglicherweise über mehrere Instanzen solcher Sensoranordnungen, die sich an verschiedenen Orten in der Region befinden. Die Menschen an jedem Standort müssen wissen, wie das Wetter an diesem Ort ist. In diesem Fall benötigen Sie mehrere Instanzen Ihres Melders. Die von jedem Sensor an jedem Standort gemeldeten Daten müssen ein Feld enthalten, das Sie als `key` Feld festgelegt haben. Dieses Feld ermöglicht es, eine Melderinstanz für den Bereich AWS IoT Events zu erstellen und diese Informationen dann weiterhin an diese Melderinstanz weiterzuleiten, sobald sie eintreffen. Keine ruinierten Haare oder sonnenverbrannten Nasen mehr!

Im Grunde benötigen Sie eine Melderinstanz, wenn Sie eine Situation (einen Prozess oder einen Standort) überwachen müssen. Wenn Sie viele Situationen (Standorte, Prozesse) überwachen müssen, benötigen Sie mehrere Melderinstanzen.

Einfaches step-by-step Beispiel

In diesem Beispiel rufen wir die AWS CLI Befehle AWS IoT Events APIs using auf, um einen Detektor zu erstellen, der zwei Zustände eines Motors modelliert: einen Normalzustand und einen Überdruckzustand.

Wenn der gemessene Druck im Motor einen bestimmten Schwellenwert überschreitet, wechselt das Modell in den Überdruckzustand und sendet eine Amazon Simple Notification Service (AmazonSNS) -Meldung, um einen Techniker über den Zustand zu informieren. Wenn der Druck bei drei aufeinanderfolgenden Druckmessungen unter den Schwellenwert fällt, kehrt das Modell in den Normalzustand zurück und sendet eine weitere SNS Amazon-Nachricht als Bestätigung,

dass der Zustand behoben ist. Wir benötigen drei aufeinanderfolgende Messwerte unter dem Druckschwellenwert, um ein mögliches Stottern der Meldungen zu Überdruck/Normaldruck im Falle einer nichtlinearen Erholungsphase oder eines einmaligen anomalen Erholungswerts zu vermeiden.

Im Folgenden finden Sie eine Übersicht über die Schritte zur Erstellung des Melders.

Erstellen Sie Eingaben.

Um Ihre Geräte und Prozesse zu überwachen, müssen sie über eine Möglichkeit verfügen, Telemetriedaten in AWS IoT Events zu übertragen. Dies geschieht, indem Nachrichten als Eingaben an gesendet AWS IoT Events werden. Hierfür gibt es mehrere Möglichkeiten:

- Benutze die BatchPutMessageOperation. Diese Methode ist einfach, setzt jedoch voraus, dass Ihre Geräte oder Prozesse AWS IoT Events API über eine SDK oder die darauf zugreifen können AWS CLI.
- Schreiben Sie in AWS IoT Core eine AWS IoT Events Aktionsregel für die AWS IoT Core Regel-Engine, in AWS IoT Events die Ihre Nachrichtendaten weitergeleitet werden. Dadurch wird die Eingabe anhand des Namens identifiziert. Verwenden Sie diese Methode, wenn Ihre Geräte oder Prozesse Nachrichten senden können oder dies bereits tun AWS IoT Core. Diese Methode erfordert in der Regel weniger Rechenleistung von einem Gerät.
- Verwenden Sie die CreateDatasetOperation AWS IoT Analytics, um einen Datensatz mit `contentDeliveryRules` Angabe der AWS IoT Events Eingabe zu erstellen, wobei der Inhalt des Datensatzes automatisch gesendet wird. Verwenden Sie diese Methode, wenn Sie Ihre Geräte oder Prozesse auf der Grundlage aggregierter oder analysierter Daten steuern möchten. AWS IoT Analytics

Bevor Ihre Geräte Daten auf diese Weise senden können, müssen Sie eine oder mehrere Eingaben definieren. Geben Sie dazu jeder Eingabe einen Namen und geben Sie an, welche Felder in den eingehenden Nachrichtendaten von der Eingabe überwacht werden sollen.

Erstellen Sie ein Detektormodell

Erstellen Sie mithilfe von Zuständen ein Detektormodell (ein Modell Ihrer Ausrüstung oder Ihres Prozesses). Definieren Sie für jeden Status eine bedingte (boolesche) Logik, die die eingehenden Eingaben auswertet, um signifikante Ereignisse zu erkennen. Wenn ein Ereignis erkannt wird, kann es den Status ändern oder mithilfe anderer Dienste benutzerdefinierte oder vordefinierte Aktionen auslösen. AWS Sie können zusätzliche Ereignisse definieren, die Aktionen auslösen, wenn Sie einen Status betreten oder verlassen und optional, wenn eine Bedingung erfüllt ist.

Überwachen Sie mehrere Geräte oder Prozesse

Wenn Sie mehrere Geräte oder Prozesse überwachen und diese einzeln verfolgen möchten, geben Sie in jeder Eingabe ein Feld an, das das jeweilige Gerät oder den Prozess identifiziert, von dem die Eingabe stammt. Sehen Sie sich das `key` Feld in an`CreateDetectorModel`. Wenn ein neues Gerät identifiziert wird (ein neuer Wert wird in dem durch das identifizierten Eingabefeld angezeigt`key`), wird eine Melderinstanz erstellt. Die neue Melderinstanz reagiert weiterhin auf Eingaben von diesem bestimmten Gerät, bis ihr Meldermodell aktualisiert oder gelöscht wird. Sie haben so viele eindeutige Detektoren (Instanzen), wie es eindeutige Werte in den `key` Eingabefeldern gibt.

Überwachen Sie ein einzelnes Gerät oder einen einzelnen Prozess

Wenn Sie einen einzelnen Prozess überwachen (auch wenn mehrere Geräte oder Unterprozesse Eingaben senden), geben Sie kein eindeutiges `key` Identifikationsfeld an. In diesem Fall wird ein einzelner Detektor (Instanz) erstellt, wenn die erste Eingabe eintrifft. Beispielsweise könnten Sie in jedem Raum eines Hauses Temperatursensoren haben, aber nur eine HVAC Einheit, um das gesamte Haus zu heizen oder zu kühlen. Sie können dies also nur als einen einzigen Vorgang steuern, auch wenn jeder Raumnutzer möchte, dass seine Stimme (Eingabe) Vorrang hat.

Senden Sie Nachrichten von Ihren Geräten oder Prozessen als Eingaben in Ihr Meldermodell

In den Eingängen haben wir die verschiedenen Möglichkeiten beschrieben, eine Nachricht von einem Gerät oder Prozess als Eingabe in einen AWS IoT Events Detektor zu senden. Nachdem Sie die Eingänge erstellt und das Detektormodell erstellt haben, können Sie mit dem Senden von Daten beginnen.

> **Note**
>
> Wenn Sie ein Meldermodell erstellen oder ein vorhandenes aktualisieren, dauert es einige Minuten, bis das neue oder aktualisierte Meldermodell Nachrichten empfängt und Melder (Instanzen) erstellt. Wenn das Meldermodell aktualisiert wird, kann es sein, dass Sie während dieser Zeit weiterhin ein Verhalten beobachten, das auf der vorherigen Version basiert.

Themen

- Sendet Nachrichten als Eingaben an einen Detektor

Erstellen Sie einen Eingang zur Erfassung von Gerätedaten

Nehmen wir als Beispiel an, Ihre Geräte senden Nachrichten im folgenden Format.

```
{
  "motorid": "Fulton-A32",
  "sensorData": {
    "pressure": 23,
    "temperature": 47
  }
}
```

Mit dem folgenden AWS CLI Befehl können Sie eine Eingabe erstellen, um die `pressure` Daten und die `motorid` (die das spezifische Gerät identifiziert, das die Nachricht gesendet hat) zu erfassen.

```
aws iotevents create-input  --cli-input-json file://pressureInput.json
```

Die Datei `pressureInput.json` enthält Folgendes.

```
{
  "inputName": "PressureInput",
  "inputDescription": "Pressure readings from a motor",
  "inputDefinition": {
    "attributes": [
      { "jsonPath": "sensorData.pressure" },
      { "jsonPath": "motorid" }
    ]
  }
}
```

Wenn Sie Ihre eigenen Eingaben erstellen, denken Sie daran, zunächst Beispielnachrichten als JSON Dateien von Ihren Geräten oder Prozessen zu sammeln. Sie können sie verwenden, um eine Eingabe über die Konsole oder die zu erstellenCLI.

Erstellen Sie ein Meldermodell zur Darstellung von Gerätezuständen

In Erstellen Sie einen Eingang zur Erfassung von Gerätedaten haben Sie ein auf einer Nachricht `input` basierendes System erstellt, das Druckdaten von einem Motor meldet. Um mit dem Beispiel fortzufahren: Hier ist ein Detektormodell, das auf ein Überdruckereignis in einem Motor reagiert.

Sie erstellen zwei Zustände: "`Normal`„und"`Dangerous`“. Jeder Detektor (Instanz) geht bei seiner Erstellung in den Zustand `Normal` "" über. Die Instanz wird erstellt, wenn eine Eingabe mit einem eindeutigen Wert für `key` "`motorid`" eingeht.

Wenn die Melderinstanz einen Druckwert von 70 oder mehr empfängt, wechselt sie in den Status `Dangerous` "" und sendet eine SNS Amazon-Nachricht als Warnung. Wenn die Druckwerte bei drei aufeinanderfolgenden Eingängen wieder normal sind (weniger als 70), kehrt der Detektor in den Zustand "`Normal`" zurück und sendet eine weitere SNS Amazon-Nachricht als Entwarnung.

Dieses Beispiel-Detektormodell geht davon aus, dass Sie zwei SNS Amazon-Themen erstellt haben, deren Amazon-Ressourcennamen (ARNs) in der Definition als `"targetArn": "arn:aws:sns:us-east-1:123456789012:underPressureAction"` und angezeigt werden`"targetArn": "arn:aws:sns:us-east-1:123456789012:pressureClearedAction"`.

Weitere Informationen finden Sie im Amazon Simple Notification Service Developer Guide und insbesondere in der Dokumentation des CreateTopicVorgangs in der Amazon Simple Notification Service API Reference.

In diesem Beispiel wird auch davon ausgegangen, dass Sie eine Rolle AWS Identity and Access Management (IAM) mit den entsprechenden Berechtigungen erstellt haben. Der ARN Wert dieser Rolle wird in der Definition des Detektormodells als angezeigt`"roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"`. Folgen Sie den Schritten unterBerechtigungen einrichten für AWS IoT Events, um diese Rolle zu erstellen, und kopieren Sie die ARN Rolle an die entsprechende Stelle in der Definition des Detektormodells.

Sie können das Detektormodell mit dem folgenden AWS CLI Befehl erstellen.

```
aws iotevents create-detector-model  --cli-input-json file://motorDetectorModel.json
```

Die Datei "`motorDetectorModel.json`" enthält Folgendes.

```
{
```

```
  "detectorModelName": "motorDetectorModel",
  "detectorModelDefinition": {
    "states": [
      {
        "stateName": "Normal",
        "onEnter": {
          "events": [
            {
              "eventName": "init",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "0"
                  }
                }
              ]
            }
          ]
        },
        "onInput": {
          "transitionEvents": [
            {
              "eventName": "Overpressurized",
              "condition": "$input.PressureInput.sensorData.pressure > 70",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "$variable.pressureThresholdBreached + 3"
                  }
                }
              ],
              "nextState": "Dangerous"
            }
          ]
        }
      },
      {
        "stateName": "Dangerous",
        "onEnter": {
          "events": [
            {
```

```
              "eventName": "Pressure Threshold Breached",
              "condition": "$variable.pressureThresholdBreached > 1",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-
east-1:123456789012:underPressureAction"
                  }
                }
              ]
            }
          ]
        },
        "onInput": {
          "events": [
            {
              "eventName": "Overpressurized",
              "condition": "$input.PressureInput.sensorData.pressure > 70",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "3"
                  }
                }
              ]
            },
            {
              "eventName": "Pressure Okay",
              "condition": "$input.PressureInput.sensorData.pressure <= 70",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "pressureThresholdBreached",
                    "value": "$variable.pressureThresholdBreached - 1"
                  }
                }
              ]
            }
          ],
          "transitionEvents": [
            {
              "eventName": "BackToNormal",
```

```
              "condition": "$input.PressureInput.sensorData.pressure <= 70 &&
 $variable.pressureThresholdBreached <= 1",
              "nextState": "Normal"
            }
          ]
        },
        "onExit": {
          "events": [
            {
              "eventName": "Normal Pressure Restored",
              "condition": "true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-
east-1:123456789012:pressureClearedAction"
                  }
                }
              ]
            }
          ]
        }
      }
    ],
    "initialStateName": "Normal"
  },
  "key" : "motorid",
  "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Sendet Nachrichten als Eingaben an einen Detektor

Sie haben jetzt eine Eingabe definiert, die die wichtigen Felder in Nachrichten identifiziert, die von einem Gerät gesendet werden (siehe Erstellen Sie einen Eingang zur Erfassung von Gerätedaten). Im vorherigen Abschnitt haben Sie eine erstellt, `detector model` die auf ein Überdruckereignis in einem Motor reagiert (siehe Erstellen Sie ein Meldermodell zur Darstellung von Gerätezuständen).

Um das Beispiel zu vervollständigen, senden Sie Nachrichten von einem Gerät (in diesem Fall einem Computer, auf dem der Computer AWS CLI installiert ist) als Eingänge an den Melder.

> **Note**
>
> Wenn Sie ein Meldermodell erstellen oder ein vorhandenes aktualisieren, dauert es einige Minuten, bis das neue oder aktualisierte Meldermodell Nachrichten empfängt und Melder (Instanzen) erstellt. Wenn Sie das Meldermodell aktualisieren, kann es sein, dass Sie während dieser Zeit weiterhin ein Verhalten beobachten, das auf der vorherigen Version basiert.

Verwenden Sie den folgenden AWS CLI Befehl, um eine Nachricht mit Daten zu senden, die den Schwellenwert überschreiten.

```
aws iotevents-data batch-put-message --cli-input-json file://highPressureMessage.json
 --cli-binary-format raw-in-base64-out
```

Die Datei "`highPressureMessage.json`" enthält Folgendes.

```
{
  "messages": [
    {
      "messageId": "00001",
      "inputName": "PressureInput",
      "payload": "{\"motorid\": \"Fulton-A32\", \"sensorData\": {\"pressure\": 80,
 \"temperature\": 39} }"
    }
  ]
}
```

Sie müssen das `messageId` in jeder gesendeten Nachricht ändern. Wenn Sie es nicht ändern, dedupliziert das AWS IoT Events System die Nachrichten. AWS IoT Events ignoriert eine Nachricht, wenn sie dieselbe enthält `messageID` wie eine andere Nachricht, die innerhalb der letzten fünf Minuten gesendet wurde.

An diesem Punkt wird ein Detektor (Instanz) erstellt, um Ereignisse für den Motor `"Fulton-A32"` zu überwachen. Dieser Detektor geht in den `"Normal"` Zustand über, in dem er erstellt wurde. Da wir jedoch einen Druckwert über dem Schwellenwert gesendet haben, geht er sofort in den `"Dangerous"` Zustand über. Dabei sendet der Detektor eine Nachricht an den SNS Amazon-Endpunkt, dessen ARN ist`arn:aws:sns:us-east-1:123456789012:underPressureAction`.

Führen Sie den folgenden AWS CLI Befehl aus, um eine Nachricht mit Daten zu senden, die unter dem Druckschwellenwert liegen.

```
aws iotevents-data batch-put-message --cli-input-json file://normalPressureMessage.json
 --cli-binary-format raw-in-base64-out
```

Die Datei `normalPressureMessage.json` enthält Folgendes.

```
{
  "messages": [
    {
      "messageId": "00002",
      "inputName": "PressureInput",
      "payload": "{\"motorid\": \"Fulton-A32\", \"sensorData\": {\"pressure\": 60,
 \"temperature\": 29} }"
    }
  ]
}
```

Sie müssen das `messageId` in der Datei jedes Mal ändern, wenn Sie den `BatchPutMessage` Befehl innerhalb von fünf Minuten aufrufen. Senden Sie die Nachricht noch zweimal. Nachdem die Nachricht dreimal gesendet wurde, sendet der Detektor (Instanz) für den Motor "`Fulton-A32`" eine Nachricht an den SNS Amazon-Endpunkt "`arn:aws:sns:us-east-1:123456789012:pressureClearedAction`" und wechselt erneut in den "`Normal`" Status.

> **Note**
>
> Sie können mehrere Nachrichten gleichzeitig mit `BatchPutMessage` senden. Die Reihenfolge, in der diese Nachrichten verarbeitet werden, kann jedoch nicht garantiert werden. Um sicherzustellen, dass Nachrichten (Eingaben) in der richtigen Reihenfolge verarbeitet werden, senden Sie sie nacheinander und warten Sie bei jedem Aufruf auf eine erfolgreiche Antwort. API

Im Folgenden finden Sie Beispiele für SNS Nachrichtennutzdaten, die mit dem in diesem Abschnitt beschriebenen Detektormodell erstellt wurden.

bei Ereignis „Druckschwellenwert überschritten“

```
IoT> {
  "eventTime":1558129816420,
  "payload":{
    "actionExecutionId":"5d7444df-a655-3587-a609-dbd7a0f55267",
    "detector":{
      "detectorModelName":"motorDetectorModel",
      "keyValue":"Fulton-A32",
      "detectorModelVersion":"1"
    },
    "eventTriggerDetails":{
      "inputName":"PressureInput",
      "messageId":"00001",
      "triggerType":"Message"
    },
    "state":{
      "stateName":"Dangerous",
      "variables":{
        "pressureThresholdBreached":3
      },
      "timers":{}
    }
  },
  "eventName":"Pressure Threshold Breached"
}
```

bei Ereignis „Normaldruck wiederhergestellt“

```
IoT> {
  "eventTime":1558129925568,
  "payload":{
    "actionExecutionId":"7e25fd38-2533-303d-899f-c979792a12cb",
    "detector":{
      "detectorModelName":"motorDetectorModel",
      "keyValue":"Fulton-A32",
      "detectorModelVersion":"1"
    },
    "eventTriggerDetails":{
      "inputName":"PressureInput",
      "messageId":"00004",
      "triggerType":"Message"
    },
    "state":{
      "stateName":"Dangerous",
```

```
      "variables":{
        "pressureThresholdBreached":0
      },
      "timers":{}
    }
  },
  "eventName":"Normal Pressure Restored"
}
```

Wenn Sie Timer definiert haben, wird deren aktueller Status auch in den SNS Nachrichten-Payloads angezeigt.

Die Nachrichtennutzdaten enthalten Informationen über den Status des Detektors (Instanz) zum Zeitpunkt des Sendens der Nachricht (d. h. zum Zeitpunkt der Ausführung der SNS Aktion). Sie können die https://docs.aws.amazon.com/iotevents/latest/apireference/API_iotevents-data_DescribeDetector.html Operation verwenden, um ähnliche Informationen über den Status des Melders zu erhalten.

Einschränkungen und Einschränkungen des Detektormodells

Bei der Erstellung eines Detektormodells sind die folgenden Punkte zu beachten.

Wie benutzt man das **`actions`** Feld

Das `actions` Feld ist eine Liste von Objekten. Sie können mehr als ein Objekt haben, aber in jedem Objekt ist nur eine Aktion zulässig.

Example

```
            "actions": [
              {
                "setVariable": {
                  "variableName": "pressureThresholdBreached",
                  "value": "$variable.pressureThresholdBreached - 1"
                }
              }
              {
                "setVariable": {
                  "variableName": "temperatureIsTooHigh",
                  "value": "$variable.temperatureIsTooHigh - 1"
                }
```

```
    }
  ]
```

Wie benutzt man das **`condition`** Feld

Das `condition` ist erforderlich für `transitionEvents` und in anderen Fällen optional.

Wenn das `condition` Feld nicht vorhanden ist, entspricht es`"condition": true`.

Das Ergebnis der Auswertung eines Bedingungsausdrucks sollte ein boolescher Wert sein. Wenn das Ergebnis kein boolescher Wert ist, entspricht es dem im Ereignis angegebenen Wert `false` und leitet den Übergang zu dem im `actions` Ereignis `nextState` angegebenen Wert nicht ein.

Verfügbarkeit von Variablenwerten

Wenn der Wert einer Variablen in einem Ereignis festgelegt wird, ist ihr neuer Wert standardmäßig nicht verfügbar oder wird nicht verwendet, um Bedingungen in anderen Ereignissen in derselben Gruppe auszuwerten. Der neue Wert ist nicht verfügbar oder wird in einer Ereignisbedingung im gleichen `onInput` `onExit` Feld `onEnter` oder verwendet.

Stellen Sie den `evaluationMethod` Parameter in der Definition des Detektormodells ein, um dieses Verhalten zu ändern. Wenn der auf gesetzt `evaluationMethod` ist`SERIAL`, werden Variablen aktualisiert und die Ereignisbedingungen werden in der Reihenfolge ausgewertet, in der die Ereignisse definiert sind. Andernfalls werden Variablen innerhalb eines Zustands aktualisiert, und Ereignisse innerhalb eines Zustands werden erst ausgeführt, wenn alle Ereignisbedingungen ausgewertet wurden, wenn für `BATCH` oder standardmäßig dieser Wert festgelegt ist. `evaluationMethod`

Der `"Dangerous"` Status im `onInput` Feld `"$variable.pressureThresholdBreached"` wird um eins verringert, wenn die `"Pressure Okay"` Bedingung erfüllt ist (wenn der aktuelle Eingangsdruck kleiner oder gleich 70 ist).

```
{
  "eventName": "Pressure Okay",
  "condition": "$input.PressureInput.sensorData.pressure <= 70",
  "actions": [
    {
      "setVariable": {
        "variableName": "pressureThresholdBreached",
        "value": "$variable.pressureThresholdBreached - 1"
      }
```

```
                }
              ]
            }
```

Der Detektor sollte wieder in den `"Normal"` Zustand zurückkehren, wenn 0 `"$variable.pressureThresholdBreached"` erreicht ist (d. h. wenn der Detektor drei aufeinanderfolgende Druckwerte erhalten hat, die kleiner oder gleich 70 sind). Das `"BackToNormal"` Ereignis `transitionEvents` muss testen, ob der Wert kleiner oder gleich 1 (nicht 0) `"$variable.pressureThresholdBreached"` ist. Außerdem muss erneut überprüft werden, ob der aktuelle Wert von kleiner oder gleich 70 `"$input.PressureInput.sensorData.pressure"` ist.

```
          "transitionEvents": [
            {
              "eventName": "BackToNormal",
              "condition": "$input.PressureInput.sensorData.pressure <= 70 &&
 $variable.pressureThresholdBreached <= 1",
              "nextState": "Normal"
            }
          ]
```

Andernfalls, wenn die Bedingung nur den Wert der Variablen prüft, würden zwei normale Messwerte, gefolgt von einer Überdruckmessung, die Bedingung erfüllen und in den `"Normal"` Zustand zurückkehren. Bei der Bedingung wird der Wert berücksichtigt, der bei der vorherigen Verarbeitung einer Eingabe angegeben `"$variable.pressureThresholdBreached"` wurde. Der Wert der Variablen wird in diesem `"Overpressurized"` Fall auf 3 zurückgesetzt, aber denken Sie daran, dass dieser neue Wert noch für niemanden verfügbar ist`condition`.

Standardmäßig `condition` kann jedes Mal, wenn ein Steuerelement das `onInput` Feld betritt, der Wert einer Variablen nur so sehen, wie er zu Beginn der Verarbeitung der Eingabe war, bevor er durch die unter angegebenen Aktionen geändert wird`onInput`. Das Gleiche gilt für `onEnter` und`onExit`. Jede Änderung, die an einer Variablen vorgenommen wird, wenn wir den Status betreten oder verlassen, ist nicht für andere Bedingungen verfügbar, die in denselben `onEnter` oder `onExit` -Feldern angegeben sind.

Latenz bei der Aktualisierung eines Detektormodells

Wenn Sie ein Detektormodell aktualisieren, löschen und neu erstellen (siehe UpdateDetectorModel), kommt es zu einer gewissen Verzögerung, bis alle generierten Detektoren

(Instanzen) gelöscht werden und das neue Modell zur Neuerstellung der Detektoren verwendet wird. Sie werden neu erstellt, nachdem das neue Detektormodell wirksam wird und neue Eingaben eintreffen. Während dieser Zeit werden Eingaben möglicherweise weiterhin von den Detektoren verarbeitet, die von der vorherigen Version des Detektormodells erzeugt wurden. Während dieses Zeitraums erhalten Sie möglicherweise weiterhin Warnmeldungen, die durch das vorherige Meldermodell definiert wurden.

Leerzeichen in den Eingabetasten

Leerzeichen sind in Eingabeschlüsseln zulässig, aber Verweise auf den Schlüssel müssen in Backticks eingeschlossen werden, und zwar sowohl in der Definition des Eingabeattributs als auch dann, wenn der Wert des Schlüssels in einem Ausdruck referenziert wird. Zum Beispiel bei einer Nachrichtennutzlast wie der folgenden:

```
{
  "motor id": "A32",
  "sensorData" {
    "motor pressure": 56,
    "motor temperature": 39
  }
}
```

Verwenden Sie Folgendes, um die Eingabe zu definieren.

```
{
  "inputName": "PressureInput",
  "inputDescription": "Pressure readings from a motor",
  "inputDefinition": {
    "attributes": [
      { "jsonPath": "sensorData.`motor pressure`" },
      { "jsonPath": "`motor id`" }
    ]
  }
}
```

In einem bedingten Ausdruck müssen Sie auch mithilfe von Backticks auf den Wert eines solchen Schlüssels verweisen.

```
$input.PressureInput.sensorData.`motor pressure`
```

Ein kommentiertes Beispiel: HVAC Temperaturkontrolle

Einige der folgenden JSON Beispieldateien enthalten eingebettete Kommentare, weshalb sie ungültig sindJSON. Vollständige Versionen dieser Beispiele ohne Kommentare finden Sie unterBeispiel: Verwendung der HVAC Temperatursteuerung.

Hintergrund

In diesem Beispiel wird ein Thermostatsteuerungsmodell implementiert, das Ihnen folgende Möglichkeiten bietet.

- Definieren Sie nur ein Meldermodell, das zur Überwachung und Steuerung mehrerer Bereiche verwendet werden kann. Für jeden Bereich wird eine Melderinstanz erstellt.
- Erfassen Sie Temperaturdaten von mehreren Sensoren in jedem Kontrollbereich.
- Ändern Sie den Temperatursollwert für einen Bereich.
- Stellen Sie die Betriebsparameter für jeden Bereich ein und setzen Sie diese Parameter zurück, während die Instanz verwendet wird.
- Dynamisches Hinzufügen oder Löschen von Sensoren aus einem Bereich.
- Geben Sie eine Mindestlaufzeit an, um Heiz- und Kühlgeräte zu schützen.
- Abnormale Sensormesswerte zurückweisen.
- Definieren Sie Notfall-Sollwerte, die sofort Heizen oder Kühlen einschalten, wenn ein Sensor eine Temperatur über oder unter einem bestimmten Schwellenwert meldet.
- Melden Sie anomale Messwerte und Temperaturspitzen.

Eingabedefinitionen für Detektormodelle

Wir möchten ein Detektormodell erstellen, mit dem wir die Temperatur in verschiedenen Bereichen überwachen und steuern können. Jeder Bereich kann mehrere Sensoren haben, die die Temperatur melden. Wir gehen davon aus, dass jeder Bereich von einer Heizeinheit und einer Kühleinheit versorgt wird, die ein- oder ausgeschaltet werden können, um die Temperatur in dem Bereich zu regeln. Jeder Bereich wird von einer Melderinstanz gesteuert.

Da die verschiedenen Bereiche, die wir überwachen und steuern, unterschiedliche Eigenschaften aufweisen können, die unterschiedliche Steuerparameter erfordern, definieren wir die `'seedTemperatureInput'` so, dass diese Parameter für jeden Bereich bereitgestellt

werden. Wenn wir eine dieser Eingangsnachrichten an senden AWS IoT Events, wird eine neue Detektormodellinstanz erstellt, die die Parameter enthält, die wir in diesem Bereich verwenden möchten. Hier ist die Definition dieser Eingabe.

CLIBefehl:

```
aws iotevents create-input --cli-input-json file://seedInput.json
```

Datei: `seedInput.json`

```
{
  "inputName": "seedTemperatureInput",
  "inputDescription": "Temperature seed values.",
  "inputDefinition": {
    "attributes": [
      { "jsonPath": "areaId" },
      { "jsonPath": "desiredTemperature" },
      { "jsonPath": "allowedError" },
      { "jsonPath": "rangeHigh" },
      { "jsonPath": "rangeLow" },
      { "jsonPath": "anomalousHigh" },
      { "jsonPath": "anomalousLow" },
      { "jsonPath": "sensorCount" },
      { "jsonPath": "noDelay" }
    ]
  }
}
```

Antwort:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/
seedTemperatureInput",
        "lastUpdateTime": 1557519620.736,
        "creationTime": 1557519620.736,
        "inputName": "seedTemperatureInput",
        "inputDescription": "Temperature seed values."
    }
}
```

Hinweise

- Für jedes in einer Nachricht `'areaId'` empfangene Unikat wird eine neue Detektorinstanz erstellt. Sehen Sie sich das `'key'` Feld in der `'areaDetectorModel'` Definition an.
- Die Durchschnittstemperatur kann `'desiredTemperature'` von dem abweichen, `'allowedError'` bevor die Heiz- oder Kühlgeräte für den Bereich aktiviert werden.
- Meldet ein Sensor eine Temperatur über dem`'rangeHigh'`, meldet der Melder einen Temperaturanstieg und startet sofort die Kühleinheit.
- Meldet ein Sensor eine Temperatur unter dem`'rangeLow'`, meldet der Melder einen Temperaturanstieg und startet sofort die Heizeinheit.
- Wenn ein Sensor eine Temperatur über `'anomalousHigh'` oder unter dem Wert meldet`'anomalousLow'`, meldet der Melder einen anomalen Sensorwert, ignoriert jedoch den gemeldeten Temperaturwert.
- Das `'sensorCount'` teilt dem Melder mit, wie viele Sensoren für den Bereich Bericht erstatten. Der Detektor berechnet die Durchschnittstemperatur in dem Gebiet, indem er jedem Temperaturmesswert, den er empfängt, den entsprechenden Gewichtungsfaktor zuweist. Aus diesem Grund muss der Detektor nicht nachverfolgen, was jeder Sensor meldet, und die Anzahl der Sensoren kann je nach Bedarf dynamisch geändert werden. Wenn jedoch ein einzelner Sensor offline geht, weiß der Melder dies nicht und berücksichtigt es auch nicht. Wir empfehlen Ihnen, ein anderes Meldermodell speziell für die Überwachung des Verbindungsstatus der einzelnen Sensoren zu erstellen. Zwei sich ergänzende Detektormodelle vereinfachen das Design beider.
- Der `'noDelay'` Wert kann `true` oder sein`false`. Nach dem Einschalten eines Heiz- oder Kühlgeräts sollte es für eine gewisse Mindestzeit eingeschaltet bleiben, um die Integrität des Geräts zu schützen und seine Lebensdauer zu verlängern. Wenn auf eingestellt `'noDelay'` ist`false`, erzwingt die Melderinstanz eine Verzögerung, bevor sie die Kühl- und Heizgeräte ausschaltet, um sicherzustellen, dass sie so lange wie möglich laufen. Die Anzahl der Sekunden der Verzögerung wurde in der Definition des Detektormodells fest codiert, da wir keinen Variablenwert verwenden können, um einen Timer einzustellen.

Der `'temperatureInput'` wird verwendet, um Sensordaten an eine Detektorinstanz zu übertragen.

CLIBefehl:

```
aws iotevents create-input --cli-input-json file://temperatureInput.json
```

Datei: `temperatureInput.json`

```
{
  "inputName": "temperatureInput",
  "inputDescription": "Temperature sensor unit data.",
  "inputDefinition": {
    "attributes": [
      { "jsonPath": "sensorId" },
      { "jsonPath": "areaId" },
      { "jsonPath": "sensorData.temperature" }
    ]
  }
}
```

Antwort:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/temperatureInput",
        "lastUpdateTime": 1557519707.399,
        "creationTime": 1557519707.399,
        "inputName": "temperatureInput",
        "inputDescription": "Temperature sensor unit data."
    }
}
```

Hinweise

- Die wird `'sensorId'` nicht von einer Beispiel-Detektorinstanz verwendet, um einen Sensor direkt zu steuern oder zu überwachen. Es wird automatisch an Benachrichtigungen weitergegeben, die von der Detektorinstanz gesendet werden. Von dort aus kann es verwendet werden, um die Sensoren zu identifizieren, die ausfallen (z. B. könnte ein Sensor, der regelmäßig ungewöhnliche Messwerte sendet, bald ausfallen) oder die offline gegangen sind (wenn er als Eingang für ein zusätzliches Meldermodell verwendet wird, das den Herzschlag des Geräts überwacht). `'sensorId'`Sie können auch dabei helfen, warme oder kalte Zonen in einem Gebiet zu identifizieren, wenn die Messwerte regelmäßig vom Durchschnitt abweichen.
- Das `'areaId'` wird verwendet, um die Daten des Sensors an die entsprechende Melderinstanz weiterzuleiten. Für jedes in einer Nachricht `'areaId'` empfangene Unikat wird eine

Detektorinstanz erstellt. Sehen Sie sich das `'key'` Feld in der `'areaDetectorModel'` Definition an.

Erstellen Sie eine Definition für ein Detektormodell

Das `'areaDetectorModel'` Beispiel enthält Kommentare in der Zeile.

CLIBefehl:

```
aws iotevents create-detector-model --cli-input-json file://areaDetectorModel.json
```

Datei: `areaDetectorModel.json`

```
{
  "detectorModelName": "areaDetectorModel",
  "detectorModelDefinition": {
    "states": [
      {
        "stateName": "start",
        // In the 'start' state we set up the operation parameters of the new detector
 instance.
        //   We get here when the first input message arrives. If that is a
 'seedTemperatureInput'
        //   message, we save the operation parameters, then transition to the 'idle'
 state. If
        //   the first message is a 'temperatureInput', we wait here until we get a
        //   'seedTemperatureInput' input to ensure our operation parameters are set.
 We can
        //   also reenter this state using the 'BatchUpdateDetector' API. This enables
 us to
        //   reset the operation parameters without needing to delete the detector
 instance.
        "onEnter": {
          "events": [
            {
              "eventName": "prepare",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
```

```
                    // initialize 'sensorId' to an invalid value (0) until an actual
sensor reading
                    //   arrives
                    "variableName": "sensorId",
                    "value": "0"
                  }
                },
                {
                  "setVariable": {
                    // initialize 'reportedTemperature' to an invalid value (0.1) until
an actual
                    //   sensor reading arrives
                    "variableName": "reportedTemperature",
                    "value": "0.1"
                  }
                },
                {
                  "setVariable": {
                    // When using 'BatchUpdateDetector' to re-enter this state, this
variable should
                    //   be set to true.
                    "variableName": "resetMe",
                    "value": "false"
                  }
                }
              ]
            }
          ]
        },
        "onInput": {
          "transitionEvents": [
            {
              "eventName": "initialize",
              "condition": "$input.seedTemperatureInput.sensorCount > 0",
              // When a 'seedTemperatureInput' message with a valid 'sensorCount' is
received,
              //   we use it to set the operational parameters for the area to be
monitored.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "rangeHigh",
                    "value": "$input.seedTemperatureInput.rangeHigh"
                  }
```

```
                },
                {
                  "setVariable": {
                    "variableName": "rangeLow",
                    "value": "$input.seedTemperatureInput.rangeLow"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                },
                {
                  "setVariable": {
                    // Assume we're at the desired temperature when we start.
                    "variableName": "averageTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "allowedError",
                    "value": "$input.seedTemperatureInput.allowedError"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "anomalousHigh",
                    "value": "$input.seedTemperatureInput.anomalousHigh"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "anomalousLow",
                    "value": "$input.seedTemperatureInput.anomalousLow"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "sensorCount",
                    "value": "$input.seedTemperatureInput.sensorCount"
                  }
                },
```

```
                {
                  "setVariable": {
                    "variableName": "noDelay",
                    "value": "$input.seedTemperatureInput.noDelay == true"
                  }
                }
              ],
              "nextState": "idle"
            },
            {
              "eventName": "reset",
              "condition": "($variable.resetMe == true) &&
($input.temperatureInput.sensorData.temperature < $variable.anomalousHigh &&
$input.temperatureInput.sensorData.temperature > $variable.anomalousLow)",
              // This event is triggered if we have reentered the 'start' state using
the
              //   'BatchUpdateDetector' API with 'resetMe' set to true. When we
reenter using
              //   'BatchUpdateDetector' we do not automatically continue to the 'idle'
state, but
              //   wait in 'start' until the next input message arrives. This event
enables us to
              //   transition to 'idle' on the next valid 'temperatureInput' message
that arrives.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "averageTemperature",
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ],
              "nextState": "idle"
            }
          ]
        },
        "onExit": {
          "events": [
            {
              "eventName": "resetHeatCool",
              "condition": "true",
              // Make sure the heating and cooling units are off before entering
'idle'.
```

```
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/Off"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/Off"
                  }
                }
              ]
            }
          ]
        }
      },


      {
        "stateName": "idle",
        "onInput": {
          "events": [
            {
              "eventName": "whatWasInput",
              "condition": "true",
              // By storing the 'sensorId' and the 'temperature' in variables, we make
them
              //   available in any messages we send out to report anomalies, spikes,
or just
              //   if needed for debugging.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "sensorId",
```

```
                    "value": "$input.temperatureInput.sensorId"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "reportedTemperature",
                    "value": "$input.temperatureInput.sensorData.temperature"
                  }
                }
              ]
            },
            {
              "eventName": "changeDesired",
              "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
              // This event enables us to change the desired temperature at any time by
sending a
              //   'seedTemperatureInput' message. But note that other operational
parameters are not
              //   read or changed.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                }
              ]
            },
            {
              "eventName": "calculateAverage",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
              // If a valid temperature reading arrives, we use it to update the
average temperature.
              //   For simplicity, we assume our sensors will be sending updates at
about the same rate,
              //   so we can calculate an approximate average by giving equal weight to
each reading we receive.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "averageTemperature",
```

```
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ]
            }
          ],
          "transitionEvents": [
            {
              "eventName": "anomalousInputArrived",
              "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
              // When an anomalous reading arrives, send an MQTT message, but stay in
the current state.
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/anomaly"
                  }
                }
              ],
              "nextState": "idle"
            },

            {
              "eventName": "highTemperatureSpike",
              "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
              // When even a single temperature reading arrives that is above the
'rangeHigh', take
              //   emergency action to begin cooling, and report a high temperature
spike.
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/spike"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
                  }
                },
```

```
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/On"
                  }
                },
                {
                  "setVariable": {
                    // This is necessary because we want to set a timer to delay the
shutoff
                    //   of a cooling/heating unit, but we only want to set the timer
when we
                    //   enter that new state initially.
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "cooling"
            },

            {
              "eventName": "lowTemperatureSpike",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
              // When even a single temperature reading arrives that is below the
'rangeLow', take
              //   emergency action to begin heating, and report a low-temperature
spike.
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/spike"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/On"
                  }
                },
```

```
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "heating"
            },

            {
              "eventName": "highTemperatureThreshold",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) >
($variable.desiredTemperature + $variable.allowedError))",
              // When the average temperature is above the desired temperature plus the
allowed error factor,
              //   it is time to start cooling. Note that we calculate the average
temperature here again
              //   because the value stored in the 'averageTemperature' variable is not
yet available for use
              //   in our condition.
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "cooling"
            },

            {
```

```
            "eventName": "lowTemperatureThreshold",
            "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) <
($variable.desiredTemperature - $variable.allowedError))",
            // When the average temperature is below the desired temperature minus
the allowed error factor,
            //   it is time to start heating. Note that we calculate the average
temperature here again
            //   because the value stored in the 'averageTemperature' variable is not
yet available for use
            //   in our condition.
            "actions": [
              {
                "sns": {
                  "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
                }
              },
              {
                "iotTopicPublish": {
                  "mqttTopic": "hvac/Heating/On"
                }
              },
              {
                "setVariable": {
                  "variableName": "enteringNewState",
                  "value": "true"
                }
              }
            ],
            "nextState": "heating"
          }
        ]
      }
    },


    {
      "stateName": "cooling",
      "onEnter": {
        "events": [
          {
            "eventName": "delay",
            "condition": "!$variable.noDelay && $variable.enteringNewState",
```

```
              // If the operational parameters specify that there should be a minimum
time that the
              //   heating and cooling units should be run before being shut off again,
we set
              //   a timer to ensure the proper operation here.
              "actions": [
                {
                  "setTimer": {
                    "timerName": "coolingTimer",
                    "seconds": 180
                  }
                },
                {
                  "setVariable": {
                    // We use this 'goodToGo' variable to store the status of the timer
expiration
                    //   for use in conditions that also use input variable values. If
                    //   'timeout()' is used in such mixed conditionals, its value is
lost.
                    "variableName": "goodToGo",
                    "value": "false"
                  }
                }
              ]
            },
            {
              "eventName": "dontDelay",
              "condition": "$variable.noDelay == true",
              // If the heating/cooling unit shutoff delay is not used, no need to
wait.
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            },
            {
              "eventName": "beenHere",
              "condition": "true",
              "actions": [
                {
```

```
                "setVariable": {
                  "variableName": "enteringNewState",
                  "value": "false"
                }
              }
            ]
          }
        ]
      },

      "onInput": {
        "events": [
          // These are events that occur when an input is received (if the condition
is
          //   satisfied), but don't cause a transition to another state.
          {
            "eventName": "whatWasInput",
            "condition": "true",
            "actions": [
              {
                "setVariable": {
                  "variableName": "sensorId",
                  "value": "$input.temperatureInput.sensorId"
                }
              },
              {
                "setVariable": {
                  "variableName": "reportedTemperature",
                  "value": "$input.temperatureInput.sensorData.temperature"
                }
              }
            ]
          },
          {
            "eventName": "changeDesired",
            "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
            "actions": [
              {
                "setVariable": {
                  "variableName": "desiredTemperature",
                  "value": "$input.seedTemperatureInput.desiredTemperature"
                }
              }
```

```
              ]
            },
            {
              "eventName": "calculateAverage",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "averageTemperature",
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ]
            },
            {
              "eventName": "areWeThereYet",
              "condition": "(timeout(\"coolingTimer\"))",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            }
          ],
          "transitionEvents": [
            // Note that some tests of temperature values (for example, the test for an
anomalous value)
            //   must be placed here in the 'transitionEvents' because they work
together with the tests
            //   in the other conditions to ensure that we implement the proper
"if..elseif..else" logic.
            //   But each transition event must have a destination state ('nextState'),
and even if that
            //   is actually the current state, the "onEnter" events for this state
will be executed again.
            //   This is the reason for the 'enteringNewState' variable and related.
            {
              "eventName": "anomalousInputArrived",
```

```
            "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/anomaly"
                }
              }
            ],
            "nextState": "cooling"
          },

          {
            "eventName": "highTemperatureSpike",
            "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/spike"
                }
              }
            ],
            "nextState": "cooling"
          },

          {
            "eventName": "lowTemperatureSpike",
            "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/spike"
                }
              },
              {
                "sns": {
                  "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
                }
              },
              {
                "sns": {
```

```
                "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
              }
            },
            {
              "iotTopicPublish": {
                "mqttTopic": "hvac/Cooling/Off"
              }
            },
            {
              "iotTopicPublish": {
                "mqttTopic": "hvac/Heating/On"
              }
            },
            {
              "setVariable": {
                "variableName": "enteringNewState",
                "value": "true"
              }
            }
          ],
          "nextState": "heating"
        },

        {
          "eventName": "desiredTemperature",
          "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) <=
($variable.desiredTemperature - $variable.allowedError)) && $variable.goodToGo ==
true",
          "actions": [
            {
              "sns": {
                "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
              }
            },
            {
              "iotTopicPublish": {
                "mqttTopic": "hvac/Cooling/Off"
              }
            }
          ],
          "nextState": "idle"
        }
      ]
```

```
        }
      },


      {
        "stateName": "heating",
        "onEnter": {
          "events": [
            {
              "eventName": "delay",
              "condition": "!$variable.noDelay && $variable.enteringNewState",
              "actions": [
                {
                  "setTimer": {
                    "timerName": "heatingTimer",
                    "seconds": 120
                  }
                },
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "false"
                  }
                }
              ]
            },
            {
              "eventName": "dontDelay",
              "condition": "$variable.noDelay == true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            },
            {
              "eventName": "beenHere",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
```

```
                    "variableName": "enteringNewState",
                    "value": "false"
                  }
                }
              ]
            }
          ]
        },

        "onInput": {
          "events": [
            {
              "eventName": "whatWasInput",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "sensorId",
                    "value": "$input.temperatureInput.sensorId"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "reportedTemperature",
                    "value": "$input.temperatureInput.sensorData.temperature"
                  }
                }
              ]
            },
            {
              "eventName": "changeDesired",
              "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                }
              ]
            },
            {
              "eventName": "calculateAverage",
```

```
            "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
            "actions": [
              {
                "setVariable": {
                  "variableName": "averageTemperature",
                  "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                }
              }
            ]
          },
          {
            "eventName": "areWeThereYet",
            "condition": "(timeout(\"heatingTimer\"))",
            "actions": [
              {
                "setVariable": {
                  "variableName": "goodToGo",
                  "value": "true"
                }
              }
            ]
          }
        ],
        "transitionEvents": [
          {
            "eventName": "anomalousInputArrived",
            "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/anomaly"
                }
              }
            ],
            "nextState": "heating"
          },

          {
            "eventName": "highTemperatureSpike",
```

```
              "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/spike"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/Off"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "cooling"
            },

            {
              "eventName": "lowTemperatureSpike",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
              "actions": [
                {
```

```
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/spike"
                  }
                }
              ],
              "nextState": "heating"
            },

            {
              "eventName": "desiredTemperature",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) >=
($variable.desiredTemperature + $variable.allowedError)) && $variable.goodToGo ==
true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/Off"
                  }
                }
              ],
              "nextState": "idle"
            }
          ]
        }
      }

    ],

    "initialStateName": "start"
  },
  "key": "areaId",
  "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Antwort:

```
{
```

```
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1557523491.168,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1557523491.168,
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
areaDetectorModel",
        "key": "areaId",
        "detectorModelName": "areaDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

BatchUpdateDetectorZum Aktualisieren verwenden

Sie können den `BatchUpdateDetector` Vorgang verwenden, um eine Detektorinstanz in einen bekannten Zustand zu versetzen, einschließlich Timer- und Variablenwerten. Im folgenden Beispiel werden die `BatchUpdateDetector` Betriebsparameter für einen Bereich zurückgesetzt, der unter Temperaturüberwachung und -steuerung steht. Mit diesem Vorgang können Sie dies tun, ohne das Meldermodell löschen, neu erstellen oder aktualisieren zu müssen.

CLIBefehl:

```
aws iotevents-data batch-update-detector --cli-input-json file://areaDM.BUD.json
```

Datei: `areaDM.BUD.json`

```
{
  "detectors": [
    {
      "messageId": "0001",
      "detectorModelName": "areaDetectorModel",
      "keyValue": "Area51",
      "state": {
        "stateName": "start",
        "variables": [
          {
            "name": "desiredTemperature",
            "value": "22"
          },
          {
```

```
            "name": "averageTemperature",
            "value": "22"
          },
          {
            "name": "allowedError",
            "value": "1.0"
          },
          {
            "name": "rangeHigh",
            "value": "30.0"
          },
          {
            "name": "rangeLow",
            "value": "15.0"
          },
          {
            "name": "anomalousHigh",
            "value": "60.0"
          },
          {
            "name": "anomalousLow",
            "value": "0.0"
          },
          {
            "name": "sensorCount",
            "value": "12"
          },
          {
            "name": "noDelay",
            "value": "true"
          },
          {
            "name": "goodToGo",
            "value": "true"
          },
          {
            "name": "sensorId",
            "value": "0"
          },
          {
            "name": "reportedTemperature",
            "value": "0.1"
          },
          {
```

```
            "name": "resetMe",
            // When 'resetMe' is true, our detector model knows that we have reentered
 the 'start' state
            //   to reset operational parameters, and will allow the next valid
 temperature sensor
            //   reading to cause the transition to the 'idle' state.
            "value": "true"
          }
        ],
        "timers": [
        ]
      }
    }
  ]
}
```

Antwort:

```
{
    "batchUpdateDetectorErrorEntries": []
}
```

BatchPutMessageFür Eingaben verwenden

Example 1

Verwenden Sie den `BatchPutMessage` Vorgang, um eine `"seedTemperatureInput"` Nachricht zu senden, in der die Betriebsparameter für einen bestimmten Bereich festgelegt werden, der temperaturgesteuert und überwacht wird. Jede Nachricht AWS IoT Events , die von dieser empfangen wird, hat zur `"areaId"` Folge, dass eine neue Melderinstanz erstellt wird. Die neue Melderinstanz ändert ihren Status jedoch nicht `"idle"` und beginnt erst, die Temperatur zu überwachen und Heiz- oder Kühlgeräte zu steuern, wenn eine `"seedTemperatureInput"` Meldung für den neuen Bereich eingeht.

CLIBefehl:

```
aws iotevents-data batch-put-message --cli-input-json file://seedExample.json --cli-
binary-format raw-in-base64-out
```

Datei: `seedExample.json`

```
{
  "messages": [
    {
      "messageId": "00001",
      "inputName": "seedTemperatureInput",
      "payload": "{\"areaId\": \"Area51\", \"desiredTemperature\": 20.0, \"allowedError
\": 0.7, \"rangeHigh\": 30.0, \"rangeLow\": 15.0, \"anomalousHigh\": 60.0,
 \"anomalousLow\": 0.0, \"sensorCount\": 10, \"noDelay\": false}"
    }
  ]
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Example

2

Verwenden Sie den `BatchPutMessage` Vorgang, um eine `"temperatureInput"` Nachricht zu senden, um Temperatursensordaten für einen Sensor in einem bestimmten Steuerungs- und Überwachungsbereich zu melden.

CLIBefehl:

```
aws iotevents-data batch-put-message --cli-input-json file://temperatureExample.json --
cli-binary-format raw-in-base64-out
```

Datei: `temperatureExample.json`

```
{
  "messages": [
    {
      "messageId": "00005",
      "inputName": "temperatureInput",
      "payload": "{\"sensorId\": \"05\", \"areaId\": \"Area51\", \"sensorData\":
 {\"temperature\": 23.12} }"
```

```
    }
  ]
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Example 3

Verwenden Sie den `BatchPutMessage` Vorgang, um eine `"seedTemperatureInput"` Nachricht zu senden, um den Wert der gewünschten Temperatur für einen bestimmten Bereich zu ändern.

CLIBefehl:

```
aws iotevents-data batch-put-message --cli-input-json file://seedSetDesiredTemp.json --
cli-binary-format raw-in-base64-out
```

Datei: `seedSetDesiredTemp.json`

```
{
  "messages": [
    {
      "messageId": "00001",
      "inputName": "seedTemperatureInput",
      "payload": "{\"areaId\": \"Area51\", \"desiredTemperature\": 23.0}"
    }
  ]
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Nachrichten aufnehmen MQTT

Wenn Ihre Sensordatenverarbeitungsressourcen das nicht verwenden können `"BatchPutMessage"`API, ihre Daten jedoch mithilfe eines MQTT Lightweight-Clients an den AWS IoT Core Message Broker senden können, können Sie eine AWS IoT Core Themenregel erstellen, um Nachrichtendaten an eine AWS IoT Events Eingabe umzuleiten. Im Folgenden finden Sie eine Definition einer AWS IoT Events Themenregel, die die Felder `"areaId"` und die `"sensorId"` Eingabefelder aus dem MQTT Thema und das `"sensorData.temperature"` Feld aus dem `"temp"` Nachrichten-Payload-Feld verwendet und diese Daten in unsere aufnimmt. AWS IoT Events `"temperatureInput"`

CLIBefehl:

```
aws iot create-topic-rule --cli-input-json file://temperatureTopicRule.json
```

Datei: `seedSetDesiredTemp.json`

```
{
  "ruleName": "temperatureTopicRule",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as areaId, topic(4) as sensorId, temp as
 sensorData.temperature FROM 'update/temperature/#'",
    "description": "Ingest temperature sensor messages into IoT Events",
    "actions": [
      {
        "iotEvents": {
          "inputName": "temperatureInput",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/anotheRole"
        }
      }
    ],
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23"
  }
}
```

Antwort: [keine]

Wenn der Sensor eine Nachricht zum Thema `"update/temperature/Area51/03"` mit der folgenden Nutzlast sendet.

```
{ "temp": 24.5 }
```

Dies führt dazu, dass Daten aufgenommen werden, AWS IoT Events als ob der folgende `"BatchPutMessage"` API Anruf getätigt worden wäre.

```
aws iotevents-data batch-put-message --cli-input-json file://spoofExample.json --cli-
binary-format raw-in-base64-out
```

Datei: `spoofExample.json`

```
{
  "messages": [
    {
      "messageId": "54321",
      "inputName": "temperatureInput",
      "payload": "{\"sensorId\": \"03\", \"areaId\": \"Area51\", \"sensorData\":
 {\"temperature\": 24.5} }"
    }
  ]
}
```

SNSAmazon-Nachrichten generieren

Im Folgenden finden Sie Beispiele für SNS Nachrichten, die von der `"Area51"` Detector-Instance generiert wurden.

```
Heating system off command> {
  "eventTime":1557520274729,
  "payload":{
    "actionExecutionId":"f3159081-bac3-38a4-96f7-74af0940d0a4",
    "detector":{

 "detectorModelName":"areaDetectorModel","keyValue":"Area51","detectorModelVersion":"1"},"event
{"inputName":"seedTemperatureInput","messageId":"00001","triggerType":"Message"},"state":
{"stateName":"start","variables":
{"sensorCount":10,"rangeHigh":30.0,"resetMe":false,"enteringNewState":true,"averageTemperature"
{}}},"eventName":"resetHeatCool"}
```

```
Cooling system off command> {"eventTime":1557520274729,"payload":
{"actionExecutionId":"98f6a1b5-8f40-3cdb-9256-93afd4d66192","detector":
{"detectorModelName":"areaDetectorModel","keyValue":"Area51","detectorModelVersion":"1"},"event
{"inputName":"seedTemperatureInput","messageId":"00001","triggerType":"Message"},"state":
{"stateName":"start","variables":
{"sensorCount":10,"rangeHigh":30.0,"resetMe":false,"enteringNewState":true,"averageTemperature"
{}}},"eventName":"resetHeatCool"}
```

Konfigurieren Sie die DescribeDetector API

Sie können den `DescribeDetector` Vorgang verwenden, um den aktuellen Status, die Variablenwerte und die Timer für eine Detektorinstanz anzuzeigen.

CLIBefehl:

```
aws iotevents-data describe-detector --detector-model-name areaDetectorModel --key-
value Area51
```

Antwort:

```
{
    "detector": {
        "lastUpdateTime": 1557521572.216,
        "creationTime": 1557520274.405,
        "state": {
            "variables": [
                {
                    "name": "resetMe",
                    "value": "false"
                },
                {
                    "name": "rangeLow",
                    "value": "15.0"
                },
                {
                    "name": "noDelay",
                    "value": "false"
                },
                {
                    "name": "desiredTemperature",
                    "value": "20.0"
                },
```

```
                {
                    "name": "anomalousLow",
                    "value": "0.0"
                },
                {
                    "name": "sensorId",
                    "value": "\"01\""
                },
                {
                    "name": "sensorCount",
                    "value": "10"
                },
                {
                    "name": "rangeHigh",
                    "value": "30.0"
                },
                {
                    "name": "enteringNewState",
                    "value": "false"
                },
                {
                    "name": "averageTemperature",
                    "value": "19.572"
                },
                {
                    "name": "allowedError",
                    "value": "0.7"
                },
                {
                    "name": "anomalousHigh",
                    "value": "60.0"
                },
                {
                    "name": "reportedTemperature",
                    "value": "15.72"
                },
                {
                    "name": "goodToGo",
                    "value": "false"
                }
            ],
            "stateName": "idle",
            "timers": [
                {
```

```
                    "timestamp": 1557520454.0,
                    "name": "idleTimer"
                }
            ]
        },
        "keyValue": "Area51",
        "detectorModelName": "areaDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

Verwenden Sie die AWS IoT Core Regel-Engine

Mit den folgenden Regeln werden AWS IoT Core MQTT Nachrichten als Shadow-Update-Anforderungsnachrichten erneut veröffentlicht. Wir gehen davon aus, dass für jeden Bereich, der durch das Detektormodell gesteuert wird, AWS IoT Core Dinge für eine Heiz- und eine Kühleinheit definiert sind. In diesem Beispiel haben wir Dinge mit dem Namen `"Area51HeatingUnit"` und definiert`"Area51CoolingUnit"`.

CLIBefehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowCoolOffRule.json
```

Datei: `ADMShadowCoolOffRule.json`

```
{
  "ruleName": "ADMShadowCoolOff",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Cooling/Off'",
    "description": "areaDetectorModel mqtt topic publish to cooling unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}CoolingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
```

```
    ]
  }
}
```

Antwort: [leer]

CLIBefehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowCoolOnRule.json
```

Datei: `ADMShadowCoolOnRule.json`

```
{
  "ruleName": "ADMShadowCoolOn",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Cooling/On'",
    "description": "areaDetectorModel mqtt topic publish to cooling unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}CoolingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

CLIBefehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowHeatOffRule.json
```

Datei: `ADMShadowHeatOffRule.json`

```
{
  "ruleName": "ADMShadowHeatOff",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Heating/Off'",
    "description": "areaDetectorModel mqtt topic publish to heating unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}HeatingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

CLIBefehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowHeatOnRule.json
```

Datei: `ADMShadowHeatOnRule.json`

```
{
  "ruleName": "ADMShadowHeatOn",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Heating/On'",
    "description": "areaDetectorModel mqtt topic publish to heating unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}HeatingUnit/shadow/
update",
```

```
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

Unterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen

AWS IoT Events kann Aktionen auslösen, wenn ein bestimmtes Ereignis oder ein Übergangsereignis erkannt wird. Sie können integrierte Aktionen definieren, um einen Timer zu verwenden, eine Variable festzulegen oder Daten an andere AWS Ressourcen zu senden.

> **Note**
>
> Wenn Sie eine Aktion in einem Detektormodell definieren, können Sie Ausdrücke für Parameter vom Datentyp Zeichenfolge verwenden. Weitere Informationen finden Sie unter Ausdrücke.

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie einen Timer verwenden oder eine Variable setzen können:

- `setTimer`um einen Timer zu erstellen.
- `resetTimer`um den Timer zurückzusetzen.
- `clearTimer`um den Timer zu löschen.
- `setVariable`um eine Variable zu erstellen.

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie mit AWS Diensten arbeiten können:

- `iotTopicPublish`um eine Nachricht zu einem MQTT Thema zu veröffentlichen.
- `iotEvents`um Daten AWS IoT Events als Eingabewert an zu senden.
- `iotSiteWise` zum Senden von Daten an eine Komponenteneigenschaft in AWS IoT SiteWise
- `dynamoDB`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `dynamoDBv2`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `firehose`um Daten an einen Amazon Data Firehose-Stream zu senden.
- `lambda`um eine Funktion aufzurufen. AWS Lambda
- `sns`um Daten als Push-Benachrichtigung zu senden.

- `sqs`um Daten an eine SQS Amazon-Warteschlange zu senden.

Verwenden Sie den AWS IoT Events integrierten Timer und variable Aktionen

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie einen Timer verwenden oder eine Variable setzen können:

- `setTimer`um einen Timer zu erstellen.
- `resetTimer`um den Timer zurückzusetzen.
- `clearTimer`um den Timer zu löschen.
- `setVariable`um eine Variable zu erstellen.

Stellen Sie die Timer-Aktion ein

Set timer action

Mit `setTimer` dieser Aktion können Sie einen Timer mit einer Dauer in Sekunden erstellen.

More information (2)

Wenn Sie einen Timer erstellen, müssen Sie die folgenden Parameter angeben.

`timerName`

Der Name des Timers.

`durationExpression`

(Optional) Die Dauer des Timers in Sekunden.

Das ausgewertete Ergebnis eines Ausdrucks für die Dauer wird auf die nächste ganze Zahl abgerundet. Wenn Sie den Timer beispielsweise auf 60,99 Sekunden setzen, beträgt das ausgewertete Ergebnis des Ausdrucks für die Dauer 60 Sekunden.

Weitere Informationen finden Sie SetTimerActionin der AWS IoT Events APIReferenz.

Timer-Aktion zurücksetzen

Reset timer action

Mit dieser `resetTimer` Aktion können Sie den Timer auf das zuvor ausgewertete Ergebnis des Dauerausdrucks setzen.

More information (1)

Wenn Sie einen Timer zurücksetzen, müssen Sie den folgenden Parameter angeben.

`timerName`

Der Name des Timers.

AWS IoT Events bewertet den Ausdruck für die Dauer nicht neu, wenn Sie den Timer zurücksetzen.

Weitere Informationen finden Sie ResetTimerActionin der AWS IoT Events APIReferenz.

Timer-Aktion löschen

Clear timer action

Mit `clearTimer` dieser Aktion können Sie einen vorhandenen Timer löschen.

More information (1)

Wenn Sie einen Timer löschen, müssen Sie den folgenden Parameter angeben.

`timerName`

Der Name des Timers.

Weitere Informationen finden Sie ClearTimerActionin der AWS IoT Events APIReferenz.

Variablenaktion festlegen

Set variable action

Mit der `setVariable` Aktion können Sie eine Variable mit einem bestimmten Wert erstellen.

More information (2)

Wenn Sie eine Variable erstellen, müssen Sie die folgenden Parameter angeben.

`variableName`

Der Name der Variable.

`value`

Der neue Wert der Variable.

Weitere Informationen finden Sie SetVariableActionin der AWS IoT Events APIReferenz.

Mit anderen AWS Diensten arbeiten

AWS IoT Events unterstützt die folgenden Aktionen, mit denen Sie mit AWS Diensten arbeiten können:

- `iotTopicPublish`um eine Nachricht zu einem MQTT Thema zu veröffentlichen.
- `iotEvents`um Daten AWS IoT Events als Eingabewert an zu senden.
- `iotSiteWise` zum Senden von Daten an eine Komponenteneigenschaft in AWS IoT SiteWise
- `dynamoDB`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `dynamoDBv2`um Daten an eine Amazon DynamoDB-Tabelle zu senden.
- `firehose`um Daten an einen Amazon Data Firehose-Stream zu senden.
- `lambda`um eine Funktion aufzurufen. AWS Lambda
- `sns`um Daten als Push-Benachrichtigung zu senden.
- `sqs`um Daten an eine SQS Amazon-Warteschlange zu senden.

> **Important**
>
> - Sie müssen für beide AWS IoT Events und für die AWS Dienste, mit denen Sie arbeiten möchten, dieselbe AWS Region auswählen. Eine vollständige Liste der unterstützten Regionen finden Sie unter AWS IoT Events -Endpunkte und -Kontingente in Allgemeine Amazon Web Services-Referenz.

- Sie müssen dieselbe AWS Region verwenden, wenn Sie andere AWS Ressourcen für die AWS IoT Events Aktionen erstellen. Wenn Sie die AWS Region wechseln, haben Sie möglicherweise Probleme beim Zugriff auf die AWS Ressourcen.

AWS IoT Events Generiert standardmäßig eine Standardnutzlast JSON für jede Aktion. Diese Aktionsnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Um die Aktions-Payload zu konfigurieren, können Sie einen Inhaltsausdruck verwenden. Weitere Informationen finden Sie unter Ausdrücke zum Filtern, Transformieren und Verarbeiten von Ereignisdaten und zum Payload-Datentyp in der AWS IoT Events API Referenz.

AWS IoT Core

IoT topic publish action

Mit AWS IoT Core dieser Aktion können Sie eine MQTT Nachricht über den AWS IoT Message Broker veröffentlichen. Eine vollständige Liste der unterstützten Regionen finden Sie unter AWS IoT Core -Endpunkte und -Kontingente in Allgemeine Amazon Web Services-Referenz.

Der AWS IoT Message Broker verbindet AWS IoT Clients, indem er Nachrichten von Publishing-Clients an abonnierte Clients sendet. Weitere Informationen finden Sie unter Gerätekommunikationsprotokolle im AWS IoT Entwicklerhandbuch.

More information (2)

Wenn Sie eine MQTT Nachricht veröffentlichen, müssen Sie die folgenden Parameter angeben.

`mqttTopic`

Das MQTT Thema, das die Nachricht erhält.

Sie können einen MQTT Themennamen zur Laufzeit dynamisch definieren, indem Sie Variablen oder Eingabewerte verwenden, die im Detektormodell erstellt wurden.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `iot:Publish` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie IotTopicPublishActionin der AWS IoT Events APIReferenz.

AWS IoT Events

IoT Events action

Mit AWS IoT Events dieser Aktion können Sie Daten AWS IoT Events als Eingabe an senden. Eine vollständige Liste der unterstützten Regionen finden Sie unter AWS IoT Events -Endpunkte und -Kontingente in Allgemeine Amazon Web Services-Referenz.

AWS IoT Events ermöglicht es Ihnen, Ihre Geräte oder Geräteflotten auf Ausfälle oder Betriebsänderungen zu überwachen und bei Auftreten solcher Ereignisse Aktionen auszulösen. Weitere Informationen finden Sie unter Was ist AWS IoT Events? im AWS IoT Events Entwicklerhandbuch.

More information (2)

Wenn Sie Daten an senden AWS IoT Events, müssen Sie die folgenden Parameter angeben.

`inputName`

Der Name der AWS IoT Events Eingabe, die die Daten empfängt.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `iotevents:BatchPutMessage` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie IotEventsActionin der AWS IoT Events APIReferenz.

AWS IoT SiteWise

IoT SiteWise action

Mit AWS IoT SiteWise dieser Aktion können Sie Daten an eine Anlageneigenschaft in senden AWS IoT SiteWise. Eine vollständige Liste der unterstützten Regionen finden Sie unter AWS IoT SiteWise -Endpunkte und -Kontingente in Allgemeine Amazon Web Services-Referenz.

AWS IoT SiteWise ist ein verwalteter Service, mit dem Sie Daten von Industrieanlagen in großem Umfang sammeln, organisieren und analysieren können. Weitere Informationen finden Sie unter Was ist AWS IoT SiteWise? im AWS IoT SiteWise -Benutzerhandbuch.

More information (11)

Wenn Sie Daten an ein Objekt in senden AWS IoT SiteWise, müssen Sie die folgenden Parameter angeben.

> **Important**
>
> Um die Daten zu empfangen, müssen Sie eine vorhandene Anlageneigenschaft in verwenden AWS IoT SiteWise.
>
> - Wenn Sie die AWS IoT Events Konsole verwenden, müssen Sie angeben`propertyAlias`, ob die Ziel-Asset-Eigenschaft identifiziert werden soll.
> - Wenn Sie die verwenden AWS CLI, müssen Sie eine `propertyAlias` oder beide angeben `assetId` und `propertyId` die Ziel-Asset-Eigenschaft identifizieren.
>
> Weitere Informationen finden Sie unter Zuordnung von industriellen Datenströmen zu Komponenten-Eigenschaften im Benutzerhandbuch für AWS IoT SiteWise .

propertyAlias

(Optional) Der Alias der Anlageneigenschaft. Sie können auch einen Ausdruck angeben.

assetId

(Optional) Die ID des Assets, das die angegebene Eigenschaft besitzt. Sie können auch einen Ausdruck angeben.

propertyId

(Optional) Die ID der Vermögenseigenschaft. Sie können auch einen Ausdruck angeben.

entryId

(Optional) Ein eindeutiger Bezeichner für diesen Eintrag. Sie können die Eintrags-ID verwenden, um zu verfolgen, welcher Dateneintrag im Fehlerfall einen Fehler verursacht. Der Standardwert ist ein neuer eindeutiger Bezeichner. Sie können auch einen Ausdruck angeben.

propertyValue

Eine Struktur, die Details zum Immobilienwert enthält.

quality

(Optional) Die Qualität des Vermögenswerts. Der Wert muss `GOOD`, `BAD` oder `UNCERTAIN` lauten. Sie können auch einen Ausdruck angeben.

timestamp

(Optional) Eine Struktur, die Zeitstempelinformationen enthält. Wenn Sie diesen Wert nicht angeben, ist die Standardeinstellung die Uhrzeit des Ereignisses.

timeInSeconds

Der Zeitstempel (in Sekunden) im Unix-Epoch-Format. Der gültige Bereich liegt zwischen 1-31556889864403199. Sie können auch einen Ausdruck angeben.

offsetInNanos

(Optional) Der Nanosekunden-Offset, konvertiert von`timeInSeconds`. Der gültige Bereich liegt zwischen 0-999999999. Sie können auch einen Ausdruck angeben.

value

Eine Struktur, die einen Asset-Eigenschaftswert enthält.

> **Important**
>
> Sie müssen je nach `dataType` der angegebenen Asset-Eigenschaft einen der folgenden Werttypen angeben. Weitere Informationen finden Sie AssetPropertyin der AWS IoT SiteWise APIReferenz.

`booleanValue`

(Optional) Der Eigenschaftswert der Anlage ist ein boolescher Wert, der oder sein `TRUE` muss. `FALSE` Sie können auch einen Ausdruck angeben. Wenn Sie einen Ausdruck verwenden, sollte das ausgewertete Ergebnis ein boolescher Wert sein.

`doubleValue`

(Optional) Der Wert der Anlageneigenschaft ist doppelt so hoch. Sie können auch einen Ausdruck angeben. Wenn Sie einen Ausdruck verwenden, sollte das ausgewertete Ergebnis ein Double sein.

`integerValue`

(Optional) Der Wert der Anlageneigenschaft ist eine Ganzzahl. Sie können auch einen Ausdruck angeben. Wenn Sie einen Ausdruck verwenden, sollte das ausgewertete Ergebnis eine Ganzzahl sein.

`stringValue`

(Optional) Der Wert der Anlageneigenschaft ist eine Zeichenfolge. Sie können auch einen Ausdruck angeben. Wenn Sie einen Ausdruck verwenden, sollte das ausgewertete Ergebnis eine Zeichenfolge sein.

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `iotsitewise:BatchPutAssetPropertyValue` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie IotSiteWiseActionin der AWS IoT Events APIReferenz.

Amazon-DynamoDB

DynamoDB action

Mit der Amazon DynamoDB DynamoDB-Aktion können Sie Daten an eine DynamoDB-Tabelle senden. Eine Spalte der DynamoDB-Tabelle empfängt alle Attribut-Wert-Paare in der Aktions-Payload, die Sie angeben. Eine Liste der unterstützten Regionen finden Sie unter Amazon DynamoDB DynamoDB-Endpunkte und Kontingente in der. Allgemeine Amazon Web Services-Referenz

Amazon DynamoDB ist ein vollständig verwalteter Service ohne SQL Datenbank, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet. Weitere Informationen finden Sie unter Was ist DynamoDB? im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

More information (10)

Wenn Sie Daten an eine Spalte einer DynamoDB-Tabelle senden, müssen Sie die folgenden Parameter angeben.

`tableName`

Der Name der DynamoDB-Tabelle, die die Daten empfängt. Der `tableName` Wert muss mit dem Tabellennamen der DynamoDB-Tabelle übereinstimmen. Sie können auch einen Ausdruck angeben.

`hashKeyField`

Der Name des Hash-Schlüssels (auch Partitionsschlüssel genannt). Der `hashKeyField` Wert muss mit dem Partitionsschlüssel der DynamoDB-Tabelle übereinstimmen. Sie können auch einen Ausdruck angeben.

`hashKeyType`

(Optional) Der Datentyp des Hash-Schlüssels. Der Wert des Hash-Schlüsseltyps muss `STRING` oder sein`NUMBER`. Der Standardwert ist `STRING`. Sie können auch einen Ausdruck angeben.

`hashKeyValue`

Der Wert des Hash-Schlüssels Der `hashKeyValue` verwendet Ersatzvorlagen. Diese Vorlagen stellen Daten zur Laufzeit bereit. Sie können auch einen Ausdruck angeben.

`rangeKeyField`

(Optional) Der Name des Bereichsschlüssels (auch Sortierschlüssel genannt). Der `rangeKeyField` Wert muss mit dem Sortierschlüssel der DynamoDB-Tabelle übereinstimmen. Sie können auch einen Ausdruck angeben.

`rangeKeyType`

(Optional) Der Datentyp des Bereichsschlüssels. Der Wert des Hash-Schlüsseltyps muss `STRING` oder sein`NUMBER`. Der Standardwert ist `STRING`. Sie können auch einen Ausdruck angeben.

`rangeKeyValue`

(Optional) Der Wert des Bereichsschlüssels. Der `rangeKeyValue` verwendet Ersatzvorlagen. Diese Vorlagen stellen Daten zur Laufzeit bereit. Sie können auch einen Ausdruck angeben.

operation

(Optional) Die Art des auszuführenden Vorgangs. Sie können auch einen Ausdruck angeben. Der Operationswert muss einer der folgenden Werte sein:

- `INSERT` – Fügt Daten als neues Element in die DynamoDB-Tabelle ein. Dies ist der Standardwert.
- `UPDATE` – Aktualisiert ein vorhandenes Element der DynamoDB-Tabelle mit neuen Daten.
- `DELETE`- Löscht ein vorhandenes Element aus der DynamoDB-Tabelle.

`payloadField`

(Optional) Der Name der DynamoDB-Spalte, die die Aktions-Payload empfängt. Der Standardname lautet `payload`. Sie können auch einen Ausdruck angeben.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

Wenn der angegebene Payload-Typ eine Zeichenfolge ist, werden Nichtdaten als JSON Binärdaten an die DynamoDB-Tabelle `DynamoDBAction` gesendet. Die DynamoDB-Konsole zeigt die Daten als Base64-codierten Text an. Der Wert von `payloadField` ist *`payload-field`*`_raw`. Sie können auch einen Ausdruck angeben.

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die entsprechende Genehmigung erteilt. `dynamodb:PutItem` Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie unter D ynamoDBAction in der AWS IoT Events APIReferenz.

Amazon DynamoDB (v2)

DynamoDBv2 action

Mit der Amazon DynamoDB (v2) -Aktion können Sie Daten in eine DynamoDB-Tabelle schreiben. Eine separate Spalte der DynamoDB-Tabelle erhält ein Attribut-Wert-Paar in der Aktions-Payload, die Sie angeben. Eine Liste der unterstützten Regionen finden Sie unter Amazon DynamoDB DynamoDB-Endpunkte und Kontingente in der. Allgemeine Amazon Web Services-Referenz

Amazon DynamoDB ist ein vollständig verwalteter Service ohne SQL Datenbank, der schnelle und vorhersehbare Leistung mit nahtloser Skalierbarkeit bietet. Weitere Informationen finden Sie unter Was ist DynamoDB? im Amazon DynamoDB DynamoDB-Entwicklerhandbuch.

More information (2)

Wenn Sie Daten an mehrere Spalten einer DynamoDB-Tabelle senden, müssen Sie die folgenden Parameter angeben.

`tableName`

Der Name der DynamoDB-Tabelle, die die Daten empfängt. Sie können auch einen Ausdruck angeben.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Important**
>
> Der Payload-Typ muss sein. JSON Sie können auch einen Ausdruck angeben.

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `dynamodb:PutItem` Genehmigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie unter D ynamoDBv 2Action in der AWS IoT Events APIReferenz.

Amazon Data Firehose

Firehose action

Mit der Amazon Data Firehose-Aktion können Sie Daten an einen Firehose-Lieferstream senden. Eine Liste der unterstützten Regionen finden Sie unter Amazon Data Firehose Endpoints and Quotas in der. Allgemeine Amazon Web Services-Referenz

Amazon Data Firehose ist ein vollständig verwalteter Service für die Bereitstellung von Echtzeit-Streaming-Daten an Ziele wie Amazon Simple Storage Service (Amazon Simple Storage Service), Amazon Redshift, Amazon OpenSearch Service (OpenSearch Service) und Splunk. Weitere Informationen finden Sie unter Was ist Amazon Data Firehose? im Amazon Data Firehose Developer Guide.

More information (3)

Wenn Sie Daten an einen Firehose-Lieferstream senden, müssen Sie die folgenden Parameter angeben.

`deliveryStreamName`

Der Name des Firehose-Lieferstreams, der die Daten empfängt.

`separator`

(Optional) Sie können ein Zeichentrennzeichen verwenden, um fortlaufende Daten zu trennen, die an den Firehose-Lieferstream gesendet werden. Der Wert des Trennzeichens muss `'\n'` (neue Zeile), `'\t'` (Tab), `'\r\n'` (Windows-neue Zeile) oder `','` (Komma) lauten.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `firehose:PutRecord` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie FirehoseActionin der AWS IoT Events APIReferenz.

AWS Lambda

Lambda action

Mit der AWS Lambda Aktion können Sie eine Lambda-Funktion aufrufen. Eine vollständige Liste der unterstützten Regionen finden Sie unter AWS Lambda -Endpunkte und -Kontingente in Allgemeine Amazon Web Services-Referenz.

AWS Lambda ist ein Rechendienst, mit dem Sie Code ausführen können, ohne Server bereitzustellen oder zu verwalten. Weitere Informationen finden Sie unter Was ist AWS Lambda? im AWS Lambda Entwicklerhandbuch.

More information (2)

Wenn Sie eine Lambda-Funktion aufrufen, müssen Sie die folgenden Parameter angeben.

`functionArn`

Die ARN der aufzurufenden Lambda-Funktion.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `lambda:InvokeFunction` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie LambdaActionin der AWS IoT Events APIReferenz.

Amazon Simple Notification Service

SNS action

Mit der Aktion SNS zum Veröffentlichen von Amazon-Themen können Sie eine SNS Amazon-Nachricht veröffentlichen. Eine Liste der unterstützten Regionen finden Sie unter Amazon Simple Notification Service-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Amazon Simple Notification Service (Amazon Simple Notification Service) ist ein Webservice, der die Zustellung oder den Versand von Nachrichten an abonnierte Endpunkte oder Kunden koordiniert und verwaltet. Weitere Informationen finden Sie unter Was ist AmazonSNS? im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Die Aktion zur Veröffentlichung von SNS Amazon-Themen unterstützt keine Amazon-Themen SNS FIFO (first in, first out). Da es sich bei der Rules Engine um einen vollständig verteilten Service handelt, werden die Nachrichten möglicherweise nicht in der angegebenen Reihenfolge angezeigt, wenn die SNS Amazon-Aktion ausgelöst wird.

More information (2)

Wenn Sie eine SNS Amazon-Nachricht veröffentlichen, müssen Sie die folgenden Parameter angeben.

`targetArn`

Die ARN des SNS Amazon-Ziels, das die Nachricht empfängt.

`payload`

(Optional) Die Standard-Payload enthält alle Attribut-Wert-Paare, die Informationen über die Detector-Modell-Instance und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `sns:Publish` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie SNSTopicPublishActionin der AWS IoT Events APIReferenz.

Amazon Simple Queue Service

SQS action

Mit der SQS Amazon-Aktion können Sie Daten an eine SQS Amazon-Warteschlange senden. Eine Liste der unterstützten Regionen finden Sie unter Amazon Simple Queue Service-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Amazon Simple Queue Service (AmazonSQS) bietet eine sichere, dauerhafte und verfügbare gehostete Warteschlange, mit der Sie verteilte Softwaresysteme und -komponenten integrieren und entkoppeln können. Weitere Informationen finden Sie unter Was ist Amazon Simple Queue Service> im Amazon Simple Queue Service Developer Guide.

> **Note**
>
> Die SQS Amazon-Aktion unterstützt keine >Amazon-Themen SQS FIFO (first in, first out). Da es sich bei der Rules Engine um einen vollständig verteilten Service handelt, werden die Nachrichten möglicherweise nicht in der angegebenen Reihenfolge angezeigt, wenn die SQS Amazon-Aktion ausgelöst wird.

More information (3)

Wenn Sie Daten an eine SQS Amazon-Warteschlange senden, müssen Sie die folgenden Parameter angeben.

`queueUrl`

Die URL der SQS Amazon-Warteschlange, die die Daten empfängt.

`useBase64`

(Optional) AWS IoT Events Kodiert die Daten in Base64-Text, sofern Sie dies angeben. `TRUE` Der Standardwert ist `FALSE`.

`payload`

(Optional) Die Standardnutzlast enthält alle Attribut-Wert-Paare, die Informationen über die Detektormodellinstanz und das Ereignis enthalten, das die Aktion ausgelöst hat. Sie können auch die Nutzlast anpassen. Weitere Informationen finden Sie unter Payload in der Referenz.AWS IoT Events API

> **Note**
>
> Stellen Sie sicher, dass die mit Ihrer AWS IoT Events Servicerolle verknüpfte Richtlinie die `sqs:SendMessage` Berechtigung erteilt. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events.

Weitere Informationen finden Sie SNSTopicPublishActionin der AWS IoT Events APIReferenz.

Sie können Amazon SNS und die AWS IoT Core Rules Engine auch verwenden, um eine AWS Lambda Funktion auszulösen. Dadurch ist es möglich, Aktionen mithilfe anderer Dienste wie Amazon

Connect oder sogar einer Enterprise Resource Planning (ERP) -Anwendung eines Unternehmens zu ergreifen.

> **Note**
>
> Um große Datenströme in Echtzeit zu sammeln und zu verarbeiten, können Sie andere AWS Dienste wie Amazon Kinesis verwenden. Von dort aus können Sie eine erste Analyse durchführen und die Ergebnisse dann AWS IoT Events als Eingabe an einen Detektor senden.

Ausdrücke zum Filtern, Transformieren und Verarbeiten von Ereignisdaten

Ausdrücke werden verwendet, um eingehende Daten auszuwerten, Berechnungen durchzuführen und die Bedingungen zu bestimmen, unter denen bestimmte Aktionen oder Zustandsübergänge stattfinden sollten. AWS IoT Events bietet mehrere Möglichkeiten, Werte anzugeben, wenn Sie Detektormodelle erstellen und aktualisieren. Sie können Ausdrücke verwenden, um Literalwerte anzugeben, oder Sie AWS IoT Events können die Ausdrücke auswerten, bevor Sie bestimmte Werte angeben.

Themen

Syntax zum Filtern von Gerätedaten und zum Definieren von Aktionen

Sie können Literale, Operatoren, Funktionen, Verweise und Ersetzungsvorlagen in den AWS IoT Events Ausdrücken verwenden.

Literale

- Ganzzahl
- Dezimal
- String
- Boolesch

Operatoren

Unär

- Nicht (Boolean): `!`
- Nicht (bitweise): `~`
- Minus (arithmetisch): `-`

String

- Verkettung: **+**

  Beide Operanden müssen Zeichenketten sein. Zeichenkettenliterale müssen in einfache Anführungszeichen (') eingeschlossen werden.

  Zum Beispiel: -> `'my' + 'string'` `'mystring'`

Arithmetisch

- Zusatz: **+**

  Beide Operanden müssen numerisch sein.

- Subtraktion: **-**
- Einteilung: **/**

  Das Ergebnis der Division ist ein gerundeter Ganzzahlwert, sofern nicht mindestens einer der Operanden (Divisor oder Dividend) ein Dezimalwert ist.

- Multiplikation: *****

Bitweise (Ganzzahl)

- ODER: **|**

  Zum Beispiel: `13 | 5` -> `13`

- AND: **&**

  Zum Beispiel: `13 & 5` -> `5`

- XOR: **^**

  Zum Beispiel: `13 ^ 5` -> `8`

- NOT: **~**

  Zum Beispiel: `~13` -> `-14`

Boolesch

- Weniger als: **<**
- Weniger als oder gleich: **<=**
- Gleich: **==**
- Nicht gleich: **!=**

- Größer als oder gleich: **>=**
- Größer als: **>**
- AND: **&&**
- ODER: **||**

> **Note**
>
> Wenn ein Unterausdruck von undefinierte Daten `||` enthält, wird dieser Unterausdruck als behandelt. `false`

Klammern

Sie können Klammern verwenden, um Begriffe innerhalb eines Ausdrucks zu gruppieren.

Funktionen zur Verwendung in Ausdrücken

Integrierte Funktionen

`timeout``("`*`timer-name`*`")`

Prüft, `true` ob der angegebene Timer abgelaufen ist. Ersetze“*`Name des Timers`*"mit dem Namen eines Timers, den Sie definiert haben, in Anführungszeichen. In einer Ereignisaktion können Sie einen Timer definieren und dann den Timer starten, zurücksetzen oder einen zuvor definierten Timer löschen. Sehen Sie sich das Feld an`detectorModelDefinition.states.onInput|onEnter|onExit.events.actions.setTimer.timerName`.

Auf einen Timer, der in einem Status festgelegt ist, kann in einem anderen Status verwiesen werden. Sie müssen den Status besuchen, in dem Sie den Timer erstellt haben, bevor Sie den Status aufrufen, in dem auf den Timer verwiesen wird.

Ein Detektormodell hat beispielsweise zwei Zustände, `TemperatureChecked` und`RecordUpdated`. Sie haben im `TemperatureChecked` Bundesstaat einen Timer erstellt. Sie müssen den `TemperatureChecked` Bundesstaat zuerst besuchen, bevor Sie den Timer im `RecordUpdated` Bundesstaat verwenden können.

Um die Genauigkeit zu gewährleisten, sollte die Mindestzeit, für die ein Timer eingestellt werden muss, 60 Sekunden betragen.

> **Note**
>
> `timeout()`gibt `true` nur das erste Mal zurück, wenn der Timer nach Ablauf des Timers zum ersten Mal überprüft wird, und kehrt `false` danach zurück.

`convert``(`*`type, expression`*`)`

Ergibt den Wert des Ausdrucks, der in den angegebenen Typ konvertiert wurde. Das Tool *`type`* Der Wert muss `StringBoolean`, oder `Decimal` sein. Verwenden Sie eines dieser Schlüsselwörter oder einen Ausdruck, der eine Zeichenfolge ergibt, die das Schlüsselwort enthält. Nur die folgenden Konvertierungen sind erfolgreich und geben einen gültigen Wert zurück:

- Boolean -> Zeichenfolge

  Gibt die Zeichenfolge `"true"` oder zurück. `"false"`
- Dezimal -> Zeichenfolge
- Zeichenfolge -> Boolean
- Zeichenfolge -> Dezimal

  Die angegebene Zeichenfolge muss eine gültige Darstellung einer Dezimalzahl sein, andernfalls schlägt sie `convert()` fehl.

Wenn `convert()` kein gültiger Wert zurückgegeben wird, ist der Ausdruck, zu dem er gehört, ebenfalls ungültig. Dieses Ergebnis entspricht dem Ereignis, in dem der `actions` Ausdruck auftritt, `false` und löst den Übergang zum `nextState` angegebenen Wert nicht aus.

`isNull``(`*`expression`*`)`

Wird ausgewertet, `true` ob der Ausdruck Null zurückgibt. Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "a": null }`, wird Folgendes als ausgewertet`true`, aber als `isUndefined($input.MyInput.a)` ausgewertet. `false`

```
isNull($input.MyInput.a)
```

isUndefined(*expression*)

Wird als undefiniert ausgewertet, `true` wenn der Ausdruck undefiniert ist. Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "a": null }`, wird Folgendes als ausgewertet`false`, aber `isNull($input.MyInput.a)` als ausgewertet. `true`

```
isUndefined($input.MyInput.a)
```

triggerType("*type*")

Das Tool *type* Der Wert kann oder sein. `"Message"` `"Timer"` Prüft, `true` ob die Ereignisbedingung, in der sie auftritt, ausgewertet wird, weil ein Timer abgelaufen ist, wie im folgenden Beispiel.

```
triggerType("Timer")
```

Oder es wurde eine Eingabenachricht empfangen.

```
triggerType("Message")
```

currentInput("*input*")

Prüft, `true` ob die Ereignisbedingung, in der sie auftritt, ausgewertet wird, weil die angegebene Eingabenachricht empfangen wurde. Wenn die Eingabe beispielsweise die Nachricht `Command` empfängt`{ "value": "Abort" }`, wird Folgendes als ausgewertet. `true`

```
currentInput("Command")
```

Verwenden Sie diese Funktion, um zu überprüfen, ob die Bedingung ausgewertet wird, weil eine bestimmte Eingabe empfangen wurde und ein Timer nicht abgelaufen ist, wie im folgenden Ausdruck dargestellt.

```
currentInput("Command") && $input.Command.value == "Abort"
```

Funktionen zum Abgleich von Zeichenketten

startsWith(*expression1*, *expression2*)

Prüft, `true` ob der erste Zeichenkettenausdruck mit dem zweiten Zeichenkettenausdruck beginnt. Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "status": "offline"}`, wird Folgendes als ausgewertet. `true`

```
startsWith($input.MyInput.status, "off")
```

Beide Ausdrücke müssen einen Zeichenkettenwert ergeben. Wenn einer der Ausdrücke keinen Zeichenkettenwert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

endsWith(*expression1*, *expression2*)

Prüft, `true` ob der erste Zeichenkettenausdruck mit dem zweiten Zeichenkettenausdruck endet. Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "status": "offline" }`, wird Folgendes als ausgewertet. `true`

```
endsWith($input.MyInput.status, "line")
```

Beide Ausdrücke müssen einen Zeichenkettenwert ergeben. Wenn einer der Ausdrücke keinen Zeichenkettenwert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

contains(*expression1*, *expression2*)

Prüft, `true` ob der erste Zeichenkettenausdruck den zweiten Zeichenkettenausdruck enthält. Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "status": "offline" }`, wird Folgendes als ausgewertet. `true`

```
contains($input.MyInput.value, "fli")
```

Beide Ausdrücke müssen einen Zeichenkettenwert ergeben. Wenn einer der Ausdrücke keinen Zeichenkettenwert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

Funktionen zur bitweisen Ganzzahlmanipulation

bitor(*expression1*, *expression2*)

Wertet das bitweise ODER der Integer-Ausdrücke aus (die binäre OR-Operation wird für die entsprechenden Bits der Ganzzahlen ausgeführt). Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "value1": 13, "value2": 5 }`, wird Folgendes als ausgewertet. `13`

```
bitor($input.MyInput.value1, $input.MyInput.value2)
```

Beide Ausdrücke müssen einen ganzzahligen Wert ergeben. Wenn einer der Ausdrücke keinen ganzzahligen Wert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

bitand(*expression1*, *expression2*)

Wertet die bitweisen Werte AND der Integer-Ausdrücke aus (die binäre AND Operation wird für die entsprechenden Bits der Ganzzahlen ausgeführt). Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "value1": 13, "value2": 5 }`, wird Folgendes zu ausgewertet. `5`

```
bitand($input.MyInput.value1, $input.MyInput.value2)
```

Beide Ausdrücke müssen einen ganzzahligen Wert ergeben. Wenn einer der Ausdrücke keinen ganzzahligen Wert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

bitxor(*expression1*, *expression2*)

Wertet die bitweisen Werte XOR der Integer-Ausdrücke aus (die binäre XOR Operation wird für die entsprechenden Bits der Ganzzahlen ausgeführt). Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "value1": 13, "value2": 5 }`, wird Folgendes zu ausgewertet. `8`

```
bitxor($input.MyInput.value1, $input.MyInput.value2)
```

Beide Ausdrücke müssen einen ganzzahligen Wert ergeben. Wenn einer der Ausdrücke keinen ganzzahligen Wert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

bitnot(*expression*)

Wertet den bitweisen Wert NOT des Integer-Ausdrucks aus (die binäre NOT Operation wird mit den Bits der Ganzzahl ausgeführt). Wenn die Eingabe beispielsweise die Nachricht `MyInput` empfängt`{ "value": 13 }`, wird Folgendes als ausgewertet. `-14`

```
bitnot($input.MyInput.value)
```

Beide Ausdrücke müssen einen ganzzahligen Wert ergeben. Wenn einer der Ausdrücke keinen ganzzahligen Wert ergibt, ist das Ergebnis der Funktion undefiniert. Es werden keine Konvertierungen durchgeführt.

Referenz für Eingaben und Variablen in Ausdrücken

Eingaben

`$input.`*`input-name`*`.`*`path-to-data`*

`input-name`ist eine Eingabe, die Sie mithilfe der CreateInputAktion erstellen.

Wenn Sie beispielsweise eine Eingabe benannt haben, `TemperatureInput` für die Sie `inputDefinition.attributes.jsonPath` Einträge definiert haben, werden die Werte möglicherweise in den folgenden verfügbaren Feldern angezeigt.

```
{
    "temperature": 78.5,
    "date": "2018-10-03T16:09:09Z"
  }
```

Verwenden Sie den folgenden Befehl, um `temperature` auf den Wert des Felds zu verweisen.

```
$input.TemperatureInput.temperature
```

Bei Feldern, deren Werte Arrays sind, können Sie mit Hilfe `[`*`n`*`]` von auf Elemente des Arrays verweisen. Zum Beispiel bei den folgenden Werten:

```
{
    "temperatures": [
      78.4,
      77.9,
```

```
      78.8
    ],
    "date": "2018-10-03T16:09:09Z"
  }
```

Auf den Wert `78.8` kann mit dem folgenden Befehl verwiesen werden.

```
$input.TemperatureInput.temperatures[2]
```

Variablen

`$variable.`*`variable-name`*

Das *`variable-name`* ist eine Variable, die Sie mithilfe der CreateDetectorModelAktion definiert haben.

Wenn Sie beispielsweise eine Variable benannt haben, `TechnicianID` die Sie mithilfe definiert habendetectorDefinition`.states.onInputEvents.actions.setVariable.variableName`, können Sie mit dem folgenden Befehl auf den Wert (Zeichenfolge) verweisen, der der Variablen zuletzt zugewiesen wurde.

```
$variable.TechnicianID
```

Sie können die Werte von Variablen nur mithilfe der `setVariable` Aktion festlegen. Sie können Variablen in einem Ausdruck keine Werte zuweisen. Eine Variable kann nicht rückgängig gemacht werden. Sie können ihr beispielsweise den Wert `null` nicht zuweisen.

> **Note**
>
> In Verweisen, die Bezeichner verwenden, die nicht dem Muster (regulärer Ausdruck) folgen`[a-zA-Z][a-zA-Z0-9_]*`, müssen Sie diese Bezeichner in Backticks () einschließen. ` Beispielsweise `_value` muss ein Verweis auf eine Eingabe, die `MyInput` mit einem Feld benannt ist, dieses Feld als angeben. `$input.MyInput.`_value``

Wenn Sie Verweise in Ausdrücken verwenden, überprüfen Sie Folgendes:

- Wenn Sie eine Referenz als Operanden mit einem oder mehreren Operatoren verwenden, stellen Sie sicher, dass alle Datentypen, auf die Sie verweisen, kompatibel sind.

Im folgenden Ausdruck 2 ist Integer beispielsweise ein Operand sowohl der == Operatoren als auch. && Um sicherzustellen, dass die Operanden kompatibel sind `$variable.testVariable + 1` und auf eine Ganzzahl oder Dezimalzahl verweisen `$variable.testVariable` müssen.

Außerdem 1 ist Integer ein Operand des Operators+. `$variable.testVariable`Muss daher auf eine Ganzzahl oder Dezimalzahl verweisen.

```
'$variable.testVariable + 1 == 2 && $variable.testVariable'
```

- Wenn Sie eine Referenz als Argument verwenden, das an eine Funktion übergeben wird, stellen Sie sicher, dass die Funktion die Datentypen unterstützt, auf die Sie verweisen.

  Für die folgende `timeout("time-name")` Funktion ist beispielsweise eine Zeichenfolge mit doppelten Anführungszeichen als Argument erforderlich. Wenn Sie eine Referenz für die verwenden *`timer-name`* Wert, Sie müssen auf eine Zeichenfolge mit doppelten Anführungszeichen verweisen.

  ```
  timeout("timer-name")
  ```

  > **Note**
  >
  > Für die `convert(type, expression)` Funktion, wenn Sie eine Referenz für die verwenden *`type`* Wert, das ausgewertete Ergebnis Ihrer Referenz muss `StringDecimal`, oder sein`Boolean`.

AWS IoT Events Ausdrücke unterstützen Integer-, Dezimal-, String- und Boolesche Datentypen. Die folgende Tabelle enthält eine Liste inkompatibler Typpaare.

Inkompatible Typenpaare
Ganzzahl, Zeichenfolge
Ganzzahl, Boolean
Dezimal, Zeichenfolge
Dezimal, Boolesch

Inkompatible Typenpaare
Zeichenfolge, Boolean

Ersatzvorlagen für Ausdrücke

```
'${expression}'
```

Der `${}` identifiziert die Zeichenfolge als interpolierte Zeichenfolge. Das `expression` kann ein beliebiger Ausdruck sein. AWS IoT Events Dazu gehören Operatoren, Funktionen und Verweise.

Sie haben die SetVariableAktion beispielsweise verwendet, um eine Variable zu definieren. `variableName` ist `SensorID` und `value` ist `10`. Sie können die folgenden Substitutionsvorlagen erstellen.

Substitutionsvorlage	Ergebniszeichenfolge
`'${'Sensor ' + $variable.SensorID}'`	`"Sensor 10"`
`'Sensor ' + '${$variable.SensorID + 1}'`	`"Sensor 11"`
`'Sensor 10: ${$variable.SensorID == 10}'`	`"Sensor 10: true"`
`'{\"sensor\":\"${$variable.SensorID + 1}\"}'`	`"{\"sensor"\:\"11\"}"`
`'{\"sensor\":${$variable.SensorID + 1}}'`	`"{\"sensor\":11}"`

Ausdrucksbeispiele und Verwendung für AWS IoT Events

Sie können Werte in einem Detektormodell auf folgende Weise angeben:

- Geben Sie unterstützte Ausdrücke in der AWS IoT Events Konsole ein.
- Übergeben Sie die Ausdrücke an die AWS IoT Events APIs AS-Parameter.

Ausdrücke unterstützen Literale, Operatoren, Funktionen, Verweise und Ersatzvorlagen.

> **Important**
>
> Ihre Ausdrücke müssen auf eine Ganzzahl, eine Dezimalzahl, eine Zeichenfolge oder einen booleschen Wert verweisen.

Ausdrücke schreiben AWS IoT Events

Sehen Sie sich die folgenden Beispiele an, die Ihnen beim Schreiben Ihrer AWS IoT Events Ausdrücke helfen sollen:

Literal

Bei Literalwerten müssen die Ausdrücke einfache Anführungszeichen enthalten. Ein boolescher Wert muss entweder oder `true` sein. `false`

```
'123'        # Integer
'123.12'     # Decimal
'hello'      # String
'true'       # Boolean
```

Referenz

Bei Referenzen müssen Sie entweder Variablen oder Eingabewerte angeben.

- Die folgende Eingabe bezieht sich auf eine Dezimalzahl,. `10.01`

  ```
  $input.GreenhouseInput.temperature
  ```

- Die folgende Variable verweist auf eine Zeichenfolge,`Greenhouse Temperature Table`.

  ```
  $variable.TableName
  ```

Vorlage für die Substitution

Für eine Substitutionsvorlage müssen Sie `${}` verwenden und die Vorlage muss von einfachen Anführungszeichen umschlossen sein. Eine Substitutionsvorlage kann auch eine Kombination aus Literalen, Operatoren, Funktionen, Referenzen und Substitutionsvorlagen enthalten.

- Das ausgewertete Ergebnis des folgenden Ausdrucks ist eine Zeichenfolge,`50.018 in Fahrenheit`.

```
'${$input.GreenhouseInput.temperature * 9 / 5 + 32} in Fahrenheit'
```

- Das ausgewertete Ergebnis des folgenden Ausdrucks ist eine Zeichenfolge,`{\"sensor_id\":\"Sensor_1\",\"temperature\":\"50.018\"}`.

```
'{\"sensor_id\":\"${$input.GreenhouseInput.sensors[0].sensor1}\",\"temperature\":
\"${$input.GreenhouseInput.temperature*9/5+32}\"}'
```

Zeichenfolgenverkettung

Für eine Zeichenfolgeverkettung müssen Sie + verwenden. Eine Zeichenfolgeverkettung kann auch eine Kombination aus Literalen, Operatoren, Funktionen, Referenzen und Substitutionsvorlagen enthalten.

- Das ausgewertete Ergebnis des folgenden Ausdrucks ist eine Zeichenfolge,`Greenhouse Temperature Table 2000-01-01`.

```
'Greenhouse Temperature Table ' + $input.GreenhouseInput.date
```

AWS IoT Events Beispiele für Detektormodelle

Diese Seite enthält eine Liste von Anwendungsbeispielen, die zeigen, wie verschiedene AWS IoT Events Funktionen konfiguriert werden. Die Beispiele reichen von grundlegenden Erkennungen wie Temperaturgrenzwerten bis hin zu komplexeren Szenarien zur Erkennung von Anomalien und maschinellem Lernen. Jedes Beispiel enthält Verfahren und Codefragmente, die Ihnen bei der Einrichtung von AWS IoT Events Erkennungen, Aktionen und Integrationen helfen. Diese Beispiele zeigen die Flexibilität des AWS IoT Events Dienstes und wie er für verschiedene IoT-Anwendungen und Anwendungsfälle angepasst werden kann. Auf dieser Seite finden Sie Informationen zu den AWS IoT Events Funktionen oder wenn Sie Hilfe bei der Implementierung eines bestimmten Erkennungs- oder Automatisierungsworkflows benötigen.

Themen

Beispiel: Verwendung der HVAC Temperatursteuerung

Hintergrundgeschichte

In diesem Beispiel wird ein Temperaturregelungsmodell (ein Thermostat) mit folgenden Funktionen implementiert:

- Ein von Ihnen definiertes Meldermodell, das mehrere Bereiche überwachen und steuern kann. (Für jeden Bereich wird eine Melderinstanz erstellt.)
- Jede Melderinstanz empfängt Temperaturdaten von mehreren Sensoren, die sich in jedem Kontrollbereich befinden.
- Sie können die gewünschte Temperatur (den Sollwert) für jeden Bereich jederzeit ändern.
- Sie können die Betriebsparameter für jeden Bereich definieren und diese Parameter jederzeit ändern.

- Sie können jederzeit Sensoren zu einem Bereich hinzufügen oder Sensoren aus einem Bereich löschen.
- Sie können Heiz- und Kühlgeräte mit einer Mindestlaufzeit aktivieren, um sie vor Beschädigungen zu schützen.
- Die Melder weisen anomale Sensorwerte zurück und melden sie.
- Sie können Sollwerte für die Notfalltemperatur definieren. Wenn ein Sensor eine Temperatur über oder unter den von Ihnen definierten Sollwerten meldet, werden die Heiz- oder Kühlgeräte sofort eingeschaltet und der Melder meldet diese Temperaturspitze.

Dieses Beispiel demonstriert die folgenden Funktionsmöglichkeiten:

- Erstellen Sie Modelle für Ereignisdetektoren.
- Erstellen Sie Eingaben.
- Eingaben in ein Detektormodell aufnehmen.
- Evaluieren Sie die Triggerbedingungen.
- Beziehen Sie sich auf Zustandsvariablen in Bedingungen und legen Sie die Werte der Variablen abhängig von den Bedingungen fest.
- Beziehen Sie sich auf Timer in Bedingungen und stellen Sie Timer je nach Bedingungen ein.
- Ergreifen Sie Maßnahmen, die Amazon SNS und MQTT Nachrichten senden.

Eingabedefinitionen für ein HVAC System

A `seedTemperatureInput` wird verwendet, um eine Melderinstanz für einen Bereich zu erstellen und seine Betriebsparameter zu definieren.

CLIverwendeter Befehl:

```
aws iotevents create-input --cli-input-json file://seedInput.json
```

Datei: `seedInput.json`

```
{
  "inputName": "seedTemperatureInput",
  "inputDescription": "Temperature seed values.",
  "inputDefinition": {
```

```
    "attributes": [
      { "jsonPath": "areaId" },
      { "jsonPath": "desiredTemperature" },
      { "jsonPath": "allowedError" },
      { "jsonPath": "rangeHigh" },
      { "jsonPath": "rangeLow" },
      { "jsonPath": "anomalousHigh" },
      { "jsonPath": "anomalousLow" },
      { "jsonPath": "sensorCount" },
      { "jsonPath": "noDelay" }
    ]
  }
}
```

Antwort:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/
seedTemperatureInput",
        "lastUpdateTime": 1557519620.736,
        "creationTime": 1557519620.736,
        "inputName": "seedTemperatureInput",
        "inputDescription": "Temperature seed values."
    }
}
```

Bei Bedarf `temperatureInput` sollte von jedem Sensor in jedem Bereich A gesendet werden.

CLIverwendeter Befehl:

```
aws iotevents create-input --cli-input-json file://temperatureInput.json
```

Datei: `temperatureInput.json`

```
{
  "inputName": "temperatureInput",
  "inputDescription": "Temperature sensor unit data.",
  "inputDefinition": {
    "attributes": [
      { "jsonPath": "sensorId" },
```

```
      { "jsonPath": "areaId" },
      { "jsonPath": "sensorData.temperature" }
    ]
  }
}
```

Antwort:

```
{
    "inputConfiguration": {
        "status": "ACTIVE",
        "inputArn": "arn:aws:iotevents:us-west-2:123456789012:input/temperatureInput",
        "lastUpdateTime": 1557519707.399,
        "creationTime": 1557519707.399,
        "inputName": "temperatureInput",
        "inputDescription": "Temperature sensor unit data."
    }
}
```

Definition des Detektormodells für ein HVAC System

Das `areaDetectorModel` definiert, wie jede Detektorinstanz funktioniert. Jede `state machine` Instanz nimmt Temperatursensormesswerte auf, ändert dann den Status und sendet abhängig von diesen Messwerten Steuermeldungen.

CLIverwendeter Befehl:

```
aws iotevents create-detector-model --cli-input-json file://areaDetectorModel.json
```

Datei: `areaDetectorModel.json`

```
{
  "detectorModelName": "areaDetectorModel",
  "detectorModelDefinition": {
    "states": [
      {
        "stateName": "start",
        "onEnter": {
          "events": [
            {
              "eventName": "prepare",
```

```
            "condition": "true",
            "actions": [
              {
                "setVariable": {
                  "variableName": "sensorId",
                  "value": "0"
                }
              },
              {
                "setVariable": {
                  "variableName": "reportedTemperature",
                  "value": "0.1"
                }
              },
              {
                "setVariable": {
                  "variableName": "resetMe",
                  "value": "false"
                }
              }
            ]
          }
        ]
      },
      "onInput": {
        "transitionEvents": [
          {
            "eventName": "initialize",
            "condition": "$input.seedTemperatureInput.sensorCount > 0",
            "actions": [
              {
                "setVariable": {
                  "variableName": "rangeHigh",
                  "value": "$input.seedTemperatureInput.rangeHigh"
                }
              },
              {
                "setVariable": {
                  "variableName": "rangeLow",
                  "value": "$input.seedTemperatureInput.rangeLow"
                }
              },
              {
                "setVariable": {
```

```
                "variableName": "desiredTemperature",
                "value": "$input.seedTemperatureInput.desiredTemperature"
              }
            },
            {
              "setVariable": {
                "variableName": "averageTemperature",
                "value": "$input.seedTemperatureInput.desiredTemperature"
              }
            },
            {
              "setVariable": {
                "variableName": "allowedError",
                "value": "$input.seedTemperatureInput.allowedError"
              }
            },
            {
              "setVariable": {
                "variableName": "anomalousHigh",
                "value": "$input.seedTemperatureInput.anomalousHigh"
              }
            },
            {
              "setVariable": {
                "variableName": "anomalousLow",
                "value": "$input.seedTemperatureInput.anomalousLow"
              }
            },
            {
              "setVariable": {
                "variableName": "sensorCount",
                "value": "$input.seedTemperatureInput.sensorCount"
              }
            },
            {
              "setVariable": {
                "variableName": "noDelay",
                "value": "$input.seedTemperatureInput.noDelay == true"
              }
            }
          ],
          "nextState": "idle"
        },
        {
```

```
              "eventName": "reset",
              "condition": "($variable.resetMe == true) &&
($input.temperatureInput.sensorData.temperature < $variable.anomalousHigh &&
$input.temperatureInput.sensorData.temperature > $variable.anomalousLow)",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "averageTemperature",
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ],
              "nextState": "idle"
            }
          ]
        },
        "onExit": {
          "events": [
            {
              "eventName": "resetHeatCool",
              "condition": "true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/Off"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/Off"
                  }
                }
              ]
```

```
            }
          ]
        }
      },


      {
        "stateName": "idle",
        "onInput": {
          "events": [
            {
              "eventName": "whatWasInput",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "sensorId",
                    "value": "$input.temperatureInput.sensorId"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "reportedTemperature",
                    "value": "$input.temperatureInput.sensorData.temperature"
                  }
                }
              ]
            },
            {
              "eventName": "changeDesired",
              "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                }
              ]
            },
            {
              "eventName": "calculateAverage",
```

```
            "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
            "actions": [
              {
                "setVariable": {
                  "variableName": "averageTemperature",
                  "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                }
              }
            ]
          }
        ],
        "transitionEvents": [
          {
            "eventName": "anomalousInputArrived",
            "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/anomaly"
                }
              }
            ],
            "nextState": "idle"
          },

          {
            "eventName": "highTemperatureSpike",
            "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/spike"
                }
              },
              {
                "sns": {
                  "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
                }
```

```
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "cooling"
            },

            {
              "eventName": "lowTemperatureSpike",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/spike"
                  }
                },
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "heating"
```

```
            },

            {
              "eventName": "highTemperatureThreshold",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) >
($variable.desiredTemperature + $variable.allowedError))",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "cooling"
            },

            {
              "eventName": "lowTemperatureThreshold",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) <
($variable.desiredTemperature - $variable.allowedError))",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/On"
                  }
                },
```

```
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "heating"
            }
          ]
        }
      },


      {
        "stateName": "cooling",
        "onEnter": {
          "events": [
            {
              "eventName": "delay",
              "condition": "!$variable.noDelay && $variable.enteringNewState",
              "actions": [
                {
                  "setTimer": {
                    "timerName": "coolingTimer",
                    "seconds": 180
                  }
                },
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "false"
                  }
                }
              ]
            },
            {
              "eventName": "dontDelay",
              "condition": "$variable.noDelay == true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
```

```
                }
              }
            ]
          },
          {
            "eventName": "beenHere",
            "condition": "true",
            "actions": [
              {
                "setVariable": {
                  "variableName": "enteringNewState",
                  "value": "false"
                }
              }
            ]
          }
        ]
      },

      "onInput": {
        "events": [
          {
            "eventName": "whatWasInput",
            "condition": "true",
            "actions": [
              {
                "setVariable": {
                  "variableName": "sensorId",
                  "value": "$input.temperatureInput.sensorId"
                }
              },
              {
                "setVariable": {
                  "variableName": "reportedTemperature",
                  "value": "$input.temperatureInput.sensorData.temperature"
                }
              }
            ]
          },
          {
            "eventName": "changeDesired",
            "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
            "actions": [
```

```
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                }
              ]
            },
            {
              "eventName": "calculateAverage",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "averageTemperature",
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ]
            },
            {
              "eventName": "areWeThereYet",
              "condition": "(timeout(\"coolingTimer\"))",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            }
          ],
          "transitionEvents": [
            {
              "eventName": "anomalousInputArrived",
              "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
              "actions": [
                {
```

```
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/anomaly"
                }
              }
            ],
            "nextState": "cooling"
          },

          {
            "eventName": "highTemperatureSpike",
            "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/spike"
                }
              }
            ],
            "nextState": "cooling"
          },

          {
            "eventName": "lowTemperatureSpike",
            "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
            "actions": [
              {
                "iotTopicPublish": {
                  "mqttTopic": "temperatureSensor/spike"
                }
              },
              {
                "sns": {
                  "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
                }
              },
              {
                "sns": {
                  "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOn"
                }
              },
              {
                "iotTopicPublish": {
```

```
                    "mqttTopic": "hvac/Cooling/Off"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/On"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "true"
                  }
                }
              ],
              "nextState": "heating"
            },

            {
              "eventName": "desiredTemperature",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) <=
($variable.desiredTemperature - $variable.allowedError)) && $variable.goodToGo ==
true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOff"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Cooling/Off"
                  }
                }
              ],
              "nextState": "idle"
            }
          ]
        }
      },


      {
```

```
        "stateName": "heating",
        "onEnter": {
          "events": [
            {
              "eventName": "delay",
              "condition": "!$variable.noDelay && $variable.enteringNewState",
              "actions": [
                {
                  "setTimer": {
                    "timerName": "heatingTimer",
                    "seconds": 120
                  }
                },
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "false"
                  }
                }
              ]
            },
            {
              "eventName": "dontDelay",
              "condition": "$variable.noDelay == true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            },
            {
              "eventName": "beenHere",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "enteringNewState",
                    "value": "false"
                  }
                }
              ]
```

```
            }
          ]
        },

        "onInput": {
          "events": [
            {
              "eventName": "whatWasInput",
              "condition": "true",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "sensorId",
                    "value": "$input.temperatureInput.sensorId"
                  }
                },
                {
                  "setVariable": {
                    "variableName": "reportedTemperature",
                    "value": "$input.temperatureInput.sensorData.temperature"
                  }
                }
              ]
            },
            {
              "eventName": "changeDesired",
              "condition": "$input.seedTemperatureInput.desiredTemperature !=
$variable.desiredTemperature",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "desiredTemperature",
                    "value": "$input.seedTemperatureInput.desiredTemperature"
                  }
                }
              ]
            },
            {
              "eventName": "calculateAverage",
              "condition": "$input.temperatureInput.sensorData.temperature <
$variable.anomalousHigh && $input.temperatureInput.sensorData.temperature >
$variable.anomalousLow",
              "actions": [
                {
```

```
                  "setVariable": {
                    "variableName": "averageTemperature",
                    "value": "((($variable.averageTemperature * ($variable.sensorCount
- 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount)"
                  }
                }
              ]
            },
            {
              "eventName": "areWeThereYet",
              "condition": "(timeout(\"heatingTimer\"))",
              "actions": [
                {
                  "setVariable": {
                    "variableName": "goodToGo",
                    "value": "true"
                  }
                }
              ]
            }
          ],
          "transitionEvents": [
            {
              "eventName": "anomalousInputArrived",
              "condition": "$input.temperatureInput.sensorData.temperature >=
$variable.anomalousHigh || $input.temperatureInput.sensorData.temperature <=
$variable.anomalousLow",
              "actions": [
                {
                  "iotTopicPublish": {
                    "mqttTopic": "temperatureSensor/anomaly"
                  }
                }
              ],
              "nextState": "heating"
            },

            {
              "eventName": "highTemperatureSpike",
              "condition": "$input.temperatureInput.sensorData.temperature >
$variable.rangeHigh",
              "actions": [
                {
                  "iotTopicPublish": {
```

```
                "mqttTopic": "temperatureSensor/spike"
              }
            },
            {
              "sns": {
                "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
              }
            },
            {
              "sns": {
                "targetArn": "arn:aws:sns:us-west-2:123456789012:coolOn"
              }
            },
            {
              "iotTopicPublish": {
                "mqttTopic": "hvac/Heating/Off"
              }
            },
            {
              "iotTopicPublish": {
                "mqttTopic": "hvac/Cooling/On"
              }
            },
            {
              "setVariable": {
                "variableName": "enteringNewState",
                "value": "true"
              }
            }
          ],
          "nextState": "cooling"
        },

        {
          "eventName": "lowTemperatureSpike",
          "condition": "$input.temperatureInput.sensorData.temperature <
$variable.rangeLow",
          "actions": [
            {
              "iotTopicPublish": {
                "mqttTopic": "temperatureSensor/spike"
              }
            }
          ],
```

```
              "nextState": "heating"
            },

            {
              "eventName": "desiredTemperature",
              "condition": "((((($variable.averageTemperature * ($variable.sensorCount
 - 1)) + $input.temperatureInput.sensorData.temperature) / $variable.sensorCount) >=
 ($variable.desiredTemperature + $variable.allowedError)) && $variable.goodToGo ==
 true",
              "actions": [
                {
                  "sns": {
                    "targetArn": "arn:aws:sns:us-west-2:123456789012:heatOff"
                  }
                },
                {
                  "iotTopicPublish": {
                    "mqttTopic": "hvac/Heating/Off"
                  }
                }
              ],
              "nextState": "idle"
            }
          ]
        }
      }

    ],

    "initialStateName": "start"
  },
  "key": "areaId",
  "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole"
}
```

Antwort:

```
{
    "detectorModelConfiguration": {
        "status": "ACTIVATING",
        "lastUpdateTime": 1557523491.168,
        "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
        "creationTime": 1557523491.168,
```

```
        "detectorModelArn": "arn:aws:iotevents:us-west-2:123456789012:detectorModel/
areaDetectorModel",
        "key": "areaId",
        "detectorModelName": "areaDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

BatchPutMessageBeispiele für ein HVAC System

In diesem Beispiel `BatchPutMessage` wird verwendet, um eine Melderinstanz für einen Bereich zu erstellen und die anfänglichen Betriebsparameter zu definieren.

CLIverwendeter Befehl:

```
aws iotevents-data batch-put-message --cli-input-json file://seedExample.json --cli-
binary-format raw-in-base64-out
```

Datei: `seedExample.json`

```
{
  "messages": [
    {
      "messageId": "00001",
      "inputName": "seedTemperatureInput",
      "payload": "{\"areaId\": \"Area51\", \"desiredTemperature\": 20.0, \"allowedError
\": 0.7, \"rangeHigh\": 30.0, \"rangeLow\": 15.0, \"anomalousHigh\": 60.0,
 \"anomalousLow\": 0.0, \"sensorCount\": 10, \"noDelay\": false}"
    }
  ]
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

In diesem Beispiel `BatchPutMessage` wird es verwendet, um Temperatursensorwerte für einen einzelnen Sensor in einem Bereich zu melden.

CLIverwendeter Befehl:

```
aws iotevents-data batch-put-message --cli-input-json file://temperatureExample.json --
cli-binary-format raw-in-base64-out
```

Datei: `temperatureExample.json`

```
{
  "messages": [
    {
      "messageId": "00005",
      "inputName": "temperatureInput",
      "payload": "{\"sensorId\": \"05\", \"areaId\": \"Area51\", \"sensorData\":
 {\"temperature\": 23.12} }"
    }
  ]
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

In diesem Beispiel `BatchPutMessage` wird verwendet, um die gewünschte Temperatur für einen Bereich zu ändern.

CLIverwendeter Befehl:

```
aws iotevents-data batch-put-message --cli-input-json file://seedSetDesiredTemp.json --
cli-binary-format raw-in-base64-out
```

Datei: `seedSetDesiredTemp.json`

```
{
  "messages": [
    {
      "messageId": "00001",
      "inputName": "seedTemperatureInput",
      "payload": "{\"areaId\": \"Area51\", \"desiredTemperature\": 23.0}"
    }
  ]
```

```
}
```

Antwort:

```
{
    "BatchPutMessageErrorEntries": []
}
```

Beispiele für SNS Amazon-Nachrichten, die von der `Area51` Detector-Instance generiert wurden:

```
Heating system off command> {
  "eventTime":1557520274729,
  "payload":{
    "actionExecutionId":"f3159081-bac3-38a4-96f7-74af0940d0a4",
    "detector":{
      "detectorModelName":"areaDetectorModel",
      "keyValue":"Area51",
      "detectorModelVersion":"1"
    },
    "eventTriggerDetails":{
      "inputName":"seedTemperatureInput",
      "messageId":"00001",
      "triggerType":"Message"
    },
    "state":{
      "stateName":"start",
      "variables":{
        "sensorCount":10,
        "rangeHigh":30.0,
        "resetMe":false,
        "enteringNewState":true,
        "averageTemperature":20.0,
        "rangeLow":15.0,
        "noDelay":false,
        "allowedError":0.7,
        "desiredTemperature":20.0,
        "anomalousHigh":60.0,
        "reportedTemperature":0.1,
        "anomalousLow":0.0,
        "sensorId":0
      },
```

```
      "timers":{}
    }
  },
  "eventName":"resetHeatCool"
}
```

```
Cooling system off command> {
  "eventTime":1557520274729,
  "payload":{
    "actionExecutionId":"98f6a1b5-8f40-3cdb-9256-93afd4d66192",
    "detector":{
      "detectorModelName":"areaDetectorModel",
      "keyValue":"Area51",
      "detectorModelVersion":"1"
    },
    "eventTriggerDetails":{
      "inputName":"seedTemperatureInput",
      "messageId":"00001",
      "triggerType":"Message"
    },
    "state":{
      "stateName":"start",
      "variables":{
        "sensorCount":10,
        "rangeHigh":30.0,
        "resetMe":false,
        "enteringNewState":true,
        "averageTemperature":20.0,
        "rangeLow":15.0,
        "noDelay":false,
        "allowedError":0.7,
        "desiredTemperature":20.0,
        "anomalousHigh":60.0,
        "reportedTemperature":0.1,
        "anomalousLow":0.0,
        "sensorId":0
      },
      "timers":{}
    }
  },
  "eventName":"resetHeatCool"
}
```

In diesem Beispiel verwenden wir die, `DescribeDetector` API um Informationen über den aktuellen Status einer Detector-Instance abzurufen.

```
aws iotevents-data describe-detector --detector-model-name areaDetectorModel --key-
value Area51
```

Antwort:

```
{
    "detector": {
        "lastUpdateTime": 1557521572.216,
        "creationTime": 1557520274.405,
        "state": {
            "variables": [
                {
                    "name": "resetMe",
                    "value": "false"
                },
                {
                    "name": "rangeLow",
                    "value": "15.0"
                },
                {
                    "name": "noDelay",
                    "value": "false"
                },
                {
                    "name": "desiredTemperature",
                    "value": "20.0"
                },
                {
                    "name": "anomalousLow",
                    "value": "0.0"
                },
                {
                    "name": "sensorId",
                    "value": "\"01\""
                },
                {
                    "name": "sensorCount",
                    "value": "10"
                },
                {
```

```
                    "name": "rangeHigh",
                    "value": "30.0"
                },
                {
                    "name": "enteringNewState",
                    "value": "false"
                },
                {
                    "name": "averageTemperature",
                    "value": "19.572"
                },
                {
                    "name": "allowedError",
                    "value": "0.7"
                },
                {
                    "name": "anomalousHigh",
                    "value": "60.0"
                },
                {
                    "name": "reportedTemperature",
                    "value": "15.72"
                },
                {
                    "name": "goodToGo",
                    "value": "false"
                }
            ],
            "stateName": "idle",
            "timers": [
                {
                    "timestamp": 1557520454.0,
                    "name": "idleTimer"
                }
            ]
        },
        "keyValue": "Area51",
        "detectorModelName": "areaDetectorModel",
        "detectorModelVersion": "1"
    }
}
```

BatchUpdateDetectorBeispiel für ein HVAC System

In diesem Beispiel `BatchUpdateDetector` wird es verwendet, um Betriebsparameter für eine funktionierende Melderinstanz zu ändern.

CLIverwendeter Befehl:

```
aws iotevents-data batch-update-detector --cli-input-json file://areaDM.BUD.json
```

Datei: `areaDM.BUD.json`

```
{
  "detectors": [
    {
      "messageId": "0001",
      "detectorModelName": "areaDetectorModel",
      "keyValue": "Area51",
      "state": {
        "stateName": "start",
        "variables": [
          {
            "name": "desiredTemperature",
            "value": "22"
          },
          {
            "name": "averageTemperature",
            "value": "22"
          },
          {
            "name": "allowedError",
            "value": "1.0"
          },
          {
            "name": "rangeHigh",
            "value": "30.0"
          },
          {
            "name": "rangeLow",
            "value": "15.0"
          },
          {
            "name": "anomalousHigh",
```

```
            "value": "60.0"
          },
          {
            "name": "anomalousLow",
            "value": "0.0"
          },
          {
            "name": "sensorCount",
            "value": "12"
          },
          {
            "name": "noDelay",
            "value": "true"
          },
          {
            "name": "goodToGo",
            "value": "true"
          },
          {
            "name": "sensorId",
            "value": "0"
          },
          {
            "name": "reportedTemperature",
            "value": "0.1"
          },
          {
            "name": "resetMe",
            "value": "true"
          }
        ],
        "timers": [
        ]
      }
    }
  ]
}
```

Antwort:

```
{
    An error occurred (InvalidRequestException) when calling the BatchUpdateDetector
 operation: Number of variables in the detector exceeds the limit 10
```

```
}
```

AWS IoT Core Regel-Engine

Die folgenden Regeln veröffentlichen AWS IoT Events MQTT Nachrichten erneut als Shadow-Update-Anforderungsnachrichten. Wir gehen davon aus, dass für jeden Bereich, der durch das Detektormodell gesteuert wird, AWS IoT Core Dinge für eine Heiz- und eine Kühleinheit definiert sind.

In diesem Beispiel haben wir Dinge mit dem Namen `Area51HeatingUnit` und definiert`Area51CoolingUnit`.

CLIverwendeter Befehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowCoolOffRule.json
```

Datei: `ADMShadowCoolOffRule.json`

```
{
  "ruleName": "ADMShadowCoolOff",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Cooling/Off'",
    "description": "areaDetectorModel mqtt topic publish to cooling unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}CoolingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

CLIverwendeter Befehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowCoolOnRule.json
```

Datei: `ADMShadowCoolOnRule.json`

```
{
  "ruleName": "ADMShadowCoolOn",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Cooling/On'",
    "description": "areaDetectorModel mqtt topic publish to cooling unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}CoolingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

CLIverwendeter Befehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowHeatOffRule.json
```

Datei: `ADMShadowHeatOffRule.json`

```
{
  "ruleName": "ADMShadowHeatOff",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Heating/Off'",
    "description": "areaDetectorModel mqtt topic publish to heating unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
```

```
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}HeatingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

CLIverwendeter Befehl:

```
aws iot create-topic-rule --cli-input-json file://ADMShadowHeatOnRule.json
```

Datei: `ADMShadowHeatOnRule.json`

```
{
  "ruleName": "ADMShadowHeatOn",
  "topicRulePayload": {
    "sql": "SELECT topic(3) as state.desired.command FROM 'hvac/Heating/On'",
    "description": "areaDetectorModel mqtt topic publish to heating unit shadow
 request",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [
      {
        "republish": {
          "topic": "$$aws/things/${payload.detector.keyValue}HeatingUnit/shadow/
update",
          "roleArn": "arn:aws:iam::123456789012:role/service-role/ADMShadowRole"
        }
      }
    ]
  }
}
```

Antwort: [leer]

Beispiel: Ein Kran erkennt Zustände

Hintergrundgeschichte

Ein Betreiber vieler Krane möchte erkennen, wann die Maschinen gewartet oder ausgetauscht werden müssen, und entsprechende Benachrichtigungen auslösen. Jeder Kran hat einen Motor. Ein Motor sendet Nachrichten (Eingänge) mit Informationen über Druck und Temperatur aus. Der Betreiber benötigt zwei Stufen von Ereignismeldern:

- Ein Ereignismelder auf Kranebene
- Ein Ereignismelder auf Motorebene

Mithilfe von Meldungen von den Motoren (die Metadaten sowohl mit dem `craneId` als auch mit enthaltenmotorid) kann der Bediener die Ereignismelder auf beiden Ebenen mithilfe eines geeigneten Routings ausführen. Wenn die Veranstaltungsbedingungen erfüllt sind, sollten Benachrichtigungen an die entsprechenden SNS Amazon-Themen gesendet werden. Der Bediener kann die Meldermodelle so konfigurieren, dass keine doppelten Benachrichtigungen ausgelöst werden.

Dieses Beispiel demonstriert die folgenden Funktionsfähigkeiten:

- Eingaben erstellen, lesen, aktualisieren, löschen (CRUD).
- Erstellen, Lesen, Aktualisieren, Löschen (CRUD) von Ereignismeldermodellen und verschiedenen Versionen von Ereignismeldern.
- Weiterleitung eines Eingangs an mehrere Ereignismelder.
- Aufnahme von Eingaben in ein Detektormodell.
- Bewertung von Triggerbedingungen und Lebenszyklusereignissen.
- Fähigkeit, in Bedingungen auf Zustandsvariablen zu verweisen und ihre Werte in Abhängigkeit von den Bedingungen festzulegen.
- Orchestrierung der Laufzeit mit Definition, Status, Trigger-Evaluator und Aktionsausführung.
- Ausführung von Aktionen mit einem `ActionsExecutor` Ziel. SNS

Sendet Befehle als Reaktion auf festgestellte Bedingungen

Diese Seite enthält ein Beispiel für die Verwendung von AWS IoT Events Befehlen zum Einrichten von Eingängen, zum Erstellen von Detektormodellen und zum Senden simulierter Sensordaten. Die

Beispiele zeigen, wie Industrieanlagen wie Motoren und Krane optimal AWS IoT Events überwacht werden können.

```
#Create Pressure Input
aws iotevents create-input  --cli-input-json file://pressureInput.json
aws iotevents describe-input --input-name PressureInput
aws iotevents update-input  --cli-input-json file://pressureInput.json
aws iotevents list-inputs
aws iotevents delete-input --input-name PressureInput

#Create Temperature Input
aws iotevents create-input  --cli-input-json file://temperatureInput.json
aws iotevents describe-input --input-name TemperatureInput
aws iotevents update-input  --cli-input-json file://temperatureInput.json
aws iotevents list-inputs
aws iotevents delete-input --input-name TemperatureInput

#Create Motor Event Detector using pressure and temperature input
aws iotevents create-detector-model  --cli-input-json file://motorDetectorModel.json
aws iotevents describe-detector-model --detector-model-name motorDetectorModel
aws iotevents update-detector-model  --cli-input-json file://
updateMotorDetectorModel.json
aws iotevents list-detector-models
aws iotevents list-detector-model-versions --detector-model-name motorDetectorModel
aws iotevents delete-detector-model --detector-model-name motorDetectorModel

#Create Crane Event Detector using temperature input
aws iotevents create-detector-model  --cli-input-json file://craneDetectorModel.json
aws iotevents describe-detector-model --detector-model-name craneDetectorModel
aws iotevents update-detector-model  --cli-input-json file://
updateCraneDetectorModel.json
aws iotevents list-detector-models
aws iotevents list-detector-model-versions --detector-model-name craneDetectorModel
aws iotevents delete-detector-model --detector-model-name craneDetectorModel

#Replace craneIds
sed -i '' "s/100008/100009/g" messages/*

#Replace motorIds
sed -i '' "s/200008/200009/g" messages/*

#Send HighPressure message
```

```
aws iotevents-data batch-put-message --cli-input-json file://messages/
highPressureMessage.json --cli-binary-format raw-in-base64-out

#Send HighTemperature message
aws iotevents-data batch-put-message --cli-input-json file://messages/
highTemperatureMessage.json --cli-binary-format raw-in-base64-out

#Send LowPressure message
aws iotevents-data batch-put-message --cli-input-json file://messages/
lowPressureMessage.json --cli-binary-format raw-in-base64-out

#Send LowTemperature message
aws iotevents-data batch-put-message --cli-input-json file://messages/
lowTemperatureMessage.json --cli-binary-format raw-in-base64-out
```

Detektormodell für die Kranüberwachung

Überwachen Sie Ihre Geräte oder Geräteflotten auf Ausfälle oder Betriebsänderungen und lösen Sie bei Auftreten solcher Ereignisse Maßnahmen aus. Sie definieren MeldermodelleJSON, in denen Zustände, Regeln und Aktionen festgelegt werden. Auf diese Weise können Sie Eingaben wie Temperatur und Druck überwachen, Schwellenwertüberschreitungen verfolgen und Warnmeldungen senden. Die Beispiele zeigen Detektormodelle für einen Kran und Motor, die Überhitzungsprobleme erkennen und Amazon benachrichtigen, SNS wenn ein Schwellenwert überschritten wird. Sie können Modelle aktualisieren, um das Verhalten zu verfeinern, ohne die Überwachung zu unterbrechen.

Datei: `craneDetectorModel.json`

```
{
    "detectorModelName": "craneDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Running",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
```

```
                                        "variableName": "craneThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
                        {
                            "eventName": "Overheated",
                            "condition": "$input.TemperatureInput.temperature > 35",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "craneThresholdBreached",
                                        "value": "$variable.craneThresholdBreached + 1"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Crane Threshold Breached",
                            "condition": "$variable.craneThresholdBreached > 5",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:CraneSNSTopic"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Underheated",
                            "condition": "$input.TemperatureInput.temperature < 25",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "craneThresholdBreached",
                                        "value": "0"
                                    }
                                }
```

```
                            ]
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Running"
    },
    "key": "craneid",
    "roleArn": "arn:aws:iam::123456789012:role/columboSNSRole"
}
```

Um ein vorhandenes Meldermodell zu aktualisieren. Datei: `updateCraneDetectorModel.json`

```
{
    "detectorModelName": "craneDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Running",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "craneThresholdBreached",
                                        "value": "0"
                                    }
                                },
                                {
                                    "setVariable": {
                                        "variableName": "alarmRaised",
                                        "value": "'false'"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
```

```
                    "events": [
                        {
                            "eventName": "Overheated",
                            "condition": "$input.TemperatureInput.temperature > 30",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "craneThresholdBreached",
                                        "value": "$variable.craneThresholdBreached + 1"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Crane Threshold Breached",
                            "condition": "$variable.craneThresholdBreached > 5 &&
 $variable.alarmRaised == 'false'",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:CraneSNSTopic"
                                    }
                                },
                                {
                                    "setVariable": {
                                        "variableName": "alarmRaised",
                                        "value": "'true'"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Underheated",
                            "condition": "$input.TemperatureInput.temperature < 10",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "craneThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
```

```
                    ]
                }
            }
        ],
        "initialStateName": "Running"
    },
    "roleArn": "arn:aws:iam::123456789012:role/columboSNSRole"
}
```

Datei: `motorDetectorModel.json`

```
{
    "detectorModelName": "motorDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Running",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "motorThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
                        {
                            "eventName": "Overheated And Overpressurized",
                            "condition": "$input.PressureInput.pressure > 70 &&
 $input.TemperatureInput.temperature > 30",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "motorThresholdBreached",
```

```
                                        "value": "$variable.motorThresholdBreached + 1"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Motor Threshold Breached",
                            "condition": "$variable.motorThresholdBreached > 5",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:MotorSNSTopic"
                                    }
                                }
                            ]
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Running"
    },
    "key": "motorId",
    "roleArn": "arn:aws:iam::123456789012:role/columboSNSRole"
}
```

Um ein vorhandenes Meldermodell zu aktualisieren. Datei: `updateMotorDetectorModel.json`

```
{
    "detectorModelName": "motorDetectorModel",
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "Running",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
```

```
                                        "variableName": "motorThresholdBreached",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onInput": {
                    "events": [
                        {
                            "eventName": "Overheated And Overpressurized",
                            "condition": "$input.PressureInput.pressure > 70 &&
 $input.TemperatureInput.temperature > 30",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "motorThresholdBreached",
                                        "value": "$variable.motorThresholdBreached + 1"
                                    }
                                }
                            ]
                        },
                        {
                            "eventName": "Motor Threshold Breached",
                            "condition": "$variable.motorThresholdBreached > 5",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
east-1:123456789012:MotorSNSTopic"
                                    }
                                }
                            ]
                        }
                    ]
                }
            }
        ],
        "initialStateName": "Running"
    },
    "roleArn": "arn:aws:iam::123456789012:role/columboSNSRole"
}
```

Eingänge für die Kranüberwachung

Datei: `pressureInput.json`

```
{
    "inputName": "PressureInput",
    "inputDescription": "this is a pressure input description",
    "inputDefinition": {
        "attributes": [
          {"jsonPath": "pressure"}
        ]
    }
}
```

Datei: `temperatureInput.json`

```
{
    "inputName": "TemperatureInput",
    "inputDescription": "this is temperature input description",
    "inputDefinition": {
        "attributes": [
            {"jsonPath": "temperature"}
        ]
    }
}
```

Senden Sie Alarm- und Betriebsmeldungen

Datei: `highPressureMessage.json`

```
{
   "messages": [
        {
           "messageId": "1",
           "inputName": "PressureInput",
           "payload": "{\"craneid\": \"100009\", \"pressure\": 80, \"motorid\":
 \"200009\"}"

        }
    ]
}
```

Datei: `highTemperatureMessage.json`

```
{
   "messages": [
        {
           "messageId": "2",
           "inputName": "TemperatureInput",
           "payload": "{\"craneid\": \"100009\", \"temperature\": 40, \"motorid\":
 \"200009\"}"
        }
    ]
}
```

Datei: `lowPressureMessage.json`

```
{
   "messages": [
        {
           "messageId": "1",
           "inputName": "PressureInput",
           "payload": "{\"craneid\": \"100009\", \"pressure\": 20, \"motorid\":
 \"200009\"}"
        }
    ]
}
```

Datei: `lowTemperatureMessage.json`

```
{
   "messages": [
        {
           "messageId": "2",
           "inputName": "TemperatureInput",
           "payload": "{\"craneid\": \"100009\", \"temperature\": 20, \"motorid\":
 \"200009\"}"
        }
    ]
}
```

Beispiel: Ereigniserkennung mit Sensoren und Anwendungen

Dieses Detektormodell ist eine der Vorlagen, die auf der AWS IoT Events Konsole verfügbar sind. Es ist hier der Einfachheit halber enthalten.

```
{
    "detectorModelName": "EventDetectionSensorsAndApplications",
    "detectorModelDefinition": {
        "states": [
            {
                "onInput": {
                    "transitionEvents": [],
                    "events": []
                },
                "stateName": "Device_exception",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Send_mqtt",
                            "actions": [
                                {
                                    "iotTopicPublish": {
                                        "mqttTopic": "Device_stolen"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "To_in_use",
                            "actions": [],
                            "condition": "$variable.position !=
 $input.AWS_IoTEvents_Blueprints_Tracking_DeviceInput.gps_position",
                            "nextState": "Device_in_use"
```

```
                        }
                    ],
                    "events": []
                },
                "stateName": "Device_idle",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Set_position",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "position",
                                        "value":
"$input.AWS_IoTEvents_Blueprints_Tracking_DeviceInput.gps_position"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "To_exception",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_Tracking_UserInput.device_id !=
$input.AWS_IoTEvents_Blueprints_Tracking_DeviceInput.device_id",
                            "nextState": "Device_exception"
                        }
                    ],
                    "events": []
                },
                "stateName": "Device_in_use",
                "onEnter": {
                    "events": []
                },
```

```
                "onExit": {
                    "events": []
                }
            }
        ],
        "initialStateName": "Device_idle"
    }
}
```

Beispiel: Gerät HeartBeat zur Überwachung von Geräteverbindungen

Dieses Meldermodell ist eine der Vorlagen, die auf der AWS IoT Events Konsole verfügbar sind. Es ist hier der Einfachheit halber enthalten.

```
{
    "detectorModelDefinition": {
        "states": [
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "To_normal",
                            "actions": [],
                            "condition":
 "currentInput(\"AWS_IoTEvents_Blueprints_Heartbeat_Input\")",
                            "nextState": "Normal"
                        }
                    ],
                    "events": []
                },
                "stateName": "Offline",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Send_notification",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "sns-topic-arn"
                                    }
                                }
```

```
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "Go_offline",
                            "actions": [],
                            "condition": "timeout(\"awake\")",
                            "nextState": "Offline"
                        }
                    ],
                    "events": [
                        {
                            "eventName": "Reset_timer",
                            "actions": [
                                {
                                    "resetTimer": {
                                        "timerName": "awake"
                                    }
                                }
                            ],
                            "condition":
"currentInput(\"AWS_IoTEvents_Blueprints_Heartbeat_Input\")"
                        }
                    ]
                },
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Create_timer",
                            "actions": [
                                {
                                    "setTimer": {
                                        "seconds": 300,
                                        "timerName": "awake"
```

```
                                    }
                                }
                            ],
                            "condition":
 "$input.AWS_IoTEvents_Blueprints_Heartbeat_Input.value > 0"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            }
        ],
        "initialStateName": "Normal"
    }
}
```

Beispiel: Ein ISA Alarm

Dieses Meldermodell ist eine der Vorlagen, die auf der AWS IoT Events Konsole verfügbar sind. Es ist hier der Einfachheit halber enthalten.

```
{
    "detectorModelName": "AWS_IoTEvents_Blueprints_ISA_Alarm",
    "detectorModelDefinition": {
        "states": [
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "unshelve",
                            "actions": [],
                            "condition":
 "$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unshelve\" &&
 $variable.state == \"rtnunack\"",
                            "nextState": "RTN_Unacknowledged"
                        },
                        {
                            "eventName": "unshelve",
                            "actions": [],
```

```
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unshelve\" &&
$variable.state == \"ack\"",
                            "nextState": "Acknowledged"
                        },
                        {
                            "eventName": "unshelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unshelve\" &&
$variable.state == \"unack\"",
                            "nextState": "Unacknowledged"
                        },
                        {
                            "eventName": "unshelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unshelve\" &&
$variable.state == \"normal\"",
                            "nextState": "Normal"
                        }
                    ],
                    "events": []
                },
                "stateName": "Shelved",
                "onEnter": {
                    "events": []
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "abnormal_condition",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value > $variable.higher_threshold ||
$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value < $variable.lower_threshold",
                            "nextState": "Unacknowledged"
                        },
                        {
```

```
                            "eventName": "acknowledge",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"acknowledge\"",
                            "nextState": "Normal"
                        },
                        {
                            "eventName": "shelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"shelve\"",
                            "nextState": "Shelved"
                        },
                        {
                            "eventName": "remove_from_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"remove\"",
                            "nextState": "Out_of_service"
                        },
                        {
                            "eventName": "suppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"suppressed\"",
                            "nextState": "Suppressed_by_design"
                        }
                    ],
                    "events": []
                },
                "stateName": "RTN_Unacknowledged",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "State Save",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "state",
                                        "value": "\"rtnunack\""
                                    }
                                }
                            ],
                            "condition": "true"
```

```
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "abnormal_condition",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value > $variable.higher_threshold ||
$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value < $variable.lower_threshold",
                            "nextState": "Unacknowledged"
                        },
                        {
                            "eventName": "shelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"shelve\"",
                            "nextState": "Shelved"
                        },
                        {
                            "eventName": "remove_from_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"remove\"",
                            "nextState": "Out_of_service"
                        },
                        {
                            "eventName": "suppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"suppressed\"",
                            "nextState": "Suppressed_by_design"
                        }
                    ],
                    "events": [
                        {
                            "eventName": "Create Config variables",
                            "actions": [
```

```
                                {
                                    "setVariable": {
                                        "variableName": "lower_threshold",
                                        "value":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.lower_threshold"
                                    }
                                },
                                {
                                    "setVariable": {
                                        "variableName": "higher_threshold",
                                        "value":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.higher_threshold"
                                    }
                                }
                            ],
                            "condition": "$variable.lower_threshold !=
$variable.lower_threshold"
                        }
                    ]
                },
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "State Save",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "state",
                                        "value": "\"normal\""
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
```

```
                        {
                            "eventName": "acknowledge",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"acknowledge\"",
                            "nextState": "Acknowledged"
                        },
                        {
                            "eventName": "return_to_normal",
                            "actions": [],
                            "condition":
"($input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value <= $variable.higher_threshold
&& $input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.value >=
$variable.lower_threshold)",
                            "nextState": "RTN_Unacknowledged"
                        },
                        {
                            "eventName": "shelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"shelve\"",
                            "nextState": "Shelved"
                        },
                        {
                            "eventName": "remove_from_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"remove\"",
                            "nextState": "Out_of_service"
                        },
                        {
                            "eventName": "suppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"suppressed\"",
                            "nextState": "Suppressed_by_design"
                        }
                    ],
                    "events": []
                },
                "stateName": "Unacknowledged",
                "onEnter": {
                    "events": [
                        {
```

```
                            "eventName": "State Save",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "state",
                                        "value": "\"unack\""
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "unsuppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unsuppressed\" &&
$variable.state == \"normal\"",
                            "nextState": "Normal"
                        },
                        {
                            "eventName": "unsuppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unsuppressed\" &&
$variable.state == \"unack\"",
                            "nextState": "Unacknowledged"
                        },
                        {
                            "eventName": "unsuppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unsuppressed\" &&
$variable.state == \"ack\"",
                            "nextState": "Acknowledged"
                        },
```

```
                        {
                            "eventName": "unsuppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"unsuppressed\" &&
$variable.state == \"rtnunack\"",
                            "nextState": "RTN_Unacknowledged"
                        }
                    ],
                    "events": []
                },
                "stateName": "Suppressed_by_design",
                "onEnter": {
                    "events": []
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "return_to_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"add\" && $variable.state
== \"rtnunack\"",
                            "nextState": "RTN_Unacknowledged"
                        },
                        {
                            "eventName": "return_to_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"add\" && $variable.state
== \"unack\"",
                            "nextState": "Unacknowledged"
                        },
                        {
                            "eventName": "return_to_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"add\" && $variable.state
== \"ack\"",
```

```
                            "nextState": "Acknowledged"
                        },
                        {
                            "eventName": "return_to_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"add\" && $variable.state
== \"normal\"",
                            "nextState": "Normal"
                        }
                    ],
                    "events": []
                },
                "stateName": "Out_of_service",
                "onEnter": {
                    "events": []
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "re-alarm",
                            "actions": [],
                            "condition": "timeout(\"snooze\")",
                            "nextState": "Unacknowledged"
                        },
                        {
                            "eventName": "return_to_normal",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"reset\"",
                            "nextState": "Normal"
                        },
                        {
                            "eventName": "shelve",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"shelve\"",
                            "nextState": "Shelved"
                        },
```

```
                        {
                            "eventName": "remove_from_service",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"remove\"",
                            "nextState": "Out_of_service"
                        },
                        {
                            "eventName": "suppression",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_ISA_Alarm_Input.command == \"suppressed\"",
                            "nextState": "Suppressed_by_design"
                        }
                    ],
                    "events": []
                },
                "stateName": "Acknowledged",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Create Timer",
                            "actions": [
                                {
                                    "setTimer": {
                                        "seconds": 60,
                                        "timerName": "snooze"
                                    }
                                }
                            ],
                            "condition": "true"
                        },
                        {
                            "eventName": "State Save",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "state",
                                        "value": "\"ack\""
                                    }
                                }
                            ],
                            "condition": "true"
                        }
```

```
                    ]
                },
                "onExit": {
                    "events": []
                }
            }
        ],
        "initialStateName": "Normal"
    },
    "detectorModelDescription": "This detector model is used to detect if a monitored
 device is in an Alarming State in accordance to the ISA 18.2.",
    "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
    "key": "alarmId"
}
```

Beispiel: Erstellen Sie einen einfachen Alarm

Dieses Meldermodell ist eine der Vorlagen, die auf der AWS IoT Events Konsole verfügbar sind. Es ist hier der Einfachheit halber enthalten.

```
{
    "detectorModelDefinition": {
        "states": [
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "not_fixed",
                            "actions": [],
                            "condition": "timeout(\"snoozeTime\")",
                            "nextState": "Alarming"
                        },
                        {
                            "eventName": "reset",
                            "actions": [],
                            "condition":
 "$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.command == \"reset\"",
                            "nextState": "Normal"
                        }
                    ],
                    "events": [
                        {
```

```
                            "eventName": "DND",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "dnd_active",
                                        "value": "1"
                                    }
                                }
                            ],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.command == \"dnd\""
                        }
                    ]
                },
                "stateName": "Snooze",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Create Timer",
                            "actions": [
                                {
                                    "setTimer": {
                                        "seconds": 120,
                                        "timerName": "snoozeTime"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "out_of_range",
                            "actions": [],
                            "condition":
"$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.value > $variable.threshold",
                            "nextState": "Alarming"
```

```
                        }
                    ],
                    "events": [
                        {
                            "eventName": "Create Config variables",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "threshold",
                                        "value":
"$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.threshold"
                                    }
                                }
                            ],
                            "condition": "$variable.threshold != $variable.threshold"
                        }
                    ]
                },
                "stateName": "Normal",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Init",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "dnd_active",
                                        "value": "0"
                                    }
                                }
                            ],
                            "condition": "true"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            },
            {
                "onInput": {
                    "transitionEvents": [
                        {
                            "eventName": "reset",
```

```
                            "actions": [],
                            "condition":
 "$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.command == \"reset\"",
                            "nextState": "Normal"
                        },
                        {
                            "eventName": "acknowledge",
                            "actions": [],
                            "condition":
 "$input.AWS_IoTEvents_Blueprints_Simple_Alarm_Input.command == \"acknowledge\"",
                            "nextState": "Snooze"
                        }
                    ],
                    "events": [
                        {
                            "eventName": "Escalated Alarm Notification",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
west-2:123456789012:escalatedAlarmNotification"
                                    }
                                }
                            ],
                            "condition": "timeout(\"unacknowledgeTIme\")"
                        }
                    ]
                },
                "stateName": "Alarming",
                "onEnter": {
                    "events": [
                        {
                            "eventName": "Alarm Notification",
                            "actions": [
                                {
                                    "sns": {
                                        "targetArn": "arn:aws:sns:us-
west-2:123456789012:alarmNotification"
                                    }
                                },
                                {
                                    "setTimer": {
                                        "seconds": 300,
                                        "timerName": "unacknowledgeTIme"
```

```
                                    }
                                }
                            ],
                            "condition": "$variable.dnd_active != 1"
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            }
        ],
        "initialStateName": "Normal"
    },
    "detectorModelDescription": "This detector model is used to detect if a monitored
 device is in an Alarming State.",
    "roleArn": "arn:aws:iam::123456789012:role/IoTEventsRole",
    "key": "alarmId"
}
```

Überwachung mit -Alarmen

AWS IoT Events Mithilfe von Alarmen können Sie Ihre Daten auf Änderungen überwachen. Bei den Daten kann es sich um Kennzahlen handeln, die Sie für Ihre Ausrüstung und Prozesse messen. Sie können Alarme erstellen, die Benachrichtigungen senden, wenn ein Schwellenwert überschritten wird. Alarme helfen Ihnen dabei, Probleme zu erkennen, die Wartung zu rationalisieren und die Leistung Ihrer Geräte und Prozesse zu optimieren.

Alarme sind Beispiele von Alarmmodellen. Das Alarmmodell legt fest, was erkannt werden soll, wann Benachrichtigungen gesendet werden sollen, wer benachrichtigt wird und vieles mehr. Sie können auch eine oder mehrere unterstützte Aktionen angeben, die ausgeführt werden, wenn sich der Alarmstatus ändert. AWS IoT Events leitet aus Ihren Daten abgeleitete Eingabeattribute an die entsprechenden Alarme weiter. Wenn die Daten, die Sie überwachen, außerhalb des angegebenen Bereichs liegen, wird der Alarm ausgelöst. Sie können die Alarme auch bestätigen oder sie in den Schlummermodus versetzen.

Arbeitet mit AWS IoT SiteWise

Sie können AWS IoT Events Alarme verwenden, um die Eigenschaften von Vermögenswerten in zu überwachen AWS IoT SiteWise. AWS IoT SiteWise sendet Eigenschaftswerte von Vermögenswerten an AWS IoT Events Alarme. AWS IoT Events sendet den Alarmstatus an AWS IoT SiteWise.

AWS IoT SiteWise unterstützt auch externe Alarme. Sie können externe Alarme wählen, wenn Sie Alarme außerhalb von verwenden AWS IoT SiteWise und über eine Lösung verfügen, die Alarmstatusdaten zurückgibt. Der externe Alarm enthält eine Messeigenschaft, die die Alarmzustandsdaten aufnimmt.

AWS IoT SiteWise wertet den Status externer Alarme nicht aus. Außerdem können Sie einen externen Alarm nicht bestätigen oder deaktivieren, wenn sich der Alarmstatus ändert.

Sie können die SiteWise Überwachungsfunktion verwenden, um den Status externer Alarme in SiteWise Monitor-Portalen einzusehen.

Weitere Informationen finden Sie unter Überwachen von Daten mit Alarmen im AWS IoT SiteWise Benutzerhandbuch und Überwachen mit Alarmen im SiteWise Monitor-Anwendungshandbuch.

Bestätigen Sie den Ablauf

Wenn Sie ein Alarmmodell erstellen, wählen Sie aus, ob der Bestätigungsfluss aktiviert werden soll. Wenn Sie den Bestätigungsfluss aktivieren, wird Ihr Team benachrichtigt, wenn sich der Alarmstatus ändert. Ihr Team kann den Alarm bestätigen und eine Notiz hinterlassen. Sie können beispielsweise die Informationen zum Alarm und die Maßnahmen, die Sie ergreifen werden, um das Problem zu beheben, angeben. Wenn die Daten, die Sie überwachen, außerhalb des angegebenen Bereichs liegen, wird der Alarm ausgelöst.

Alarme haben die folgenden Status:

`DISABLED`

Wenn sich der Alarm im `DISABLED` Status befindet, ist er nicht bereit, Daten auszuwerten. Um den Alarm zu aktivieren, müssen Sie den Alarm in den `NORMAL` Status ändern.

`NORMAL`

Wenn sich der Alarm im `NORMAL` Status befindet, ist er bereit, Daten auszuwerten.

`ACTIVE`

Befindet sich der Alarm im `ACTIVE` Status, wird der Alarm ausgelöst. Die Daten, die Sie überwachen, liegen außerhalb des angegebenen Bereichs.

`ACKNOWLEDGED`

Wenn sich der Alarm im `ACKNOWLEDGED` Status befindet, wurde der Alarm ausgelöst und Sie haben den Alarm bestätigt.

`LATCHED`

Der Alarm wurde ausgelöst, aber Sie haben den Alarm nach einer gewissen Zeit nicht bestätigt. Der Alarm wechselt automatisch in den `NORMAL` Status.

`SNOOZE_DISABLED`

Wenn sich der Alarm im `SNOOZE_DISABLED` Status befindet, ist der Alarm für einen bestimmten Zeitraum deaktiviert. Nach Ablauf der Schlummerzeit wechselt der Alarm automatisch in den `NORMAL` Status.

Ein Alarmmodell erstellen

Sie können AWS IoT Events Alarme verwenden, um Ihre Daten zu überwachen und sich benachrichtigen zu lassen, wenn ein Schwellenwert überschritten wird. Alarme stellen Parameter bereit, die Sie verwenden, um ein Alarmmodell zu erstellen oder zu konfigurieren. Sie können die AWS IoT Events Konsole verwenden oder AWS IoT Events API um das Alarmmodell zu erstellen oder zu konfigurieren. Wenn Sie das Alarmmodell konfigurieren, werden Änderungen wirksam, sobald neue Daten eintreffen.

Voraussetzungen

Die folgenden Anforderungen gelten, wenn Sie ein Alarmmodell erstellen.

- Sie können ein Alarmmodell erstellen, um ein Eingabeattribut AWS IoT Events oder eine Anlageneigenschaft in zu überwachen AWS IoT SiteWise.
  - Wenn Sie sich dafür entscheiden, ein Eingabeattribut in zu überwachen AWS IoT Events, Erstellen Sie eine Eingabe für Modelle bevor Sie das Alarmmodell erstellen.
  - Wenn Sie sich dafür entscheiden, eine Anlageneigenschaft zu überwachen, müssen Sie AWS IoT SiteWise vor der Erstellung des Alarmmodells ein Asset-Modell in erstellen.
- Sie müssen über eine IAM Rolle verfügen, die es Ihrem Alarm ermöglicht, Aktionen auszuführen und auf AWS Ressourcen zuzugreifen. Weitere Informationen finden Sie unter Berechtigungen einrichten für AWS IoT Events.
- Alle AWS Ressourcen, die in diesem Tutorial verwendet werden, müssen sich in derselben AWS Region befinden.

Ein Alarmmodell (Konsole) erstellen

Im Folgenden wird gezeigt, wie Sie ein Alarmmodell zur Überwachung eines AWS IoT Events Attributs in der AWS IoT Events Konsole erstellen.

1. Melden Sie sich an der AWS IoT Events -Konsole an.
2. Wählen Sie im Navigationsbereich die Option Alarmmodelle aus.
3. Wählen Sie auf der Seite Alarmmodelle die Option Alarmmodell erstellen aus.
4. Gehen Sie im Abschnitt Details zum Alarmmodell wie folgt vor:

   a. Geben Sie einen eindeutigen Namen ein.

b. (Optional) Geben Sie eine Beschreibung ein.

5. Gehen Sie im Abschnitt Alarmziel wie folgt vor:

> **Important**
>
> Wenn Sie sich für eine AWS IoT SiteWise Anlageneigenschaft entscheiden, müssen Sie in ein Asset-Modell erstellt haben AWS IoT SiteWise.

a. Wählen Sie das AWS IoT Events Eingabeattribut.

b. Wählen Sie die Eingabe aus.

c. Wählen Sie den Schlüssel für das Eingabeattribut aus. Dieses Eingabeattribut wird als Schlüssel zum Erstellen des Alarms verwendet. AWS IoT Events leitet die mit diesem Schlüssel verknüpften Eingaben an den Alarm weiter.

> **Important**
>
> Wenn die Nutzdaten der Eingabenachricht diesen Schlüssel für das Eingabeattribut nicht enthalten oder wenn sich der Schlüssel nicht in demselben JSON Pfad befindet, der im Schlüssel angegeben ist, schlägt die Eingabe in der Nachricht fehl. AWS IoT Events

6. Im Abschnitt Schwellenwertdefinitionen definieren Sie das Eingabeattribut, den Schwellenwert und den Vergleichsoperator, der AWS IoT Events verwendet wird, um den Status des Alarms zu ändern.

a. Wählen Sie unter Eingabeattribut das Attribut aus, das Sie überwachen möchten.

Jedes Mal, wenn dieses Eingabeattribut neue Daten empfängt, werden diese ausgewertet, um den Status des Alarms zu bestimmen.

b. Wählen Sie unter Operator den Vergleichsoperator aus. Der Operator vergleicht Ihr Eingabeattribut mit dem Schwellenwert für Ihr Attribut.

Sie können aus diesen Optionen wählen:

- > größer als
- >= größer als oder gleich

- < kleiner als
- <= kleiner als oder gleich
- = gleich
- ! = ungleich

c. Geben Sie für den Schwellenwert eine Zahl ein, oder wählen Sie ein Attribut in den AWS IoT Events Eingaben aus. AWS IoT Events vergleicht diesen Wert mit dem Wert des von Ihnen ausgewählten Eingabeattributs.

d. (Optional) Verwenden Sie für Schweregrad eine Zahl, von der Ihr Team weiß, dass sie den Schweregrad dieses Alarms wiedergibt.

7. (Optional) Konfigurieren Sie im Abschnitt Benachrichtigungseinstellungen die Benachrichtigungseinstellungen für den Alarm.

   Sie können bis zu 10 Benachrichtigungen hinzufügen. Gehen Sie für Benachrichtigung 1 wie folgt vor:

   a. Wählen Sie für Protokoll eine der folgenden Optionen aus:

      - E-Mail und Text — Der Alarm sendet eine SMS Benachrichtigung und eine E-Mail-Benachrichtigung.
      - E-Mail — Der Alarm sendet eine E-Mail-Benachrichtigung.
      - Text — Der Alarm sendet eine SMS Benachrichtigung.

   b. Geben Sie als Absender die E-Mail-Adresse an, an die Benachrichtigungen zu diesem Alarm gesendet werden können.

      Um Ihrer Absenderliste weitere E-Mail-Adressen hinzuzufügen, wählen Sie Absender hinzufügen.

   c. (Optional) Wählen Sie unter Empfänger den Empfänger aus.

      Um Ihrer Empfängerliste weitere Benutzer hinzuzufügen, wählen Sie Neuen Benutzer hinzufügen. Sie müssen Ihrem IAM Identity Center-Shop neue Benutzer hinzufügen, bevor Sie sie zu Ihrem Alarmmodell hinzufügen können. Weitere Informationen finden Sie unter Verwalten Sie den IAM Identity Center-Zugriff von Alarmempfängern.

   d. (Optional) Geben Sie unter Zusätzliche benutzerdefinierte Nachricht eine Nachricht ein, die beschreibt, was der Alarm erkennt und welche Maßnahmen die Empfänger ergreifen sollten.

8. Im Abschnitt Instanz können Sie alle Alarminstanzen aktivieren oder deaktivieren, die auf der Grundlage dieses Alarmmodells erstellt wurden.

9. Gehen Sie im Abschnitt Erweiterte Einstellungen wie folgt vor:

   a. Für den Acknowledge-Flow können Sie Benachrichtigungen aktivieren oder deaktivieren.

      - Wenn Sie Aktiviert wählen, erhalten Sie eine Benachrichtigung, wenn sich der Alarmstatus ändert. Sie müssen die Benachrichtigung bestätigen, bevor der Alarmstatus wieder normal werden kann.
      - Wenn Sie Deaktiviert wählen, ist keine Aktion erforderlich. Der Alarm wechselt automatisch in den Normalzustand, wenn die Messung in den angegebenen Bereich zurückkehrt.

      Weitere Informationen finden Sie unter Bestätigen Sie den Ablauf.

   b. Wählen Sie für Berechtigungen eine der folgenden Optionen aus:

      - Sie können eine neue Rolle anhand von AWS Richtlinienvorlagen erstellen und AWS IoT Events automatisch eine IAM Rolle für Sie erstellen.
      - Sie können eine vorhandene IAM Rolle verwenden, die es diesem Alarmmodell ermöglicht, Aktionen auszuführen und auf andere AWS Ressourcen zuzugreifen.

      Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung für AWS IoT Events.

   c. Für zusätzliche Benachrichtigungseinstellungen können Sie Ihre AWS Lambda Funktion zur Verwaltung von Alarmbenachrichtigungen bearbeiten. Wählen Sie eine der folgenden Optionen für Ihre AWS Lambda Funktion:

      - Neue AWS Lambda Funktion erstellen — AWS IoT Events erstellt eine neue AWS Lambda Funktion für Sie.
      - Eine bestehende AWS Lambda Funktion verwenden — Verwenden Sie eine bestehende AWS Lambda Funktion, indem Sie einen AWS Lambda Funktionsnamen wählen.

      Weitere Hinweise zu den möglichen Aktionen finden Sie unterMit anderen AWS Diensten arbeiten.

   d. (Optional) Unter Aktion „Status festlegen“ können Sie eine oder mehrere AWS IoT Events Aktionen hinzufügen, die ausgeführt werden sollen, wenn sich der Alarmstatus ändert.

10. (Optional) Sie können Tags hinzufügen, um Ihre Alarme zu verwalten. Weitere Informationen finden Sie unter Markieren Ihrer AWS IoT Events -Ressourcen.
11. Wählen Sie Create (Erstellen) aus.

Auf Alarme reagieren

Wenn Sie den Bestätigungsfluss aktiviert haben, erhalten Sie Benachrichtigungen, wenn sich der Alarmstatus ändert. Um auf den Alarm zu reagieren, können Sie den Alarm bestätigen, deaktivieren, aktivieren, zurücksetzen oder die Schlummerfunktion aktivieren.

Console

Im Folgenden wird gezeigt, wie Sie auf einen Alarm in der AWS IoT Events Konsole reagieren.

1. Melden Sie sich an der AWS IoT Events -Konsole an.
2. Wählen Sie im Navigationsbereich die Option Alarmmodelle aus.
3. Wählen Sie das Zielalarmmodell aus.
4. Wählen Sie im Bereich Liste der Alarme den Zielalarm aus.
5. Sie können unter Aktionen eine der folgenden Optionen wählen:
   - Bestätigen — Der Alarm wechselt in den `ACKNOWLEDGED` Status.
   - Deaktivieren — Der Alarm wechselt in den `DISABLED` Status.
   - Aktivieren — Der Alarm wechselt in den `NORMAL` Status.
   - Reset — Der Alarm wechselt in den `NORMAL` Status.
   - Schalten Sie die Schlummerfunktion ein und gehen Sie dann wie folgt vor:
     1. Wählen Sie die Schlummerlänge oder geben Sie eine benutzerdefinierte Schlummerlänge ein.
     2. Wählen Sie Save (Speichern) aus.

     Der Alarm wechselt in den Status `SNOOZE_DISABLED`

   Weitere Informationen zu den Alarmzuständen finden Sie unterBestätigen Sie den Ablauf.

API

Um auf einen oder mehrere Alarme zu reagieren, können Sie die folgenden AWS IoT Events API Operationen verwenden:

- BatchAcknowledgeAlarm
- BatchDisableAlarm
- BatchEnableAlarm
- BatchResetAlarm
- BatchSnoozeAlarm

Verwaltung von Alarmbenachrichtigungen

AWS IoT Events verwendet eine Lambda-Funktion zur Verwaltung von Alarmbenachrichtigungen. Sie können die von bereitgestellte Lambda-Funktion verwenden AWS IoT Events oder eine neue erstellen.

Themen

Erstellen einer Lambda-Funktion

AWS IoT Events bietet eine Lambda-Funktion, mit der Alarme E-Mails und SMS Benachrichtigungen senden und empfangen können.

Voraussetzungen

Die folgenden Anforderungen gelten, wenn Sie eine Lambda-Funktion für Alarme erstellen:

- Wenn Ihr Alarm E-Mails oder SMS Benachrichtigungen sendet, müssen Sie über eine IAM Rolle verfügen, die es Ihnen AWS Lambda ermöglicht, mit Amazon SES und Amazon zusammenzuarbeitenSNS.

  Beispiel für eine Richtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetIdentityVerificationAttributes",
                "ses:SendEmail",
                "ses:VerifyEmailIdentity"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish",
                "sns:OptInPhoneNumber",
                "sns:CheckIfPhoneNumberIsOptedOut"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:*"
        }
    ]
}
```

- Sie müssen dieselbe AWS Region für AWS IoT Events sowohl als auch wählen AWS Lambda. Eine Liste der unterstützten Regionen finden Sie unter AWS IoT Events Endpunkte und Kontingente und AWS Lambda Endpunkte und Kontingente in der. Allgemeine Amazon Web Services-Referenz

Bereitstellung einer Lambda-Funktion

In diesem Tutorial wird eine AWS CloudFormation Vorlage verwendet, um eine Lambda-Funktion bereitzustellen. Diese Vorlage erstellt automatisch eine IAM Rolle, die es der Lambda-Funktion ermöglicht, mit Amazon SES und Amazon SNS zu arbeiten.

Im Folgenden wird gezeigt, wie Sie AWS Command Line Interface (AWS CLI) verwenden, um einen CloudFormation Stack zu erstellen.

1. Führen Sie im Terminal Ihres Geräts den Befehl aus, `aws --version` um zu überprüfen, ob Sie den installiert haben AWS CLI. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.
2. Führen Sie den Vorgang aus`aws configure list`, um zu überprüfen, ob Sie das AWS CLI in der AWS Region konfiguriert haben, die alle Ihre AWS Ressourcen für dieses Tutorial enthält. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Installation oder Aktualisierung AWS CLI auf die neueste Version von
3. Laden Sie die CloudFormation Vorlage „notificationLambda.template.yaml.zip“ herunter.

   > **Note**
   >
   > Wenn Sie Schwierigkeiten beim Herunterladen der Datei haben, finden Sie die Vorlage auch im. CloudFormation Vorlage

4. Entpacken Sie den Inhalt und speichern Sie die Datei lokal als `notificationLambda.template.yaml`.
5. Öffnen Sie ein Terminal auf Ihrem Gerät und navigieren Sie zu dem Verzeichnis, in das Sie die `notificationLambda.template.yaml` Datei heruntergeladen haben.
6. Führen Sie den folgenden Befehl aus, um einen CloudFormation Stack zu erstellen:

   ```
   aws cloudformation create-stack --stack-name notificationLambda-stack --template-
   body file://notificationLambda.template.yaml --capabilities CAPABILITY_IAM
   ```

Sie können diese CloudFormation Vorlage ändern, um die Lambda-Funktion und ihr Verhalten anzupassen.

> **Note**
>
> AWS Lambda wiederholt Funktionsfehler zweimal. Wenn die Kapazität der Funktion nicht für die Verarbeitung aller eingehenden Anforderungen ausreicht, verbleiben die an die Funktion zu sendenden Ereignisse möglicherweise stunden- oder tagelang in der Warteschlange. Sie können in der Funktion eine Warteschlange für unzugestellte Nachrichten (DLQ)

konfigurieren, um Ereignisse aufzuzeichnen, die nicht erfolgreich verarbeitet wurden. Weitere Informationen finden Sie unter Asynchroner Aufruf im AWS Lambda Entwicklerhandbuch.

Sie können den Stack auch in der Konsole erstellen oder konfigurieren. CloudFormation Weitere Informationen finden Sie im AWS CloudFormation Benutzerhandbuch unter Arbeiten mit Stacks.

Eine benutzerdefinierte Lambda-Funktion erstellen

Sie können eine Lambda-Funktion erstellen oder die von AWS IoT Events bereitgestellte ändern.

Die folgenden Anforderungen gelten, wenn Sie eine benutzerdefinierte Lambda-Funktion erstellen.

- Fügen Sie Berechtigungen hinzu, die es Ihrer Lambda-Funktion ermöglichen, bestimmte Aktionen auszuführen und auf AWS Ressourcen zuzugreifen.
- Wenn Sie die von bereitgestellte Lambda-Funktion verwenden AWS IoT Events, stellen Sie sicher, dass Sie die Python 3.7-Laufzeit wählen.

Beispiel für eine Lambda-Funktion:

```
import boto3
import json
import logging
import datetime
logger = logging.getLogger()
logger.setLevel(logging.INFO)
ses = boto3.client('ses')
sns = boto3.client('sns')
def check_value(target):
  if target:
    return True
  return False

# Check whether email is verified. Only verified emails are allowed to send emails to
 or from.
def check_email(email):
  if not check_value(email):
    return False
  result = ses.get_identity_verification_attributes(Identities=[email])
  attr = result['VerificationAttributes']
  if (email not in attr or attr[email]['VerificationStatus'] != 'Success'):
```

```
      logging.info('Verification email for {} sent. You must have all the emails
 verified before sending email.'.format(email))
      ses.verify_email_identity(EmailAddress=email)
      return False
  return True

# Check whether the phone holder has opted out of receiving SMS messages from your
 account
def check_phone_number(phone_number):
  try:
    result = sns.check_if_phone_number_is_opted_out(phoneNumber=phone_number)
    if (result['isOptedOut']):
        logger.info('phoneNumber {} is not opt in of receiving SMS messages. Phone
 number must be opt in first.'.format(phone_number))
        return False
    return True
  except Exception as e:
    logging.error('Your phone number {} must be in E.164 format in SSO. Exception
 thrown: {}'.format(phone_number, e))
    return False

def check_emails(emails):
  result = True
  for email in emails:
      if not check_email(email):
          result = False
  return result

def lambda_handler(event, context):
  logging.info('Received event: ' + json.dumps(event))
  nep = json.loads(event.get('notificationEventPayload'))
  alarm_state = nep['alarmState']
  default_msg = 'Alarm ' + alarm_state['stateName'] + '\n'
  timestamp =
 datetime.datetime.utcfromtimestamp(float(nep['stateUpdateTime'])/1000).strftime('%Y-
%m-%d %H:%M:%S')
  alarm_msg = "{} {} {} at {} UTC ".format(nep['alarmModelName'], nep.get('keyValue',
 'Singleton'), alarm_state['stateName'], timestamp)
  default_msg += 'Sev: ' + str(nep['severity']) + '\n'
  if (alarm_state['ruleEvaluation']):
    property = alarm_state['ruleEvaluation']['simpleRule']['inputProperty']
    default_msg += 'Current Value: ' + str(property) + '\n'
    operator = alarm_state['ruleEvaluation']['simpleRule']['operator']
    threshold = alarm_state['ruleEvaluation']['simpleRule']['threshold']
```

```
    alarm_msg += '({} {} {})'.format(str(property), operator, str(threshold))
  default_msg += alarm_msg + '\n'

  emails = event.get('emailConfigurations', [])
  logger.info('Start Sending Emails')
  for email in emails:
    from_adr = email.get('from')
    to_adrs = email.get('to', [])
    cc_adrs = email.get('cc', [])
    bcc_adrs = email.get('bcc', [])
    msg = default_msg + '\n' + email.get('additionalMessage', '')
    subject = email.get('subject', alarm_msg)
    fa_ver = check_email(from_adr)
    tas_ver = check_emails(to_adrs)
    ccas_ver = check_emails(cc_adrs)
    bccas_ver = check_emails(bcc_adrs)
    if (fa_ver and tas_ver and ccas_ver and bccas_ver):
      ses.send_email(Source=from_adr,
                     Destination={'ToAddresses': to_adrs, 'CcAddresses': cc_adrs,
 'BccAddresses': bcc_adrs},
                     Message={'Subject': {'Data': subject}, 'Body': {'Text': {'Data':
 msg}}})
      logger.info('Emails have been sent')

  logger.info('Start Sending SNS message to SMS')
  sns_configs = event.get('smsConfigurations', [])
  for sns_config in sns_configs:
    sns_msg = default_msg + '\n' + sns_config.get('additionalMessage', '')
    phone_numbers = sns_config.get('phoneNumbers', [])
    sender_id = sns_config.get('senderId')
    for phone_number in phone_numbers:
        if check_phone_number(phone_number):
          if check_value(sender_id):
            sns.publish(PhoneNumber=phone_number, Message=sns_msg,
 MessageAttributes={'AWS.SNS.SMS.SenderID':{'DataType': 'String','StringValue':
 sender_id}})
          else:
            sns.publish(PhoneNumber=phone_number, Message=sns_msg)
          logger.info('SNS messages have been sent')
```

Weitere Informationen finden Sie unter Was ist AWS Lambda? im AWS Lambda - Entwicklerhandbuch.

CloudFormation Vorlage

Verwenden Sie die folgende CloudFormation Vorlage, um Ihre Lambda-Funktion zu erstellen.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Notification Lambda for Alarm Model'
Resources:
  NotificationLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: sts:AssumeRole
      Path: "/"
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/AWSLambdaExecute'
      Policies:
        - PolicyName: "NotificationLambda"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: "Allow"
                Action:
                  - "ses:GetIdentityVerificationAttributes"
                  - "ses:SendEmail"
                  - "ses:VerifyEmailIdentity"
                Resource: "*"
              - Effect: "Allow"
                Action:
                  - "sns:Publish"
                  - "sns:OptInPhoneNumber"
                  - "sns:CheckIfPhoneNumberIsOptedOut"
                Resource: "*"
              - Effect: "Deny"
                Action:
                  - "sns:Publish"
                Resource: "arn:aws:sns:*:*:*"
  NotificationLambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      Role: !GetAtt NotificationLambdaRole.Arn
```

```
      Runtime: python3.7
      Handler: index.lambda_handler
      Timeout: 300
      MemorySize: 3008
      Code:
        ZipFile: |
          import boto3
          import json
          import logging
          import datetime
          logger = logging.getLogger()
          logger.setLevel(logging.INFO)
          ses = boto3.client('ses')
          sns = boto3.client('sns')
          def check_value(target):
            if target:
              return True
            return False

          # Check whether email is verified. Only verified emails are allowed to send
 emails to or from.
          def check_email(email):
            if not check_value(email):
              return False
            result = ses.get_identity_verification_attributes(Identities=[email])
            attr = result['VerificationAttributes']
            if (email not in attr or attr[email]['VerificationStatus'] != 'Success'):
                logging.info('Verification email for {} sent. You must have all the
 emails verified before sending email.'.format(email))
                ses.verify_email_identity(EmailAddress=email)
                return False
            return True

          # Check whether the phone holder has opted out of receiving SMS messages from
 your account
          def check_phone_number(phone_number):
            try:
              result = sns.check_if_phone_number_is_opted_out(phoneNumber=phone_number)
              if (result['isOptedOut']):
                  logger.info('phoneNumber {} is not opt in of receiving SMS messages.
 Phone number must be opt in first.'.format(phone_number))
                  return False
              return True
            except Exception as e:
```

```
              logging.error('Your phone number {} must be in E.164 format in SSO.
 Exception thrown: {}'.format(phone_number, e))
              return False

          def check_emails(emails):
            result = True
            for email in emails:
                if not check_email(email):
                    result = False
            return result

          def lambda_handler(event, context):
            logging.info('Received event: ' + json.dumps(event))
            nep = json.loads(event.get('notificationEventPayload'))
            alarm_state = nep['alarmState']
            default_msg = 'Alarm ' + alarm_state['stateName'] + '\n'
            timestamp =
 datetime.datetime.utcfromtimestamp(float(nep['stateUpdateTime'])/1000).strftime('%Y-
%m-%d %H:%M:%S')
            alarm_msg = "{} {} {} at {} UTC ".format(nep['alarmModelName'],
 nep.get('keyValue', 'Singleton'), alarm_state['stateName'], timestamp)
            default_msg += 'Sev: ' + str(nep['severity']) + '\n'
            if (alarm_state['ruleEvaluation']):
              property = alarm_state['ruleEvaluation']['simpleRule']['inputProperty']
              default_msg += 'Current Value: ' + str(property) + '\n'
              operator = alarm_state['ruleEvaluation']['simpleRule']['operator']
              threshold = alarm_state['ruleEvaluation']['simpleRule']['threshold']
              alarm_msg += '({} {} {})'.format(str(property), operator, str(threshold))
            default_msg += alarm_msg + '\n'

            emails = event.get('emailConfigurations', [])
            logger.info('Start Sending Emails')
            for email in emails:
              from_adr = email.get('from')
              to_adrs = email.get('to', [])
              cc_adrs = email.get('cc', [])
              bcc_adrs = email.get('bcc', [])
              msg = default_msg + '\n' + email.get('additionalMessage', '')
              subject = email.get('subject', alarm_msg)
              fa_ver = check_email(from_adr)
              tas_ver = check_emails(to_adrs)
              ccas_ver = check_emails(cc_adrs)
              bccas_ver = check_emails(bcc_adrs)
              if (fa_ver and tas_ver and ccas_ver and bccas_ver):
```

```
                ses.send_email(Source=from_adr,
                               Destination={'ToAddresses': to_adrs, 'CcAddresses':
cc_adrs, 'BccAddresses': bcc_adrs},
                               Message={'Subject': {'Data': subject}, 'Body': {'Text':
{'Data': msg}}})
                logger.info('Emails have been sent')

            logger.info('Start Sending SNS message to SMS')
            sns_configs = event.get('smsConfigurations', [])
            for sns_config in sns_configs:
              sns_msg = default_msg + '\n' + sns_config.get('additionalMessage', '')
              phone_numbers = sns_config.get('phoneNumbers', [])
              sender_id = sns_config.get('senderId')
              for phone_number in phone_numbers:
                  if check_phone_number(phone_number):
                    if check_value(sender_id):
                      sns.publish(PhoneNumber=phone_number, Message=sns_msg,
MessageAttributes={'AWS.SNS.SMS.SenderID':{'DataType': 'String','StringValue':
sender_id}})
                    else:
                      sns.publish(PhoneNumber=phone_number, Message=sns_msg)
                    logger.info('SNS messages have been sent')
```

Verwenden der Lambda-Funktion von AWS IoT Events

Die folgenden Anforderungen gelten, wenn Sie die Lambda-Funktion von verwenden AWS IoT Events , um Ihre Alarmbenachrichtigungen zu verwalten:

- Sie müssen die E-Mail-Adresse, mit der die E-Mail-Benachrichtigungen gesendet werden, in Amazon Simple Email Service (AmazonSES) verifizieren. Weitere Informationen finden Sie unter Verifizieren von E-Mail-Adressen bei Amazon im Amazon SES Simple Email Service Developer Guide.

  Wenn Sie einen Bestätigungslink erhalten, klicken Sie auf den Link, um Ihre E-Mail-Adresse zu verifizieren. Sie können auch in Ihrem Spam-Ordner nach einer Bestätigungs-E-Mail suchen.
- Wenn Ihr Alarm SMS Benachrichtigungen sendet, müssen Sie die internationale E.164-Telefonnummernformatierung für Telefonnummern verwenden. Dieses Format enthält+`<country-calling-code><area-code><phone-number>`.

  Beispiele für Telefonnummern:

Land	Lokale Telefonnummer	E.164 formatierte Nummer
Vereinigte Staaten	206-555-0100	+12065550100
Großbritannien und Nordirland	020-1234-1234	+442012341234
Litauen	+601+12345	+37060112345

Um eine Landesvorwahl zu finden, gehen Sie zu countrycode.org.

Die von bereitgestellte Lambda-Funktion AWS IoT Events überprüft, ob Sie E.164-formatierte Telefonnummern verwenden. Die Telefonnummern werden jedoch nicht überprüft. Wenn Sie sicherstellen, dass Sie korrekte Telefonnummern eingegeben, aber keine SMS Benachrichtigungen erhalten haben, können Sie sich an die Telefonanbieter wenden. Die Mobilfunkanbieter können die Nachrichten blockieren.

Verwalten Sie den IAM Identity Center-Zugriff von Alarmempfängern

AWS IoT Events wird verwendet AWS IAM Identity Center , um den SSO Zugriff von Alarmempfängern zu verwalten. Damit der Alarm Benachrichtigungen an die Empfänger senden kann, müssen Sie IAM Identity Center aktivieren und Empfänger zu Ihrem IAM Identity Center-Shop hinzufügen. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Benutzer hinzufügen.

> **Important**
>
> - Sie müssen dieselbe AWS Region für AWS IoT Events AWS Lambda, und IAM Identity Center wählen.
> - AWS Organizations unterstützt jeweils nur eine IAM Identity Center-Region. Wenn Sie IAM Identity Center in einer anderen Region verfügbar machen möchten, müssen Sie zuerst Ihre aktuelle IAM Identity Center-Konfiguration löschen. Weitere Informationen finden Sie unter IAMIdentity Center-Regionsdaten im AWS IAM Identity Center Benutzerhandbuch.

Sicherheit in AWS IoT Events

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

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud 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. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des AWS -Compliance-Programms getestet und überprüft. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS IoT Events, finden Sie unter AWS Services nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

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

Themen

Identitäts- und Zugriffsmanagement für AWS IoT Events

AWS Identity and Access Management (IAM) ist ein AWS Dienst, der einem Administrator hilft, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AWS IoT Events Ressourcen zu verwenden. IAMist ein AWS Service, den Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten AWS IoT Events.

Dienstbenutzer — Wenn Sie den AWS IoT Events Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS IoT Events 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 Fehlerbehebung bei AWS IoT Events Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS IoT Events haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS IoT Events Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS IoT Events. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS IoT Events Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite,

um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit verwenden kann AWS IoT Events, finden Sie unterWie AWS IoT Events funktioniert mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten AWS IoT Events. Beispiele für AWS IoT Events identitätsbasierte Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. AWS IoT Events 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 übernehmen. 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 (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, 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 darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. 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 IAMBenutzerhandbuch 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) 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. Sie können darauf zugreifen, 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 im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. 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 AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- 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 im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, 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 verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS -Services verwenden Funktionen in anderen. AWS -Services Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen

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 beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.
- Dienstbezogene Rolle — Eine dienstverknüpfte 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 dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

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 in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und

zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

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 oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren 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 zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (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 Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung 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 im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

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 IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

Weitere Informationen

Weitere Informationen zur Identitäts- und Zugriffsverwaltung für AWS IoT Events finden Sie auf den folgenden Seiten:

- Wie AWS IoT Events funktioniert mit IAM
- Fehlerbehebung bei AWS IoT Events Identität und Zugriff

Wie AWS IoT Events funktioniert mit IAM

Bevor Sie IAM den Zugriff auf verwalten AWS IoT Events, sollten Sie sich darüber im Klaren sein, welche IAM Funktionen zur Verwendung verfügbar sind AWS IoT Events. Einen allgemeinen Überblick darüber, wie AWS IoT Events und mit anderen AWS Diensten funktioniertIAM, finden Sie IAM im IAMBenutzerhandbuch unter AWS Dienste, mit denen Sie arbeiten können.

Themen

- AWS IoT Events identitätsbasierte Richtlinien
- Ressourcenbasierte AWS IoT Events -Richtlinien
- Autorisierung auf der Basis von AWS IoT Events -Tags
- AWS IoT Events IAMRollen

AWS IoT Events identitätsbasierte Richtlinien

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. AWS IoT Events unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Aktionen

Das `Action` Element einer IAM identitätsbasierten Richtlinie beschreibt die spezifischen Aktionen, die durch die Richtlinie zugelassen oder verweigert werden. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Die Aktion wird in einer Richtlinie verwendet, um Berechtigungen zur Durchführung der zugehörigen Aktion zu gewähren.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS IoT Events verwendet:`iotevents:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, mit der AWS IoT Events `CreateInput` API Operation eine AWS IoT Events Eingabe zu erstellen, nehmen Sie die `iotevents:CreateInput` Aktion in seine Richtlinie auf. Um jemandem die Erlaubnis zu erteilen, eine Eingabe zusammen mit dem AWS IoT Events `BatchPutMessage` API Vorgang zu

senden, nehmen Sie die `iotevents-data:BatchPutMessage` Aktion in seine Richtlinie auf. Richtlinienerklärungen müssen `Action` entweder ein `NotAction` Oder-Element enthalten. AWS IoT Events 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 wie folgt durch Kommata:

```
"Action": [
      "iotevents:action1",
      "iotevents: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": "iotevents:Describe*"
```

Eine Liste der AWS IoT Events Aktionen finden Sie AWS IoT Events im IAMBenutzerhandbuch unter Definierte Aktionen von.

Ressourcen

Das Element `Resource` gibt die Objekte an, auf die die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource`- oder ein `NotResource`-Element enthalten. Sie geben eine Ressource mit einem ARN oder mit dem Platzhalter (*) an, um anzugeben, dass die Anweisung für alle Ressourcen gilt.

Die Modellressource des AWS IoT Events Detektors hat Folgendes: ARN

```
arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${detectorModelName}
```

Weitere Informationen zum Format von ARNs finden Sie unter Identifizieren von AWS Ressourcen mit Amazon-Ressourcennamen (ARNs).

Um beispielsweise das `Foobar` Detektormodell in Ihrer Anweisung zu spezifizieren, verwenden Sie FolgendesARN:

```
"Resource": "arn:aws:iotevents:us-east-1:123456789012:detectorModel/Foobar"
```

Um alle Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:iotevents:us-east-1:123456789012:detectorModel/*"
```

Einige AWS IoT Events Aktionen, z. B. die zum Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

Manche AWS IoT Events API Aktionen betreffen mehrere Ressourcen. Verweist beispielsweise in seinen Bedingungsanweisungen `CreateDetectorModel` auf Eingaben, sodass ein Benutzer über Berechtigungen zur Verwendung der Eingabe und des Detektormodells verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

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

Eine Liste der AWS IoT Events Ressourcentypen und ihrer Eigenschaften ARNs finden Sie unter Ressourcen definiert von AWS IoT Events im IAMBenutzerhandbuch. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Definierte Aktionen von AWS IoT Events.

Bedingungsschlüssel

Mithilfe des Elements `Condition`(oder des Blocks `Condition`) können Sie die Bedingungen angeben, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungs-Operatoren 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 Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS IoT Events stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.“

Beispiele

Beispiele für AWS IoT Events identitätsbasierte Richtlinien finden Sie unter. AWS IoT Events Beispiele für identitätsbasierte Richtlinien

Ressourcenbasierte AWS IoT Events -Richtlinien

AWS IoT Events unterstützt keine ressourcenbasierten Richtlinien.“ Ein Beispiel für eine detaillierte Seite zu ressourcenbasierten Richtlinien finden Sie unter https://docs.aws.amazon.com/lambda/latest/dg/access-control-resource-based.html.

Autorisierung auf der Basis von AWS IoT Events -Tags

Sie können Tags an AWS IoT Events Ressourcen anhängen oder Tags in einer Anfrage an übergeben. AWS IoT Events Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `iotevents:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen über das Markieren von AWS IoT Events -Ressourcen mit Tags finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT Events.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Auf Tags basierende AWS IoT Events Eingaben anzeigen.

AWS IoT Events IAMRollen

Eine IAMRolle ist eine Entität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit AWS IoT Events

Sie können temporäre Anmeldeinformationen verwenden, um sich beim Verband anzumelden, eine IAM Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS Security Token Service (AWS STS) API -Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

AWS IoT Events unterstützt die Verwendung temporärer Anmeldeinformationen nicht.

Service-verknüpfte Rollen

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

AWS IoT Events unterstützt keine dienstbezogenen Rollen.

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 dem Konto. Das bedeutet, dass ein IAM Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

AWS IoT Events unterstützt Servicerollen.

AWS IoT Events Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AWS IoT Events Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit dem AWS Management Console AWS CLI, oder ausführen AWS API. Ein IAM Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Berechtigung gewähren, bestimmte API Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter Richtlinien erstellen auf der JSON Registerkarte im IAMBenutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand AWS IoT Events 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:

- Erste Schritte mit AWS verwalteten Richtlinien — Um AWS IoT Events schnell mit der Nutzung zu beginnen, sollten Sie AWS verwaltete Richtlinien verwenden, um Ihren Mitarbeitern die erforderlichen Berechtigungen zu erteilen. Diese Richtlinien sind bereits in Ihrem Konto verfügbar und werden von AWS. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erste Schritte zur Nutzung von Berechtigungen mit AWS verwalteten Richtlinien.
- Gewähren Sie die geringstmöglichen Berechtigungen – Gewähren Sie beim Erstellen benutzerdefinierter Richtlinien nur die Berechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Beginnen Sie mit einem Mindestsatz von Berechtigungen und gewähren Sie zusätzliche Berechtigungen wie erforderlich. Dies ist sicherer, als mit Berechtigungen zu beginnen, die zu weit gefasst sind, und dann später zu versuchen, sie zu begrenzen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Gewährung der geringsten Zugriffsrechte.
- MFAFür vertrauliche Operationen aktivieren — Für zusätzliche Sicherheit müssen Benutzer für den Zugriff auf vertrauliche Ressourcen oder API Vorgänge die Multi-Faktor-Authentifizierung (MFA) verwenden. Weitere Informationen finden Sie im AWSIAMBenutzerhandbuch unter Verwenden der Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie Richtlinienbedingungen, um zusätzliche Sicherheit zu bieten – Definieren Sie die Bedingungen, unter denen Ihre identitätsbasierten Richtlinien den Zugriff auf eine Ressource zulassen, soweit praktikabel. Beispielsweise können Sie Bedingungen schreiben, die eine Reihe von zulässigen IP-Adressen festlegen, von denen eine Anforderung stammen muss. Sie können auch Bedingungen schreiben, um Anfragen nur innerhalb eines bestimmten Datums- oder Zeitbereichs zuzulassen oder die Verwendung von SSL oder MFA vorzuschreiben.

Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.

Verwenden der AWS IoT Events -Konsole

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

Um sicherzustellen, dass diese Entitäten die AWS IoT Events Konsole weiterhin verwenden können, fügen Sie den Entitäten außerdem die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents-data:BatchPutMessage",
                "iotevents-data:BatchUpdateDetector",
                "iotevents:CreateDetectorModel",
                "iotevents:CreateInput",
                "iotevents:DeleteDetectorModel",
                "iotevents:DeleteInput",
                "iotevents-data:DescribeDetector",
                "iotevents:DescribeDetectorModel",
                "iotevents:DescribeInput",
                "iotevents:DescribeLoggingOptions",
                "iotevents:ListDetectorModelVersions",
                "iotevents:ListDetectorModels",
                "iotevents-data:ListDetectors",
                "iotevents:ListInputs",
                "iotevents:ListTagsForResource",
                "iotevents:PutLoggingOptions",
                "iotevents:TagResource",
                "iotevents:UntagResource",
```

```
                "iotevents:UpdateDetectorModel",
                "iotevents:UpdateInput",
                "iotevents:UpdateInputRouting"
            ],
            "Resource": "arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/
${detectorModelName}",
            "Resource": "arn:${Partition}:iotevents:${Region}:${Account}:input/
${inputName}"
        }
    ]
}
```

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder den tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den Sie ausführen möchten.

Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen

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

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

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

Zugreifen auf eine Eingabe AWS IoT Events

In diesem Beispiel möchten Sie einem Benutzer AWS-Konto Zugriff auf eine Ihrer AWS IoT Events Eingaben gewährenexampleInput. Sie möchten dem Benutzer auch ermöglichen, Eingaben hinzuzufügen, zu aktualisieren und zu löschen.

Die Richtlinie gewährt dem Benutzer die Berechtigungen `iotevents:ListInputs`, `iotevents:DescribeInput`, `iotevents:CreateInput`, `iotevents:DeleteInput` und `iotevents:UpdateInput`. Ein Beispiel für den Amazon Simple Storage Service (Amazon S3), der Benutzern Berechtigungen erteilt und sie mithilfe der Konsole testet, finden Sie unter Steuern des Zugriffs auf einen Bucket mit Benutzerrichtlinien.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListInputsInConsole",
         "Effect":"Allow",
         "Action":[
            "iotevents:ListInputs"
         ],
         "Resource":"arn:aws:iotevents:::*"
      },
      {
         "Sid":"ViewSpecificInputInfo",
         "Effect":"Allow",
```

```
            "Action":[
               "iotevents:DescribeInput"
            ],
            "Resource":"arn:aws:iotevents:::exampleInput"
         },
         {
            "Sid":"ManageInputs",
            "Effect":"Allow",
            "Action":[
               "iotevents:CreateInput",
               "iotevents:DeleteInput",
               "iotevents:DescribeInput",
               "iotevents:ListInputs",
               "iotevents:UpdateInput"
            ],
            "Resource":"arn:aws:iotevents:::exampleInput/*"
         }
      ]
   }
```

Auf Tags basierende AWS IoT Events Eingaben anzeigen

Sie können in Ihrer identitätsbasierten Richtlinie Bedingungen für die Steuerung des Zugriffs auf AWS IoT Events -Ressourcen auf der Basis von Tags verwenden. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die das Anzeigen eines *`input`*. Die Genehmigung wird jedoch nur erteilt, wenn *`input`* Tag `Owner` hat den Wert des Benutzernamens dieses Benutzers. Diese Richtlinie gewährt auch die Berechtigungen, die für die Ausführung dieser Aktion auf der Konsole erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListInputsInConsole",
            "Effect": "Allow",
            "Action": "iotevents:ListInputs",
            "Resource": "*"
        },
        {
            "Sid": "ViewInputsIfOwner",
            "Effect": "Allow",
            "Action": "iotevents:ListInputs",
```

```
            "Resource": "arn:aws:iotevents:*:*:input/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Sie können diese Richtlinie den -Benutzern in Ihrem Konto zuweisen. Wenn ein benannter Benutzer `richard-roe` versucht, ein AWS IoT Events *`input`*, der *`input`* muss markiert sein `Owner=richard-roe` oder`owner=richard-roe`. Andernfalls wird der Zugriff abgelehnt. Der Tag-Schlüssel `Owner` der Bedingung stimmt sowohl mit `Owner` als auch mit `owner` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAMJSONRichtlinienelemente: Zustand im IAMBenutzerhandbuch.

Serviceübergreifende Confused-Deputy-Prävention

> **Note**
>
> - Der AWS IoT Events Dienst ermöglicht es Kunden nur, Rollen zu verwenden, um Aktionen in demselben Konto zu starten, in dem eine Ressource erstellt wurde. Das bedeutet, dass ein Confused Deputy Attack mit diesem Service nicht durchgeführt werden kann.
> - Diese Seite dient Kunden als Referenz, um zu erfahren, wie das Problem mit dem verwirrten Stellvertreter funktioniert. Sie kann verhindert werden, wenn kontoübergreifende Ressourcen für den AWS IoT Events Service zugelassen wurden.

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In der AWS Praxis kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit dem verwirrten Stellvertreter führen.

Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS bietet Tools, mit denen Sie Ihre Daten für alle Dienste mit Dienstprinzipalen schützen können, denen Zugriff auf Ressourcen in Ihrem Konto gewährt wurde.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, AWS IoT Events die der Ressource einen anderen Dienst gewähren. Wenn der `aws:SourceArn` Wert die Konto-ID nicht enthält, z. B. ein Amazon S3 S3-BucketARN, müssen Sie beide globalen Bedingungskontextschlüssel verwenden, um die Berechtigungen einzuschränken. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird.

Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden. Der Wert von `aws:SourceArn` muss dem Detektor- oder Alarmmodell entsprechen, das der `sts:AssumeRole` Anfrage zugeordnet ist.

Der wirksamste Schutz vor dem Problem mit dem verwirrten Deputy ist die Verwendung des `aws:SourceArn` globalen Condition-Kontextschlüssels mit ARN der gesamten Ressource. Wenn Sie die gesamte ARN Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit Platzhaltern (`*`) für die unbekannten Teile von. ARN Beispiel, `arn:aws:iotevents:*:123456789012:*`.

Die folgenden Beispiele zeigen, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, AWS IoT Events um das Problem des verwirrten Stellvertreters zu vermeiden.

Themen

- Beispiel: Zugriff auf ein Detektormodell
- Beispiel: Zugriff auf ein Alarmmodell
- Beispiel: Zugriff auf eine Ressource in einer bestimmten Region
- Beispiel: Protokollierungsoptionen

Beispiel: Zugriff auf ein Detektormodell

In diesem Beispiel kann die angegebene Rolle nur für den Zugriff auf das angegebene `foo` Detektormodell verwendet werden.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account_id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:iotevents:region:account_id:detectorModel/foo"
        }
      }
    }
  ]
 }
}
```

Beispiel: Zugriff auf ein Alarmmodell

Das folgende Beispiel zeigt, wie Sie AWS IoT Events Zugriff auf das Senden von Daten an einen Alarm gewähren und gleichzeitig die Rechte zur Änderung der Alarmkonfiguration mithilfe einer IAM Richtlinie einschränken.

Die folgende Rolle kann nur für den Zugriff auf ein beliebiges Alarmmodell verwendet werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "account_id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:iotevents:region:account_id:alarmModel/*"
        }
      }
    }
  ]
}
```

Beispiel: Zugriff auf eine Ressource in einer bestimmten Region

Das folgende Beispiel zeigt eine Rolle, mit der Sie auf eine Ressource in einer bestimmten Region zugreifen können. Die Region in diesem Beispiel ist *us-east-1*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account_id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:iotevents:us-east-1:account_id:*"
        }
      }
    }
  ]
}
```

Beispiel: Protokollierungsoptionen

Um den Protokollierungsoptionen eine Rolle zuzuweisen, müssen Sie zulassen, dass sie von jeder AWS IoT Events Ressource übernommen wird. Verwenden Sie sowohl für den Ressourcentyp als auch für den Namen einen Platzhalter (*).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotevents.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account_id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:iotevents:region:account_id:*"
        }
      }
    }
  ]
}
```

Fehlerbehebung bei AWS IoT Events Identität und Zugriff

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

Themen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS IoT Events

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 folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einem anzuzeigen *`input`* hat aber keine `iotevents:`*`ListInputs`* Berechtigungen.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotevents:ListInputs on resource: my-example-input
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-input`* auf die Ressource `iotevents:`*`ListInput`* zugreifen zu können.

Ich bin nicht zur Ausführung von **`iam:PassRole`** autorisiert.

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 IoT Eventsübergeben 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 IoT Events 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 zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS IoT Events 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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Sehen Sie sich die folgenden Themen an, um herauszufinden, welche Optionen am besten geeignet sind:

- Informationen darüber, ob diese Funktionen AWS IoT Events unterstützt werden, finden Sie unterWie AWS IoT Events funktioniert mit IAM.
- Informationen darüber, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen IAMBenutzer AWS-Konto , dessen Eigentümer Sie sind.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Überwachung AWS IoT Events

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS IoT Events und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. Bevor Sie mit der Überwachung beginnen AWS IoT Events, sollten Sie einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Überwachungsziele?
- Welche Ressourcen möchten Sie überwachen?
- Wie oft werden diese Ressourcen überwacht?

- Welche Überwachungs-Tools möchten Sie verwenden?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Der nächste Schritt besteht darin, eine Ausgangsbasis für die normale AWS IoT Events Leistung in Ihrer Umgebung festzulegen, indem Sie die Leistung zu verschiedenen Zeiten und unter verschiedenen Lastbedingungen messen. Speichern Sie bei der Überwachung von AWS IoT Events historische Überwachungsdaten, damit Sie diese mit aktuellen Leistungsdaten vergleichen, normale Leistungsmuster bestimmen, Leistungsprobleme erkennen und Methoden zur Fehlerbehebung ableiten können.

Wenn Sie beispielsweise Amazon verwenden, können Sie die CPU AuslastungEC2, Festplatten-I/O und Netzwerkauslastung für Ihre Instances überwachen. Wenn die Leistung außerhalb Ihrer festgelegten Ausgangswerte liegt, müssen Sie die Instance möglicherweise neu konfigurieren oder optimieren, um die CPU Auslastung zu reduzieren, die Festplatten-I/O zu verbessern oder den Netzwerkverkehr zu reduzieren.

Themen

Überwachungstools

AWS bietet verschiedene Tools, die Sie zur Überwachung verwenden können AWS IoT Events. Sie können einige dieser Tools so konfigurieren, dass diese die Überwachung für Sie übernehmen, während bei anderen Tools ein manuelles Eingreifen nötig ist. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Automatisierte Überwachungstools

Sie können die folgenden automatisierten Überwachungstools verwenden, um zu beobachten AWS IoT Events und zu melden, wenn etwas nicht stimmt:

- Amazon CloudWatch Logs — Überwachen, speichern und greifen Sie auf Ihre Protokolldateien aus AWS CloudTrail oder anderen Quellen zu. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Dashboards im CloudWatch Amazon-Benutzerhandbuch.

- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Protokollverarbeitungsanwendungen in Java und überprüfen Sie, ob sich Ihre Protokolldateien nach der Lieferung von nicht geändert haben. CloudTrail Weitere Informationen finden Sie unter Arbeiten mit CloudTrail Protokolldateien im AWS CloudTrail Benutzerhandbuch.

Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung AWS IoT Events umfasst die manuelle Überwachung der Elemente, die von den CloudWatch Alarmen nicht abgedeckt werden. Die Dashboards AWS IoT Events CloudWatch, und andere AWS Konsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand Ihrer AWS Umgebung. Wir empfehlen, dass Sie auch die Protokolldateien unter AWS IoT Eventsüberprüfen.

- Die AWS IoT Events Konsole zeigt:
  - Detektormodelle
  - Detektoren
  - Eingaben
  - Einstellungen
- Auf der CloudWatch Startseite wird Folgendes angezeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

  Darüber hinaus können CloudWatch Sie Folgendes verwenden:
  - Erstellen angepasster Dashboards zur Überwachung der gewünschten Services.
  - Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen
  - Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden

Überwachung mit Amazon CloudWatch

Wenn Sie ein AWS IoT Events Detektormodell entwickeln oder debuggen, müssen Sie wissen, was AWS IoT Events gerade passiert und welche Fehler dabei auftreten. Amazon CloudWatch überwacht

Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Damit CloudWatch erhalten Sie systemweiten Einblick in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand. Aktivieren Sie die CloudWatch Amazon-Protokollierung bei der Entwicklung von AWS IoT Events Detektormodellenenthält Informationen zur Aktivierung der CloudWatch Protokollierung für AWS IoT Events. Um Protokolle wie das unten gezeigte zu generieren, müssen Sie den Ausführlichkeitsgrad auf „Debug“ setzen und ein oder mehrere Debug-Ziele angeben, d. h. einen Modellnamen des Detektors und ein optionales. KeyValue

Das folgende Beispiel zeigt einen CloudWatch DEBUG Level-Logeintrag, der von generiert wurde. AWS IoT Events

```
{
  "timestamp": "2019-03-15T15:56:29.412Z",
  "level": "DEBUG",
  "logMessage": "Summary of message evaluation",
  "context": "MessageEvaluation",
  "status": "Success",
  "messageId": "SensorAggregate_2th846h",
  "keyValue": "boiler_1",
  "detectorModelName": "BoilerAlarmDetector",
  "initialState": "high_temp_alarm",
  "initialVariables": {
    "high_temp_count": 1,
    "high_pressure_count": 1
  },
  "finalState": "no_alarm",
  "finalVariables": {
    "high_temp_count": 0,
    "high_pressure_count": 0
  },
  "message": "{ \"temp\": 34.9, \"pressure\": 84.5}",
  "messageType": "CUSTOMER_MESSAGE",
  "conditionEvaluationResults": [
    {
      "result": "True",
      "eventName": "alarm_cleared",
      "state": "high_temp_alarm",
      "lifeCycle": "OnInput",
      "hasTransition": true
    },
    {
      "result": "Skipped",
```

```
      "eventName": "alarm_escalated",
      "state": "high_temp_alarm",
      "lifeCycle": "OnInput",
      "hasTransition": true,
      "resultDetails": "Skipped due to transition from alarm_cleared event"
    },
    {
      "result": "True",
      "eventName": "should_recall_technician",
      "state": "no_alarm",
      "lifeCycle": "OnEnter",
      "hasTransition": true
    }
  ]
}
```

AWS IoT Events APIAnrufe protokollieren mit AWS CloudTrail

AWS IoT Events ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS IoT Events. CloudTrail erfasst alle API Aufrufe AWS IoT Events als Ereignisse, einschließlich Aufrufe von der AWS IoT Events Konsole und von Codeaufrufen an den AWS IoT Events APIs.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS IoT Events. 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 ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS IoT Events, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS IoT Events Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS IoT Events, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Ereignishistorie aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS IoT Events, 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 der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. 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 unter:

- Einen Trail für dein AWS Konto erstellen
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von SNS Amazon-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder IAM Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie im CloudTrail userIdentityElement. AWS IoT Events Aktionen sind in der AWS IoT Events APIReferenz dokumentiert.

AWS IoT Events Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. AWS 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.

Wenn die CloudTrail Protokollierung in Ihrem AWS Konto aktiviert ist, werden die meisten API Aufrufe von AWS IoT Events Aktionen in CloudTrail Protokolldateien aufgezeichnet, wo sie zusammen

mit anderen AWS Serviceaufzeichnungen geschrieben werden. CloudTrailbestimmt anhand eines Zeitraums und der Dateigröße, wann eine neue Datei erstellt und in diese geschrieben werden soll.

Jeder Protokolleintrag enthält Informationen über den Ersteller der Anforderung. Der Benutzeridentität im Protokolleintrag können Sie folgende Informationen entnehmen:

- Ob die Anfrage mit Root- oder IAM Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

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

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

Sie können auch AWS IoT Events 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.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DescribeDetector` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/bertholt-brecht",
    "accountId": "123456789012",
    "accessKeyId": "access-key-id",
    "sessionContext": {
      "attributes": {
```

```
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-08T18:53:58Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  },
  "eventTime": "2019-02-08T19:02:44Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DescribeDetector",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-cli/1.15.65 Python/3.7.1 Darwin/16.7.0 botocore/1.10.65",
  "requestParameters": {
    "detectorModelName": "pressureThresholdEventDetector-brecht",
    "keyValue": "1"
  },
  "responseElements": null,
  "requestID": "00f41283-ea0f-4e85-959f-bee37454627a",
  "eventID": "5eb0180d-052b-49d9-a289-0eb8d08d4c27",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateDetectorModel` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-Lambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEvents-RoleForIotEvents-
ABC123DEF456/IotEvents-Lambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
```

```
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABC123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABC123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:54:43Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "CreateDetectorModel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "myDetectorModel",
    "key": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "roleArn": "arn:aws:iam::123456789012:role/events_action_execution_role"
  },
  "responseElements": null,
  "requestID": "cecfbfa1-e452-4fa6-b86b-89a89f392b66",
  "eventID": "8138d46b-50a3-4af0-9c5e-5af5ef75ea55",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateInput` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-Lambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABC123DEF456/IotEvents-Lambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
```

```
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABC123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABC123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:54:43Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "CreateInput",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "inputName": "batchputmessagedetectorupdated",
    "inputDescription": "batchputmessagedetectorupdated"
  },
  "responseElements": null,
  "requestID": "fb315af4-39e9-4114-94d1-89c9183394c1",
  "eventID": "6d8cf67b-2a03-46e6-bbff-e113a7bded1e",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DeleteDetectorModel` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
```

```
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:54:11Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DeleteDetectorModel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "myDetectorModel"
  },
  "responseElements": null,
  "requestID": "149064c1-4e24-4160-a5b2-1065e63ee2e4",
  "eventID": "7669db89-dcc0-4c42-904b-f24b764dd808",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DeleteInput` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
```

```
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:54:38Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DeleteInput",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "errorCode": "ResourceNotFoundException",
  "errorMessage": "Input of name: NoSuchInput not found",
  "requestParameters": {
    "inputName": "NoSuchInput"
  },
  "responseElements": null,
  "requestID": "ce6d28ac-5baf-423d-a5c3-afd009c967e3",
  "eventID": "be0ef01d-1c28-48cd-895e-c3ff3172c08e",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DescribeDetectorModel` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
```

```
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:54:20Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DescribeDetectorModel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "myDetectorModel"
  },
  "responseElements": null,
  "requestID": "18a11622-8193-49a9-85cb-1fa6d3929394",
  "eventID": "1ad80ff8-3e2b-4073-ac38-9cb3385beb04",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DescribeInput` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
```

```
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AAKIAI44QH8DHBEXAMPLE",
    "sessionContext": {

      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:56:09Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DescribeInput",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "inputName": "input_createinput"
  },
  "responseElements": null,
  "requestID": "3af641fa-d8af-41c9-ba77-ac9c6260f8b8",
  "eventID": "bc4e6cc0-55f7-45c1-b597-ec99aa14c81a",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `DescribeLoggingOptions` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
```

```
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:23Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "DescribeLoggingOptions",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "b624b6c5-aa33-41d8-867b-025ec747ee8f",
  "eventID": "9c7ce626-25c8-413a-96e7-92b823d6c850",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListDetectorModels` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
```

```
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:23Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "ListDetectorModels",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "nextToken": "CkZEZXRlY3Rvck1vZGVsMl9saXN0ZGV0ZWN0b3Jtb2RlbHN0ZXN0X2VlOWJkZTk1YT",
    "maxResults": 3
  },
  "responseElements": null,
  "requestID": "6d70f262-da95-4bb5-94b4-c08369df75bb",
  "eventID": "2d01a25c-d5c7-4233-99fe-ce1b8ec05516",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListDetectorModelVersions` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
```

```
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:33Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "ListDetectorModelVersions",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "myDetectorModel",
    "maxResults": 2
  },
  "responseElements": null,
  "requestID": "ebecb277-6bd8-44ea-8abd-fbf40ac044ee",
  "eventID": "fc6281a2-3fac-4e1e-98e0-ca6560b8b8be",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListDetectors` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
```

```
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:54Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "ListDetectors",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "batchputmessagedetectorinstancecreated",
    "stateName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "4783666d-1e87-42a8-85f7-22d43068af94",
  "eventID": "0d2b7e9b-afe6-4aef-afd2-a0bb1e9614a9",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListInputs` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
```

```
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:57Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "ListInputs",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "nextToken": "CkhjYW5hcnlfdGVzdF9pbnB1dF9saXN0ZGV0ZWN0b3Jtb2RlbHN0ZXN0ZDU3OGZ",
    "maxResults": 3
  },
  "responseElements": null,
  "requestID": "dd6762a1-1f24-4e63-a986-5ea3938a03da",
  "eventID": "c500f6d8-e271-4366-8f20-da4413752469",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `PutLoggingOptions` Aktion demonstriert.

```
{
```

```
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:56:43Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "PutLoggingOptions",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "loggingOptions": {
      "roleArn": "arn:aws:iam::123456789012:role/logging__logging_role",
      "level": "INFO",
      "enabled": false
    }
  },
  "responseElements": null,
  "requestID": "df570e50-fb19-4636-9ec0-e150a94bc52c",
  "eventID": "3247f928-26aa-471e-b669-e4a9e6fbc42c",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateDetectorModel` Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:55:51Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "UpdateDetectorModel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "detectorModelName": "myDetectorModel",
    "roleArn": "arn:aws:iam::123456789012:role/Events_action_execution_role"
  },
  "responseElements": null,
  "requestID": "add29860-c1c5-4091-9917-d2ef13c356cf",
  "eventID": "7baa9a14-6a52-47dc-aea0-3cace05147c3",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateInput` Aktion demonstriert.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAI44QH8DHBEXAMPLE:IotEvents-EventsLambda",
    "arn": "arn:aws:sts::123456789012:assumed-role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456/IotEvents-EventsLambda",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-02-07T22:22:30Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/IotEventsLambda-RoleForIotEvents-
ABCD123DEF456",
        "accountId": "123456789012",
        "userName": "IotEventsLambda-RoleForIotEvents-ABCD123DEF456"
      }
    }
  },
  "eventTime": "2019-02-07T23:53:00Z",
  "eventSource": "iotevents.amazonaws.com",
  "eventName": "UpdateInput",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.1",
  "userAgent": "aws-internal/3",
  "errorCode": "ResourceNotFoundException",
  "errorMessage": "Input of name: NoSuchInput not found",
  "requestParameters": {
    "inputName": "NoSuchInput",
    "inputDescription": "this is a description of an input"
  },
  "responseElements": null,
  "requestID": "58d5d2bb-4110-4c56-896a-ee9156009f41",
  "eventID": "c2df241a-fd53-4fd0-936c-ba309e5dc62d",
  "eventType": "AwsApiCall",
```

```
  "recipientAccountId": "123456789012"
}
```

Konformitätsvalidierung für AWS IoT Events

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 Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

  > **Note**
  >
  > Nicht alle sind berechtigt AWS -Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- 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 für 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)) zusammengefasst.

- 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— Auf diese AWS -Service Weise erhalten Sie 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.
- Amazon GuardDuty — Dies AWS -Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- 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 IoT Events

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

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

Infrastruktursicherheit in AWS IoT Events

Als verwalteter Dienst AWS IoT Events ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung

der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API Aufrufe für den Zugriff über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

AWS Servicekontingenten für AWS IoT Events Ressourcen

Der Allgemeine AWS-Referenz Leitfaden enthält die Standardkontingente AWS IoT Events für ein AWS Konto. Sofern nicht anders angegeben, gilt jedes Kontingent pro AWS Region. Weitere Informationen finden Sie im Allgemeine AWS-Referenz Handbuch unter AWS IoT Events Endpunkte und Kontingente und AWS Service Quotas.

Um eine Erhöhung des Servicekontingents zu beantragen, reichen Sie in der Support Center-Konsole eine Support-Anfrage ein. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

> **Note**
>
> - Alle Namen für Meldermodelle und Eingänge müssen innerhalb eines Kontos eindeutig sein.
> - Sie können die Namen von Meldermodellen und Eingängen nicht mehr ändern, nachdem sie erstellt wurden.

Verschlagworten Sie Ihre Ressourcen AWS IoT Events

Um Ihnen die Verwaltung und Organisation Ihrer Detektormodelle und Eingänge zu erleichtern, können Sie optional jeder dieser Ressourcen Ihre eigenen Metadaten in Form von Tags zuweisen. In diesem Abschnitt werden Tags und deren Erstellung beschrieben.

Grundlagen zu Tags (Markierungen)

Mithilfe von Tags können Sie Ihre AWS IoT Events Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. Sie können eine bestimmte Ressource anhand der ihr zugewiesenen Tags schnell identifizieren.

Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, die Sie beide selbst definieren können. Sie könnten beispielsweise eine Reihe von Tags für Ihre Eingaben definieren, mit deren Hilfe Sie die Geräte, die diese Eingaben senden, anhand ihres Typs verfolgen können. Wir empfehlen die Erstellung von Tag-Schlüsseln, die die Anforderungen der jeweiligen Ressourcenart erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen.

Sie können anhand der von Ihnen hinzugefügten oder angewendeten Tags nach Ressourcen suchen und diese filtern, Tags verwenden, um Ihre Kosten zu kategorisieren und nachzuverfolgen, und auch Tags verwenden, um den Zugriff auf Ihre Ressourcen zu kontrollieren, wie unter Verwenden von Tags mit IAM Richtlinien im AWS IoT Entwicklerhandbuch beschrieben.

Um die Bedienung zu vereinfachen, AWS Management Console bietet der Tag-Editor im eine zentrale, einheitliche Möglichkeit, Ihre Tags zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Erste Schritte mit dem Tag-Editor im AWS Tagging-Ressourcen- und Tag-Editor-Benutzerhandbuch.

Sie können auch mit Tags arbeiten, indem Sie den AWS CLI und den AWS IoT Events API verwenden. Sie können Tags bei der Erstellung mit Detektormodellen und Eingaben verknüpfen, indem Sie das `"Tags"` Feld in den folgenden Befehlen verwenden:

- CreateDetectorModel
- CreateInput

Sie können Tags für vorhandene Ressourcen, die das Markieren unterstützen, hinzufügen, ändern oder löschen. Verwenden Sie dazu die folgenden Befehle:

- TagResource
- ListTagsForResource
- UntagResource

Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle der Ressource zugeordneten Tags ebenfalls gelöscht.

Weitere Informationen finden Sie unter Bewährte Methoden für das Markieren von Ressourcen AWS

Tag-Beschränkungen und -Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Maximale Schlüssellänge — 127 Unicode-Zeichen in UTF -8
- Maximale Wertlänge — 255 Unicode-Zeichen in UTF -8
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Verwenden Sie das `"aws:"` Präfix nicht in Ihren Tagnamen oder -Werten, da es für die AWS Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht zum Limit für Tags pro Ressource gezählt.
- Wenn Ihr Markierungsschema für mehrere -Services und -Ressourcen verwendet wird, denken Sie daran, dass andere Services möglicherweise Einschränkungen für zulässige Zeichen haben. Im Allgemeinen sind folgende Zeichen zulässig: Buchstaben, Leerzeichen und Zahlen, die in UTF -8 dargestellt werden können, sowie die folgenden Sonderzeichen: + - =. _:/@.

Verwenden von Tags mit IAM-Richtlinien

In den IAM Richtlinien, die Sie für Aktionen verwenden, können Sie tagbasierte Berechtigungen auf Ressourcenebene anwenden. AWS IoT Events API Dies ermöglicht Ihnen eine bessere Kontrolle darüber, welche Ressourcen ein Benutzer erstellen, ändern oder verwenden kann.

Sie verwenden das `Condition` Element (auch `Condition` Block genannt) mit den folgenden Bedingungskontextschlüsseln und Werten in einer IAM Richtlinie, um den Benutzerzugriff (Berechtigungen) auf der Grundlage der Tags einer Ressource zu steuern:

- Verwenden Sie `aws:ResourceTag/<tag-key>: <tag-value>`, um Benutzeraktionen für Ressourcen mit bestimmten Tags zuzulassen oder zu verweigern.
- Verwenden Sie diese Option, `aws:RequestTag/<tag-key>: <tag-value>` um zu verlangen, dass ein bestimmtes Tag verwendet (oder nicht verwendet) wird, wenn Sie eine API Anfrage zum Erstellen oder Ändern einer Ressource stellen, die Tags zulässt.
- Wird verwendet, `aws:TagKeys: [<tag-key>, ...]` um zu verlangen, dass ein bestimmter Satz von Tag-Schlüsseln verwendet (oder nicht verwendet) wird, wenn eine API Anfrage zur Erstellung oder Änderung einer Ressource gestellt wird, die Tags zulässt.

> **Note**
>
> Die Bedingungskontextschlüssel und -werte in einer IAM Richtlinie gelten nur für AWS IoT Events Aktionen, bei denen ein Bezeichner für eine Ressource, die markiert werden kann, ein erforderlicher Parameter ist.

Im AWS Identity and Access Management Benutzerhandbuch finden Sie zusätzliche Informationen zur Verwendung von Tags zur Steuerung des Zugriffs mithilfe von Tags. Der Abschnitt mit den IAMJSONRichtlinienreferenzen dieses Handbuchs enthält ausführliche Syntax, Beschreibungen und Beispiele der Elemente, Variablen und Bewertungslogik von JSON Richtlinien inIAM.

Die folgende Beispielrichtlinie wendet zwei auf Tags basierende Einschränkungen an. Ein Benutzer, der durch diese Richtlinie eingeschränkt ist:

- Kann keiner Ressource den Tag „env = prod“ zuweisen (im Beispiel vgl. die Zeile `"aws:RequestTag/env" : "prod"`
- Kann keine Ressource modifizieren oder darauf zugreifen, die den Tag „env=prod“ aufweist (im Beispiel vgl. die Zeile `"aws:ResourceTag/env" : "prod"`).

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

```
            "Effect": "Deny",
            "Action": [
                "iotevents:CreateDetectorModel",
                "iotevents:CreateAlarmModel",
                "iotevents:CreateInput",
                "iotevents:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/env": "prod"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "iotevents:DescribeDetectorModel",
                "iotevents:DescribeAlarmModel",
                "iotevents:UpdateDetectorModel",
                "iotevents:UpdateAlarmModel",
                "iotevents:DeleteDetectorModel",
                "iotevents:DeleteAlarmModel",
                "iotevents:ListDetectorModelVersions",
                "iotevents:ListAlarmModelVersions",
                "iotevents:UpdateInput",
                "iotevents:DescribeInput",
                "iotevents:DeleteInput",
                "iotevents:ListTagsForResource",
                "iotevents:TagResource",
                "iotevents:UntagResource",
                "iotevents:UpdateInputRouting"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/env": "prod"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:*"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können auch mehrere Tag-Werte für einen bestimmten Tag-Schlüssel angeben, indem Sie sie wie folgt in eine Liste einschließen.

```
            "StringEquals" : {
              "aws:ResourceTag/env" : ["dev", "test"]
            }
```

> **Note**
>
> Wenn Sie Benutzern den Zugriff zu Ressourcen auf der Grundlage von Tags (Markierungen) gewähren oder verweigern, müssen Sie daran denken, Benutzern explizit das Hinzufügen und Entfernen dieser Tags (Markierungen) von den jeweiligen Ressourcen unmöglich zu machen. Andernfalls können Benutzer möglicherweise Ihre Einschränkungen umgehen und sich Zugriff auf eine Ressource verschaffen, indem sie ihre Tags (Markierungen) modifizieren.

Problembehebung AWS IoT Events

Diese Anleitung zur Fehlerbehebung bietet Lösungen für häufig auftretende Probleme, die bei der Verwendung auftreten können AWS IoT Events. Lesen Sie die Themen, um Probleme bei der Erkennung von Ereignissen, beim Zugriff auf Daten, Berechtigungen, Serviceintegrationen, Gerätekonfigurationen und mehr zu identifizieren und zu lösen. Dieses Handbuch enthält Hinweise zur Fehlerbehebung für die AWS IoT Events Konsole,API,CLI, Fehler, Latenz und Integrationen. Es soll Ihnen helfen, Ihre Probleme schnell zu lösen, damit Sie zuverlässige und skalierbare ereignisgesteuerte Anwendungen erstellen können.

Themen

Allgemeine AWS IoT Events Probleme und Lösungen

Im folgenden Abschnitt finden Sie Informationen zur Behebung von Fehlern und möglichen Lösungen zur Behebung von Problemen mit AWS IoT Events.

Fehler

Fehler bei der Erstellung des Detektormodells

Ich erhalte Fehler, wenn ich versuche, ein Detektormodell zu erstellen.

Lösung

Wenn Sie ein Detektormodell erstellen, müssen Sie die folgenden Einschränkungen berücksichtigen.

- In jedem `action` Feld ist nur eine Aktion zulässig.
- Das `condition` ist erforderlich für`transitionEvents`. Es ist optional für `OnEnter``OnInput`, und `OnExit` Ereignisse.
- Wenn das `condition` Feld leer ist, entspricht das ausgewertete Ergebnis des Bedingungsausdruck`true`.
- Das ausgewertete Ergebnis des Bedingungsausdrucks sollte ein boolescher Wert sein. Wenn das Ergebnis kein boolescher Wert ist, entspricht es dem `actions` im Ereignis `nextState` angegebenen Wert `false` und löst diesen nicht aus.

Weitere Informationen finden Sie unter Einschränkungen und Einschränkungen des Detektormodells.

Aktualisierungen aus einem gelöschten Meldermodell

Ich habe vor ein paar Minuten ein Meldermodell aktualisiert oder gelöscht, erhalte aber immer noch Statusaktualisierungen vom alten Meldermodell in Form von MQTT Meldungen oder SNS Warnmeldungen.

Lösung

Wenn Sie ein Meldermodell aktualisieren, löschen oder neu erstellen (siehe UpdateDetectorModel), kommt es zu einer gewissen Verzögerung, bis alle Melderinstanzen gelöscht werden und das neue Modell verwendet wird. Während dieser Zeit werden Eingaben möglicherweise weiterhin von den Instanzen der vorherigen Version des Detektormodells verarbeitet. Möglicherweise erhalten Sie weiterhin Warnmeldungen, die durch das vorherige Meldermodell definiert wurden. Warten Sie mindestens sieben Minuten, bevor Sie das Update erneut überprüfen oder einen Fehler melden.

Fehler beim Auslösen einer Aktion (wenn eine Bedingung erfüllt ist)

Der Detektor kann keine Aktion auslösen oder in einen neuen Zustand übergehen, wenn die Bedingung erfüllt ist.

Lösung

Stellen Sie sicher, dass das ausgewertete Ergebnis des bedingten Ausdrucks des Detektors ein boolescher Wert ist. Wenn das Ergebnis kein boolescher Wert ist, entspricht es dem `action` im Ereignis `nextState` angegebenen Wert `false` und löst diesen nicht aus. Weitere Informationen finden Sie unter Syntax für bedingte Ausdrücke.

Fehler beim Auslösen einer Aktion (bei Überschreitung eines Schwellenwerts)

Der Detektor löst keine Aktion oder keinen Ereignisübergang aus, wenn die Variable in einem bedingten Ausdruck einen bestimmten Wert erreicht.

Lösung

Wenn Sie `setVariable` für`onInput`, `onEnter` oder aktualisieren`onExit`, wird der neue Wert bei der Auswertung `condition` während des aktuellen Verarbeitungszyklus nicht verwendet. Stattdessen wird der ursprüngliche Wert verwendet, bis der aktuelle Zyklus abgeschlossen ist. Sie können dieses Verhalten ändern, indem Sie den `evaluationMethod` Parameter in der Definition des Detektormodells festlegen. Wenn auf gesetzt `evaluationMethod` ist`SERIAL`, werden Variablen aktualisiert und die Ereignisbedingungen in der Reihenfolge ausgewertet, in der die Ereignisse definiert sind. Wenn auf gesetzt `evaluationMethod` ist `BATCH` (Standardeinstellung), werden Variablen aktualisiert und Ereignisse erst ausgeführt, nachdem alle Ereignisbedingungen ausgewertet wurden.

Falsche Verwendung des Status

Der Detektor wechselt in den falschen Status, wenn ich versuche, Nachrichten an Eingänge zu senden, indem `BatchPutMessage` ich

Lösung

Wenn Sie früher BatchPutMessagemehrere Nachrichten an Eingänge senden, ist die Reihenfolge, in der die Nachrichten oder Eingaben verarbeitet werden, nicht garantiert. Um die Bestellung zu garantieren, senden Sie Nachrichten nacheinander und warten Sie jedes Mal`BatchPutMessage`, bis Sie den Erfolg bestätigen.

Verbindungsnachricht

Ich erhalte eine `('Connection aborted.', error(54, 'Connection reset by peer'))` Fehlermeldung, wenn ich versuche, eine API anzurufen oder aufzurufen.

Lösung

Stellen Sie sicher, dass Open TLS 1.1 oder eine neuere Version SSL verwendet, um die Verbindung herzustellen. Dies sollte unter den meisten Linux-Distributionen oder Windows Version 7 und höher die Standardeinstellung sein. Benutzer von macOS müssen möglicherweise Open aktualisierenSSL.

InvalidRequestException Nachricht

Ich erhalte InvalidRequestException , wenn ich versuche anzurufen `CreateDetectorModel` und `UpdateDetectorModel`APIs.

Lösung

Überprüfen Sie Folgendes, um das Problem zu lösen. Weitere Informationen finden Sie unter CreateDetectorModelund UpdateDetectorModel.

- Stellen Sie sicher, dass Sie nicht beide `seconds` und `durationExpression` als Parameter von `SetTimerAction` gleichzeitig verwenden.
- Stellen Sie sicher, dass Ihr Zeichenkettenausdruck für gültig `durationExpression` ist. Der Zeichenkettenausdruck kann Zahlen, Variablen (`$variable.<variable-name>`) oder Eingabewerte (`$input.<input-name>.<path-to-datum>`) enthalten.

Amazon CloudWatch **`action.setTimer`** Logs-Fehler

Sie können Amazon CloudWatch Logs einrichten, um AWS IoT Events Detector-Modell-Instances zu überwachen. Im Folgenden sind die häufigsten Fehler aufgeführt AWS IoT Events, die bei der Verwendung von generiert `action.setTimer` werden.

- Fehler: Ihr Dauerausdruck für den angegebenen Timer *`<timer-name>`* konnte nicht zu einer Zahl ausgewertet werden.

Lösung

Stellen Sie sicher, dass Ihr Zeichenkettenausdruck für in eine Zahl umgewandelt werden `durationExpression` kann. Andere Datentypen, wie z. B. Boolean, sind nicht zulässig.

- Fehler: Das ausgewertete Ergebnis Ihres Dauerausdrucks für den angegebenen Timer *<timer-name>* ist größer als 31622440. Um die Genauigkeit zu gewährleisten, stellen Sie sicher, dass sich Ihr Ausdruck für die Dauer auf einen Wert zwischen 60 und 31622400 bezieht.

Lösung

Stellen Sie sicher, dass die Dauer Ihres Timers mindestens 31622400 Sekunden beträgt. Das ausgewertete Ergebnis der Dauer wird auf die nächste ganze Zahl abgerundet.

- Fehler: Das ausgewertete Ergebnis Ihres Ausdrucks für die Dauer für den angegebenen Timer *<timer-name>* ist kleiner als 60. Um die Genauigkeit zu gewährleisten, stellen Sie sicher, dass sich Ihr Ausdruck für die Dauer auf einen Wert zwischen 60-31622400 bezieht.

Lösung

Stellen Sie sicher, dass die Dauer Ihres Timers mindestens 60 Sekunden beträgt. Das ausgewertete Ergebnis der Dauer wird auf die nächste ganze Zahl abgerundet.

- Fehler: Ihr Dauerausdruck für den genannten Timer *<timer-name>* konnte nicht ausgewertet werden. Überprüfen Sie die Variablennamen, Eingabenamen und Pfade zu den Daten, um sicherzustellen, dass Sie auf die vorhandenen Variablen und Eingaben verweisen.

Lösung

Stellen Sie sicher, dass sich Ihr Zeichenkettenausdruck auf die vorhandenen Variablen und Eingaben bezieht. Der Zeichenkettenausdruck kann Zahlen, Variablen (`$variable.`*variable-name*) und Eingabewerte (`$input.`*input-name*`.`*path-to-datum*) enthalten.

- Fehler: Der angegebene Timer konnte nicht festgelegt `<timer-name>` werden. Überprüfen Sie den Ausdruck für die Dauer, und versuchen Sie es erneut.

Lösung

Sehen Sie sich die SetTimerActionAktion an, um sicherzustellen, dass Sie die richtigen Parameter angegeben haben, und stellen Sie dann den Timer erneut ein.

Weitere Informationen finden Sie unter CloudWatch Amazon-Protokollierung bei der Entwicklung von AWS IoT Events Meldermodellen aktivieren.

CloudWatch Amazon-Payload-Fehler

Sie können Amazon CloudWatch Logs einrichten, um AWS IoT Events Detector-Modell-Instances zu überwachen. Im Folgenden finden Sie häufig auftretende Fehler und Warnungen AWS IoT Events, die bei der Konfiguration der Aktions-Payload generiert werden.

- Fehler: Wir konnten Ihren Ausdruck für die Aktion nicht auswerten. Stellen Sie sicher, dass sich die Variablennamen, Eingabenamen und Pfade zu den Daten auf die vorhandenen Variablen und Eingabewerte beziehen. Stellen Sie außerdem sicher, dass die Größe der Payload weniger als 1 KB beträgt, was der maximal zulässigen Größe einer Payload entspricht.

  Lösung

  Stellen Sie sicher, dass Sie die richtigen Variablennamen, Eingabenamen und Pfade zu den Daten eingeben. Möglicherweise erhalten Sie diese Fehlermeldung auch, wenn die Aktionsnutzlast größer als 1 KB ist.

- Fehler: Wir konnten Ihren Inhaltsausdruck nicht nach der Payload von analysieren. *<action-type>* Geben Sie einen Inhaltsausdruck mit der richtigen Syntax ein.

  Lösung

  Der Inhaltsausdruck kann Zeichenfolgen (`'`*`string`*`'`), Variablen (`$variable.`*`variable-name`*), Eingabewerte (`$input.`*`input-name`*`.`*`path-to-datum`*), Zeichenkettenverkettungen und Zeichenfolgen enthalten, die Folgendes enthalten: `${}`

- Fehler: Ihr Nutzdatenausdruck {*expression*} ist nicht gültig. Der definierte Payload-Typ istJSON, Sie müssen also einen Ausdruck angeben, der eine Zeichenfolge ergeben AWS IoT Events würde.

  Lösung

  Wenn der angegebene Payload-Typ istJSON, wird AWS IoT Events zunächst geprüft, ob der Dienst Ihren Ausdruck als Zeichenfolge auswerten kann. Das ausgewertete Ergebnis darf weder ein boolescher Wert noch eine Zahl sein. Wenn die Überprüfung fehlschlägt, erhalten Sie möglicherweise diesen Fehler.

- Warnung: Die Aktion wurde ausgeführt, aber wir konnten Ihren Inhaltsausdruck nicht dahingehend auswerten, dass die Aktionsnutzlast gültig istJSON. Der definierte Payload-Typ ist. JSON

Lösung

Stellen Sie sicher, dass Ihr Inhaltsausdruck für die Aktions-Payload als gültig bewertet werden AWS IoT Events kannJSON, wenn Sie den Payload-Typ als definieren. `JSON` AWS IoT Events führt die Aktion aus, auch wenn der Inhaltsausdruck nicht als gültig bewertet werden AWS IoT Events kann. JSON

Weitere Informationen finden Sie unter CloudWatch Amazon-Protokollierung bei der Entwicklung von AWS IoT Events Meldermodellen aktivieren.

Inkompatible Datentypen

Meldung: `<reference>` Im folgenden Ausdruck wurden inkompatible Datentypen [`<inferred-types>`] gefunden: `<expression>`

Lösung

Dieser Fehler kann aus einem der folgenden Gründe auftreten:

- Die ausgewerteten Ergebnisse Ihrer Verweise sind nicht mit anderen Operanden in Ihren Ausdrücken kompatibel.
- Der Typ des an eine Funktion übergebenen Arguments wird nicht unterstützt.

Wenn Sie Verweise in Ausdrücken verwenden, überprüfen Sie Folgendes:

- Wenn Sie eine Referenz als Operanden mit einem oder mehreren Operatoren verwenden, stellen Sie sicher, dass alle Datentypen, auf die Sie verweisen, kompatibel sind.

  Im folgenden Ausdruck 2 ist Integer beispielsweise ein Operand sowohl der == Operatoren als auch. && Um sicherzustellen, dass die Operanden kompatibel sind `$variable.testVariable + 1` und auf eine Ganzzahl oder Dezimalzahl verweisen `$variable.testVariable` müssen.

  Außerdem 1 ist Integer ein Operand des Operators+. `$variable.testVariable`Muss daher auf eine Ganzzahl oder Dezimalzahl verweisen.

  ```
  '$variable.testVariable + 1 == 2 && $variable.testVariable'
  ```

- Wenn Sie eine Referenz als Argument verwenden, das an eine Funktion übergeben wird, stellen Sie sicher, dass die Funktion die Datentypen unterstützt, auf die Sie verweisen.

Für die folgende `timeout("time-name")` Funktion ist beispielsweise eine Zeichenfolge mit doppelten Anführungszeichen als Argument erforderlich. Wenn Sie eine Referenz für die verwenden *`timer-name`* Wert, Sie müssen auf eine Zeichenfolge mit doppelten Anführungszeichen verweisen.

```
timeout("timer-name")
```

> **Note**
>
> Für die `convert(type, expression)` Funktion, wenn Sie eine Referenz für die verwenden *`type`* Wert, das ausgewertete Ergebnis Ihrer Referenz muss `StringDecimal`, oder sein`Boolean`.

Weitere Informationen finden Sie unter Referenz für Eingaben und Variablen in Ausdrücken.

Nachricht konnte nicht gesendet werden an AWS IoT Events

Nachricht: Nachricht konnte nicht an Iot Events gesendet werden

Lösung

Dieser Fehler kann aus den folgenden Gründen auftreten:

- Die Nutzlast der Eingabenachricht enthält nicht die`Input attribute Key`.
- Der `Input attribute Key` befindet sich nicht in demselben JSON Pfad wie in der Eingabedefinition angegeben.
- Die Eingabenachricht entspricht nicht dem Schema, wie es in der AWS IoT Events Eingabe definiert ist.

> **Note**
>
> Bei der Datenaufnahme von anderen Diensten wird es ebenfalls zu einem Fehler kommen.

Example

Beispielsweise schlägt die AWS IoT Core AWS IoT Regel mit der folgenden Meldung fehl `Verify the Input Attribute key.`

Um dieses Problem zu lösen, stellen Sie sicher, dass das Eingabe-Payload-Nachrichtenschema der AWS IoT Events Eingabedefinition entspricht und der `Input attribute Key` Speicherort übereinstimmt. Weitere Informationen finden Sie unter, Erstellen Sie eine Eingabe für Modelle um zu erfahren, wie Sie Eingaben definieren AWS IoT Events .

Fehlerbehebung bei einem Detektormodell durch Ausführen von Analysen

AWS IoT Events kann Ihr Detektormodell analysieren und Analyseergebnisse generieren, ohne Eingabedaten an Ihr Detektormodell zu senden. AWS IoT Events führt eine Reihe von Analysen durch, die in diesem Abschnitt beschrieben werden, um Ihr Detektormodell zu überprüfen. Diese erweiterte Lösung zur Fehlerbehebung fasst auch Diagnoseinformationen zusammen, einschließlich Schweregrad und Lokalisation, sodass Sie potenzielle Probleme in Ihrem Meldermodell schnell finden und beheben können. Weitere Informationen zu Diagnosefehlertypen und Meldungen für Ihr Meldermodell finden Sie unterAnalyse und Diagnoseinformationen zu Detektormodellen.

Sie können die AWS IoT Events Konsole, API, AWS Command Line Interface (AWS CLI) oder verwenden, AWS SDKum diagnostische Fehlermeldungen aus der Analyse Ihres Meldermodells anzuzeigen.

> **Note**
>
> - Sie müssen alle Fehler beheben, bevor Sie Ihr Detektormodell veröffentlichen können.
> - Wir empfehlen Ihnen, die Warnungen zu lesen und die erforderlichen Maßnahmen zu ergreifen, bevor Sie Ihr Detektormodell in Produktionsumgebungen verwenden. Andernfalls funktioniert das Meldermodell möglicherweise nicht wie erwartet.
> - Sie können bis zu 10 Analysen gleichzeitig im `RUNNING` Status haben.

Informationen zur Analyse Ihres Detektormodells finden Sie unter Analysieren eines Detektormodells (Konsole) oderAnalysieren eines Detektormodells (AWS CLI).

Themen

Analyse und Diagnoseinformationen zu Detektormodellen

Bei Analysen von Detektormodellen werden die folgenden Diagnoseinformationen gesammelt:

- Stufe — Der Schweregrad des Analyseergebnisses. Basierend auf dem Schweregrad lassen sich die Analyseergebnisse in drei allgemeine Kategorien einteilen:
  - Information (`INFO`) — Ein Informationsergebnis gibt Aufschluss über ein bedeutendes Feld in Ihrem Detektormodell. Für diese Art von Ergebnis sind in der Regel keine sofortigen Maßnahmen erforderlich.
  - Warnung (`WARNING`) — Ein Warnungsergebnis lenkt besondere Aufmerksamkeit auf Felder, die Probleme mit Ihrem Meldermodell verursachen könnten. Wir empfehlen Ihnen, die Warnungen zu lesen und die erforderlichen Maßnahmen zu ergreifen, bevor Sie Ihr Meldermodell in Produktionsumgebungen verwenden. Andernfalls funktioniert das Meldermodell möglicherweise nicht wie erwartet.
  - Fehler (`ERROR`) — Ein Fehlerergebnis informiert Sie über ein Problem in Ihrem Detektormodell. AWS IoT Events führt diesen Satz von Analysen automatisch durch, wenn Sie versuchen, das Detektormodell zu veröffentlichen. Sie müssen alle Fehler beheben, bevor Sie das Detektormodell veröffentlichen können.
- Position — Enthält Informationen, anhand derer Sie das Feld in Ihrem Detektormodell lokalisieren können, auf das sich das Analyseergebnis bezieht. Ein Standort umfasst in der Regel den Namen des Status, den Namen des Übergangsereignisses, den Namen des Ereignisses und den Ausdruck (z. B.`in state TemperatureCheck in onEnter in event Init in action setVariable`).
- Typ — Der Typ des Analyseergebnisses. Analysetypen lassen sich in die folgenden Kategorien einteilen:
  - `supported-actions`— AWS IoT Events kann Aktionen aufrufen, wenn ein bestimmtes Ereignis oder ein Übergangsereignis erkannt wird. Sie können integrierte Aktionen definieren, um einen Timer zu verwenden oder eine Variable festzulegen oder Daten an andere AWS Dienste zu senden. Sie müssen Aktionen angeben, die mit anderen AWS Diensten in einer AWS Region funktionieren, in der die AWS Dienste verfügbar sind.

- `service-limits`— Dienstkontingente, auch Limits genannt, sind die maximale oder minimale Anzahl von Serviceressourcen oder Vorgängen für Ihr AWS Konto. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Je nach Ihren Geschäftsanforderungen können Sie Ihr Meldermodell aktualisieren, um Grenzwerte zu vermeiden, oder eine Erhöhung des Kontingents beantragen. Sie können für einige Kontingente eine Erhöhung beantragen, während andere Kontingente nicht erhöht werden können. Weitere Informationen finden Sie unter Kontingente.

- **`structure`**— Das Detektormodell muss alle erforderlichen Komponenten wie Zustände enthalten und einer Struktur folgen, die dies AWS IoT Events unterstützt. Ein Detektormodell muss mindestens einen Zustand und eine Bedingung haben, die die eingehenden Eingabedaten auswertet, um signifikante Ereignisse zu erkennen. Wenn ein Ereignis erkannt wird, wechselt das Detektormodell in den nächsten Status und kann Aktionen auslösen. Diese Ereignisse werden als Übergangsereignisse bezeichnet. Ein Übergangsereignis muss den nächsten Status anweisen, in den Status einzutreten.

- **`expression-syntax`**— AWS IoT Events bietet mehrere Möglichkeiten, Werte anzugeben, wenn Sie Detektormodelle erstellen und aktualisieren. Sie können Literale, Operatoren, Funktionen, Referenzen und Substitutionsvorlagen in den Ausdrücken verwenden. Sie können Ausdrücke verwenden, um Literalwerte anzugeben, oder Sie AWS IoT Events können die Ausdrücke auswerten, bevor Sie bestimmte Werte angeben. Ihr Ausdruck muss der erforderlichen Syntax entsprechen. Weitere Informationen finden Sie unter Ausdrücke zum Filtern, Transformieren und Verarbeiten von Ereignisdaten.

  Detector Model-Ausdrücke in AWS IoT Events können auf bestimmte Daten oder eine Ressource verweisen.

  - **`data-type`**— AWS IoT Events unterstützt Integer-, Dezimal-, String- und Boolesche Datentypen. Wenn die Daten eines Datentyps bei der Auswertung von Ausdrücken automatisch in einen anderen konvertiert werden AWS IoT Events können, sind diese Datentypen kompatibel.

    > **Note**
    >
    > - Integer und Decimal sind die einzigen kompatiblen Datentypen, die von unterstützt werden AWS IoT Events.
    > - AWS IoT Events kann keine arithmetischen Ausdrücke auswerten, da eine Ganzzahl nicht in eine Zeichenfolge konvertiert werden AWS IoT Events kann.

- **`referenced-data`**— Sie müssen die Daten definieren, auf die in Ihrem Detektormodell verwiesen wird, bevor Sie die Daten verwenden können. Wenn Sie beispielsweise Daten an eine DynamoDB-Tabelle senden möchten, müssen Sie eine Variable definieren, die auf den Tabellennamen verweist, bevor Sie die Variable in einem Ausdruck () `$variable.TableName` verwenden können.
- **`referenced-resource`**— Ressourcen, die das Detektormodell verwendet, müssen verfügbar sein. Sie müssen Ressourcen definieren, bevor Sie sie verwenden können. Sie möchten beispielsweise ein Detektormodell zur Überwachung der Temperatur eines Gewächshauses erstellen. Sie müssen eine Eingabe (`$input.TemperatureInput`) definieren, um eingehende Temperaturdaten an Ihr Meldermodell weiterzuleiten, bevor Sie `$input.TemperatureInput.sensorData.temperature` die Temperatur als Referenz verwenden können.

Im folgenden Abschnitt finden Sie Informationen zur Behebung von Fehlern und zur Suche nach möglichen Lösungen anhand der Analyse Ihres Detektormodells.

Beheben Sie Fehler im Detektormodell

Die oben beschriebenen Fehlertypen liefern Diagnoseinformationen zu einem Detektormodell und entsprechen Meldungen, die Sie möglicherweise abrufen. Verwenden Sie diese Meldungen und Lösungsvorschläge, um Fehler mit Ihrem Meldermodell zu beheben.

Nachrichten und Lösungen

- Location
- supported-actions
- service-limits
- structure
- expression-syntax
- data-type
- referenced-data
- referenced-resource

`Location`

Ein Analyseergebnis mit Informationen über`Location`, entspricht der folgenden Fehlermeldung:

- Meldung — Enthält zusätzliche Informationen zum Analyseergebnis. Dies kann eine Information, Warnung oder Fehlermeldung sein.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie eine Aktion angegeben haben, die AWS IoT Events derzeit nicht unterstützt wird. Eine Liste der unterstützten Aktionen finden Sie unterUnterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen.

`supported-actions`

Ein Analyseergebnis mit Informationen über`supported-actions`, entspricht den folgenden Fehlermeldungen:

- Meldung: Ungültiger Aktionstyp in der Aktionsdefinition vorhanden: *`action-definition`*.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie eine Aktion angegeben haben, die AWS IoT Events derzeit nicht unterstützt wird. Eine Liste der unterstützten Aktionen finden Sie unterUnterstützte Aktionen zum Empfangen von Daten und Auslösen von Aktionen.
- Meldung: Die DetectorModel Definition hat eine *`aws-Dienst`* Aktion, aber die *`AWS-Service`* Der Dienst wird in der Region nicht unterstützt *`region-name`*.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn die von Ihnen angegebene Aktion von unterstützt wird AWS IoT Events, die Aktion jedoch in Ihrer aktuellen Region nicht verfügbar ist. Dies kann auftreten, wenn Sie versuchen, Daten an einen AWS Dienst zu senden, der in der Region nicht verfügbar ist. Sie müssen außerdem dieselbe Region für beide AWS IoT Events und die AWS Dienste, die Sie verwenden, auswählen.

`service-limits`

Ein Analyseergebnis mit Informationen über`service-limits`, entspricht den folgenden Fehlermeldungen:

- Meldung: Der in der Nutzlast zulässige Inhaltsausdruck hat das Limit überschritten *`content-expression-size`* Byte im Ereignis *`event-name`* im Bundesstaat *`state-name`*.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn der Inhaltsausdruck für Ihre Aktionsnutzlast größer als 1024 Byte ist. Die Größe des Inhaltsausdrucks für eine Payload kann bis zu 1024 Byte betragen.

- Meldung: Die Anzahl der in der Definition des Detektormodells zulässigen Zustände hat den Grenzwert überschritten *states-per-detector-model*.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Ihr Detektormodell mehr als 20 Zustände hat. Ein Detektormodell kann bis zu 20 Zustände haben.

- Meldung: Die Dauer des Timers *timer-name* sollte mindestens sein *minimum-timer-duration* Sekunden lang.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn die Dauer Ihres Timers weniger als 60 Sekunden beträgt. Wir empfehlen, dass die Dauer eines Timers zwischen 60 und 31622400 Sekunden liegt. Wenn Sie einen Ausdruck für die Dauer Ihres Timers angeben, wird das ausgewertete Ergebnis des Dauerausdrucks auf die nächste ganze Zahl abgerundet.

- Meldung: Die Anzahl der pro Ereignis zulässigen Aktionen hat den Grenzwert überschritten *actions-per-event* in der Definition des Detektormodells

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn das Ereignis mehr als 10 Aktionen umfasst. Sie können bis zu 10 Aktionen für jedes Ereignis in Ihrem Meldermodell einrichten.

- Meldung: Die Anzahl der pro Status zulässigen Übergangsereignisse hat den Grenzwert überschritten *transition-events-per-state* in der Definition des Detektormodells.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn der Status mehr als 20 Übergangsereignisse hat. Sie können bis zu 20 Übergangsereignisse für jeden Status in Ihrem Detektormodell haben.

- Meldung: Die Anzahl der pro Status zulässigen Ereignisse hat den Grenzwert überschritten *events-per-state* in der Definition des Detektormodells

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn der Status mehr als 20 Ereignisse enthält. Sie können bis zu 20 Ereignisse für jeden Status in Ihrem Detektormodell haben.

- Meldung: Die maximale Anzahl von Meldermodellen, die einem einzelnen Eingang zugeordnet werden können, hat möglicherweise den Grenzwert erreicht. Eingabe *input-name* wird verwendet in *detector-models-per-input* Detektor modelliert Routen.

  Lösung: Möglicherweise erhalten Sie diese Warnmeldung, wenn Sie versuchen, eine Eingabe an mehr als 10 Detektormodelle weiterzuleiten. Einem einzelnen Detektormodell können bis zu 10 verschiedene Detektormodelle zugeordnet werden.

`structure`

Ein Analyseergebnis mit Informationen über`structure`, entspricht den folgenden Fehlermeldungen:

- Meldung: Für Aktionen ist möglicherweise nur ein Typ definiert, aber es wurde eine Aktion gefunden mit *`number-of-types`* Typen. Bitte teilen Sie es in separate Aktionen auf.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie zwei oder mehr Aktionen in einem einzigen Feld angegeben haben, indem Sie API Operationen zum Erstellen oder Aktualisieren Ihres Meldermodells verwendet haben. Sie können eine Reihe von `Action` Objekten definieren. Stellen Sie sicher, dass Sie jede Aktion als separates Objekt definieren.
- Nachricht: Die TransitionEvent *`transition-event-name`* Übergänge in einen nicht existierenden Zustand *`state-name`*.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie den nächsten Status, auf den Ihr Übergangsereignis verwiesen hat, nicht finden AWS IoT Events konnten. Stellen Sie sicher, dass der nächste Status definiert ist und dass Sie den richtigen Statusnamen eingegeben haben.
- Meldung: Der DetectorModelDefinition hatte einen gemeinsamen Statusnamen: Zustand gefunden *`state-name`* mit *`number-of-states`* Wiederholungen.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie denselben Namen für einen oder mehrere Bundesstaaten verwenden. Stellen Sie sicher, dass Sie jedem Status in Ihrem Meldermodell einen eindeutigen Namen geben. Der Name des Bundesstaates muss 1-128 Zeichen lang sein. Gültige Zeichen: a-z, A-Z, 0-9, _ (Unterstrich) und - (Bindestrich).
- Nachricht: Die Definition initialStateName *`initial-state-name`* entsprach keinem definierten Bundesstaat.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn der ursprüngliche Statusname falsch ist. Das Detektormodell bleibt im Anfangszustand (Start), bis eine Eingabe eintrifft. Sobald eine Eingabe eintrifft, geht das Detektormodell sofort in den nächsten Zustand über. Stellen Sie sicher, dass der ursprüngliche Statusname der Name eines definierten Zustands ist und dass Sie den richtigen Namen eingeben.
- Meldung: Die Definition des Detektormodells muss mindestens eine Eingabe in einer Bedingung verwenden.

  Lösung: Dieser Fehler wird möglicherweise angezeigt, wenn Sie in einer Bedingung keine Eingabe angegeben haben. Sie müssen mindestens eine Eingabe in mindestens einer Bedingung verwenden. Andernfalls werden eingehende Daten AWS IoT Events nicht ausgewertet.

- Nachricht: Nur eine von Sekunden und durationExpression kann eingegeben werden SetTimer.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie `seconds` sowohl als auch `durationExpression` für Ihren Timer verwendet haben. Stellen Sie sicher, dass Sie entweder `seconds` oder `durationExpression` als Parameter von verwenden`SetTimerAction`. Weitere Informationen finden Sie SetTimerActionin der AWS IoT Events APIReferenz.

- Meldung: Eine Aktion in Ihrem Meldermodell ist nicht erreichbar. Überprüfen Sie den Zustand, der die Aktion auslöst.

  Lösung: Wenn eine Aktion in Ihrem Meldermodell nicht erreichbar ist, wird der Zustand des Ereignisses als falsch bewertet. Überprüfen Sie die Bedingung des Ereignisses, das die Aktion enthält, um sicherzustellen, dass sie als wahr ausgewertet wird. Wenn die Bedingung des Ereignisses als wahr ausgewertet wird, sollte die Aktion erreichbar sein.

- Meldung: Ein Eingabeattribut wird gelesen, dies kann jedoch durch den Ablauf eines Timers verursacht werden.

  Lösung: Der Wert eines Eingabeattributs kann gelesen werden, wenn einer der folgenden Fälle eintritt:

  - Ein neuer Eingabewert wurde empfangen.
  - Wenn ein Timer im Melder abgelaufen ist.

  Um sicherzustellen, dass ein Eingabeattribut nur ausgewertet wird, wenn der neue Wert für diese Eingabe empfangen wird, fügen Sie einen `triggerType(“Message”)` Funktionsaufruf wie folgt in Ihre Bedingung ein:

  Der ursprüngliche Zustand wird im Detektormodell ausgewertet:

  ```
  if ($input.HeartBeat.status == “OFFLINE”)
  ```

  würde dem Folgenden ähnlich werden:

  ```
  if ( triggerType("MESSAGE") &&  $input.HeartBeat.status == “OFFLINE”)
  ```

  wobei ein Aufruf der `triggerType(“Message”)` Funktion vor der in der Bedingung angegebenen ersten Eingabe erfolgt. Bei Verwendung dieser Technik ergibt die `triggerType("Message")` Funktion den Wert true und erfüllt die Bedingung, dass ein neuer

Eingabewert empfangen wird. Weitere Informationen zur Verwendung der `triggerType` Funktion finden Sie `triggerType` im Abschnitt Ausdrücke im AWS IoT Events Entwicklerhandbuch

- Meldung: Ein Status in Ihrem Detektormodell ist nicht erreichbar. Überprüfen Sie den Zustand, der zu einem Übergang in den gewünschten Zustand führen wird.

  Lösung: Wenn ein Zustand in Ihrem Detektormodell nicht erreichbar ist, wird eine Bedingung, die zu einem eingehenden Übergang in diesen Zustand führt, als falsch bewertet. Prüfen Sie, ob die Bedingungen für eingehende Übergänge in diesen unerreichbaren Zustand in Ihrem Detektormodell als wahr ausgewertet werden, sodass der gewünschte Zustand erreichbar werden kann.

- Nachricht: Ein ablaufender Timer kann dazu führen, dass eine unerwartete Anzahl von Nachrichten gesendet wird.

  Lösung: Um zu verhindern, dass Ihr Meldermodell in einen unendlichen Zustand übergeht und eine unerwartete Anzahl von Nachrichten sendet, weil ein Timer abgelaufen ist, sollten Sie einen `triggerType("Message")` Funktionsaufruf unter den folgenden Bedingungen Ihres Meldermodells in Betracht ziehen:

  Der ursprüngliche Zustand wird im Meldermodell bewertet:

  ```
  if (timeout("awake"))
  ```

  würde in einen Zustand umgewandelt werden, der dem folgenden ähnelt:

  ```
  if (triggerType("MESSAGE") && timeout("awake"))
  ```

  wobei ein Aufruf der `triggerType(“Message”)` Funktion vor der ersten Eingabe erfolgt, die in der Bedingung bereitgestellt wird.

  Diese Änderung verhindert, dass Timer-Aktionen in Ihrem Detektor ausgelöst werden, wodurch verhindert wird, dass eine Endlosschleife von Nachrichten gesendet wird. Weitere Informationen zur Verwendung von Timer-Aktionen in Ihrem Melder finden Sie auf der Seite Verwenden integrierter Aktionen im AWS IoT Events Entwicklerhandbuch

`expression-syntax`

Ein Analyseergebnis mit Informationen über`expression-syntax`, entspricht den folgenden Fehlermeldungen:

- Nachricht: Ihr Payload-Ausdruck {*expression*} ist nicht gültig. Der definierte Payload-Typ istJSON, Sie müssen also einen Ausdruck angeben, der eine Zeichenfolge ergeben AWS IoT Events würde.

  Lösung: Wenn der angegebene Nutzdatentyp „ist“JSON, wird AWS IoT Events zunächst geprüft, ob der Dienst Ihren Ausdruck als Zeichenfolge auswerten kann. Das ausgewertete Ergebnis darf weder ein boolescher Wert noch eine Zahl sein. Wenn die Überprüfung nicht erfolgreich ist, erhalten Sie möglicherweise diesen Fehler.
- Nachricht: `SetVariableAction.value` muss ein Ausdruck sein. Der Wert '' konnte nicht analysiert werden*variable-value*'

  Lösung: Sie können es verwenden`SetVariableAction`, um eine Variable mit einem `name` und `value` zu definieren. Dabei `value` kann es sich um eine Zeichenfolge, eine Zahl oder einen booleschen Wert handeln. Sie können auch einen Ausdruck für die angeben. `value` Weitere Informationen finden Sie unter SetVariableAction, in der AWS IoT Events APIReferenz.
- Nachricht: Wir konnten Ihren Ausdruck der Attribute nicht analysieren (*attribute-name*) für die DynamoDB-Aktion. Geben Sie einen Ausdruck mit der richtigen Syntax ein.

  Lösung: Sie müssen Ausdrücke für alle Parameter in Ersatzvorlagen verwenden`DynamoDBAction`. Weitere Informationen finden Sie unter D ynamoDBAction in der AWS IoT Events APIReferenz.
- Nachricht: Wir konnten Ihren Ausdruck tableName für die Aktion D ynamoDBv 2 nicht analysieren. Geben Sie den Ausdruck mit der richtigen Syntax ein.

  Lösung: `tableName` Bei der Eingabe `DynamoDBv2Action` muss es sich um eine Zeichenfolge handeln. Sie müssen einen Ausdruck für die verwenden`tableName`. Die Ausdrücke akzeptieren Literale, Operatoren, Funktionen, Referenzen und Substitutionsvorlagen. Weitere Informationen finden Sie unter D ynamoDBv 2Action in der AWS IoT Events APIReferenz.
- Nachricht: Wir konnten Ihren Ausdruck nicht als gültig JSON bewerten. Die D ynamoDBv 2-Aktion unterstützt nur den JSON Payload-Typ.

  Lösung: Der Payload-Typ für `DynamoDBv2` muss sein. JSON Stellen Sie sicher, dass Ihr Inhaltsausdruck geprüft werden AWS IoT Events kann, damit die Payload gültig ist. JSON Weitere Informationen finden Sie unter D ynamoDBv 2Action in der AWS IoT Events API Referenz.
- Nachricht: Wir konnten Ihren Inhaltsausdruck nicht nach der Payload von analysieren *action-type*. Geben Sie einen Inhaltsausdruck mit der richtigen Syntax ein.

Lösung: Der Inhaltsausdruck kann Zeichenketten enthalten ('*string*'), Variablen ($variable.*variable-name*), Eingabewerte ($input.*input-name*.*path-to-datum*), Zeichenkettenverkettungen und Zeichenketten, die enthalten. `${}`

- Nachricht: Benutzerdefinierte Payloads dürfen nicht leer sein.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie für Ihre Aktion Benutzerdefiniertes Payload ausgewählt und keinen Inhaltsausdruck in der Konsole eingegeben haben. AWS IoT Events Wenn Sie Benutzerdefinierter Payload wählen, müssen Sie unter Benutzerdefinierter Payload einen Inhaltsausdruck eingeben. Weitere Informationen finden Sie in der Referenz unter Payload.AWS IoT Events API

- Meldung: Fehler beim Analysieren des Ausdrucks für die Dauer '*duration-expression*'für den Timer'*timer-name*'.

  Lösung: Das ausgewertete Ergebnis Ihres Dauerausdrucks für den Timer muss ein Wert zwischen 60—31622400 sein. Das ausgewertete Ergebnis der Dauer wird auf die nächste ganze Zahl abgerundet.

- Meldung: Der Ausdruck 'konnte nicht analysiert werden*expression*'für *action-name*

  Lösung: Möglicherweise erhalten Sie diese Meldung, wenn der Ausdruck für die angegebene Aktion eine falsche Syntax hat. Stellen Sie sicher, dass Sie einen Ausdruck mit der richtigen Syntax eingeben. Weitere Informationen finden Sie unter Syntax zum Filtern von Gerätedaten und zum Definieren von Aktionen.

- Nachricht: Ihr *fieldName* denn `IotSitewiseAction` konnte nicht analysiert werden. Sie müssen in Ihrem Ausdruck die richtige Syntax verwenden.

  Lösung: Möglicherweise erhalten Sie diesen Fehler, wenn Sie AWS IoT Events Ihren nicht analysieren konnten *fieldName* für `IotSitewiseAction`. Stellen Sie sicher, dass *fieldName* verwendet einen Ausdruck, der analysiert AWS IoT Events werden kann. Weitere Informationen finden Sie IotSiteWiseActionin der AWS IoT Events APIReferenz.

`data-type`

Ein Analyseergebnis mit Informationen über`data-type`, entspricht den folgenden Fehlermeldungen:

- Meldung: Ausdruck für die Dauer *duration-expression* für Timer *timer-name* ist nicht gültig, es muss eine Zahl zurückgegeben werden.

Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie den Dauerausdruck für Ihren Timer nicht als Zahl auswerten AWS IoT Events konnten. Stellen Sie sicher, dass Ihr Wert in eine Zahl umgewandelt werden `durationExpression` kann. Andere Datentypen, wie z. B. Boolean, werden nicht unterstützt.

- Nachricht: Ausdruck *`condition-expression`* ist kein gültiger Bedingungsausdruck.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie Ihren Wert nicht `condition-expression` auf einen booleschen Wert auswerten AWS IoT Events konnten. Der boolesche Wert muss entweder oder sein. `TRUE` `FALSE` Stellen Sie sicher, dass Ihr Bedingungsausdruck in einen booleschen Wert konvertiert werden kann. Wenn das Ergebnis kein boolescher Wert ist, entspricht es den Aktionen, die im Ereignis angegeben wurden, `FALSE` und ruft diese nicht auf`nextState`.

- Meldung: Inkompatible Datentypen [*`inferred-types`*] gefunden für *`reference`* im folgenden Ausdruck: *`expression`*

  Lösung: Lösung: Alle Ausdrücke für dasselbe Eingabeattribut oder dieselbe Variable im Detektormodell müssen auf denselben Datentyp verweisen.

  Verwenden Sie die folgenden Informationen, um das Problem zu beheben:

  - Wenn Sie eine Referenz als Operanden mit einem oder mehreren Operatoren verwenden, stellen Sie sicher, dass alle Datentypen, auf die Sie verweisen, kompatibel sind.

    Im folgenden Ausdruck 2 ist Integer beispielsweise ein Operand sowohl der == Operatoren als auch. && Um sicherzustellen, dass die Operanden kompatibel sind `$variable.testVariable + 1` und auf eine Ganzzahl oder Dezimalzahl verweisen `$variable.testVariable` müssen.

    Außerdem 1 ist Integer ein Operand des Operators+. `$variable.testVariable`Muss daher auf eine Ganzzahl oder Dezimalzahl verweisen.

    ```
    '$variable.testVariable + 1 == 2 && $variable.testVariable'
    ```

  - Wenn Sie eine Referenz als Argument verwenden, das an eine Funktion übergeben wird, stellen Sie sicher, dass die Funktion die Datentypen unterstützt, auf die Sie verweisen.

    Für die folgende `timeout("`*`time-name`*`")` Funktion ist beispielsweise eine Zeichenfolge mit doppelten Anführungszeichen als Argument erforderlich. Wenn Sie eine Referenz für die verwenden *`timer-name`* Wert, Sie müssen auf eine Zeichenfolge mit doppelten Anführungszeichen verweisen.

```
timeout("timer-name")
```

> **Note**
>
> Für die `convert(type, expression)` Funktion, wenn Sie eine Referenz für die *`type`* Wert, das ausgewertete Ergebnis Ihrer Referenz muss `StringDecimal`, oder sein`Boolean`.

Weitere Informationen finden Sie unter Referenz für Eingaben und Variablen in Ausdrücken.

- Meldung: Inkompatible Datentypen [*`inferred-types`*] verwendet mit *`reference`*. Dies kann zu einem Laufzeitfehler führen.

  Lösung: Möglicherweise erhalten Sie diese Warnmeldung, wenn zwei Ausdrücke für dasselbe Eingabeattribut oder dieselbe Variable auf zwei Datentypen verweisen. Stellen Sie sicher, dass Ihre Ausdrücke für dasselbe Eingabeattribut oder dieselbe Variable auf denselben Datentyp im Detektormodell verweisen.

- Meldung: Die Datentypen [*`inferred-types`*], die Sie für den Operator [eingegeben haben*`operator`*] sind für den folgenden Ausdruck nicht kompatibel: '*`expression`*'

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Ihr Ausdruck Datentypen kombiniert, die mit einem angegebenen Operator nicht kompatibel sind. Im folgenden Ausdruck + ist der Operator beispielsweise mit den Datentypen Integer, Decimal und String kompatibel, nicht jedoch mit Operanden des Booleschen Datentyps.

  ```
  true + false
  ```

  Sie müssen sicherstellen, dass die Datentypen, die Sie mit einem Operator verwenden, kompatibel sind.

- Meldung: Die Datentypen [*`inferred-types`*] gefunden für *`input-attribute`* sind nicht kompatibel und können zu einem Laufzeitfehler führen.

  Lösung: Diese Fehlermeldung wird möglicherweise angezeigt, wenn zwei Ausdrücke für dasselbe Eingabeattribut auf zwei Datentypen verweisen, entweder für den `OnEnterLifecycle` eines Zustands oder für den `OnInputLifecycle` und `OnExitLifecycle` eines Zustands. Stellen Sie sicher, dass Ihre Ausdrücke in `OnEnterLifecycle` (oder, `OnInputLifecycle` sowohl

als auch`OnExitLifecycle`) für jeden Status Ihres Detektormodells auf denselben Datentyp verweisen.

- Nachricht: Der Payload-Ausdruck [*`expression`*] ist nicht gültig. Geben Sie einen Ausdruck an, der zur Laufzeit zu einer Zeichenfolge ausgewertet wird, da der Nutzdatentyp JSON Format ist.

  Lösung: Möglicherweise erhalten Sie diesen Fehler, wenn der angegebene Payload-Typ zwar lautetJSON, aber AWS IoT Events Sie können seinen Ausdruck nicht als Zeichenfolge auswerten. Stellen Sie sicher, dass das ausgewertete Ergebnis eine Zeichenfolge und kein boolescher Wert oder eine Zahl ist.

- Nachricht: Ihr interpolierter Ausdruck {*`interpolated-expression`*} muss zur Laufzeit entweder eine Ganzzahl oder einen booleschen Wert ergeben. Andernfalls ist Ihr Payload-Ausdruck {*`payload-expression`*} kann zur Laufzeit nicht als gültig analysiert werden. JSON

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie Ihren interpolierten Ausdruck nicht zu einer Ganzzahl oder einem booleschen Wert auswerten AWS IoT Events konnten. Stellen Sie sicher, dass Ihr interpolierter Ausdruck in eine Ganzzahl oder einen booleschen Wert konvertiert werden kann, da andere Datentypen, wie z. B. Zeichenfolge, nicht unterstützt werden.

- Meldung: Der Ausdruckstyp im Feld `IotSitewiseAction` *`expression`* ist als Typ definiert *`defined-type`* und als Typ abgeleitet *`inferred-type`*. Der definierte Typ und der abgeleitete Typ müssen identisch sein.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Ihr Ausdruck in `propertyValue` of einen Datentyp `IotSitewiseAction` hat, der anders definiert ist als der von abgeleitete Datentyp. AWS IoT Events Stellen Sie sicher, dass Sie für alle Instanzen dieses Ausdrucks in Ihrem Detektormodell denselben Datentyp verwenden.

- Meldung: Die Datentypen [*`inferred-types`*], die für eine `setTimer` Aktion verwendet werden, werden nicht `Integer` für den folgenden Ausdruck ausgewertet: *`expression`*

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn der abgeleitete Datentyp für Ihren Dauerausdruck nicht Integer oder Decimal ist. Stellen Sie sicher, dass Ihr `durationExpression` Wert in eine Zahl umgewandelt werden kann. Andere Datentypen wie Boolean und String werden nicht unterstützt.

- Meldung: Die Datentypen [*`inferred-types`*] wird mit Operanden des Vergleichsoperators [verwendet*`operator`*] sind im folgenden Ausdruck nicht kompatibel: *`expression`*

Lösung: Die abgeleiteten Datentypen für die Operanden von *operator* im bedingten Ausdruck (*expression*) Ihres Detektormodells stimmen nicht überein. Die Operanden müssen mit den passenden Datentypen in allen anderen Teilen Ihres Detektormodells verwendet werden.

> **Tip**
>
> Sie können sie verwendenconvert, um den Datentyp eines Ausdrucks in Ihrem Detektormodell zu ändern. Weitere Informationen finden Sie unter Funktionen zur Verwendung in Ausdrücken.

referenced-data

Ein Analyseergebnis mit Informationen überreferenced-data, entspricht den folgenden Fehlermeldungen:

- Meldung: Defekter Timer: Timer erkannt *timer-name* wird in einem Ausdruck verwendet, aber nie gesetzt.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie einen Timer verwenden, der nicht eingestellt ist. Sie müssen einen Timer festlegen, bevor Sie ihn in einem Ausdruck verwenden können. Stellen Sie außerdem sicher, dass Sie den richtigen Timer-Namen eingeben.
- Meldung: Fehlerhaft erkannt Variable: Variable *variable-name* wird in einem Ausdruck verwendet, aber nie gesetzt.

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie eine Variable verwenden, die nicht festgelegt ist. Sie müssen eine Variable festlegen, bevor Sie sie in einem Ausdruck verwenden können. Stellen Sie außerdem sicher, dass Sie den richtigen Variablennamen eingeben.
- Meldung: Fehlerhafte Variable erkannt: Eine Variable wird in einem Ausdruck verwendet, bevor sie auf einen Wert gesetzt wird.

  Lösung: Jeder Variablen muss ein Wert zugewiesen werden, bevor sie in einem Ausdruck ausgewertet werden kann. Legen Sie den Wert der Variablen vor jeder Verwendung fest, damit ihr Wert abgerufen werden kann. Stellen Sie außerdem sicher, dass Sie den richtigen Variablennamen eingeben.

`referenced-resource`

Ein Analyseergebnis mit Informationen über`referenced-resource`, entspricht den folgenden Fehlermeldungen:

- Meldung: Die Detector Model Definition enthält einen Verweis auf Input, der nicht existiert.

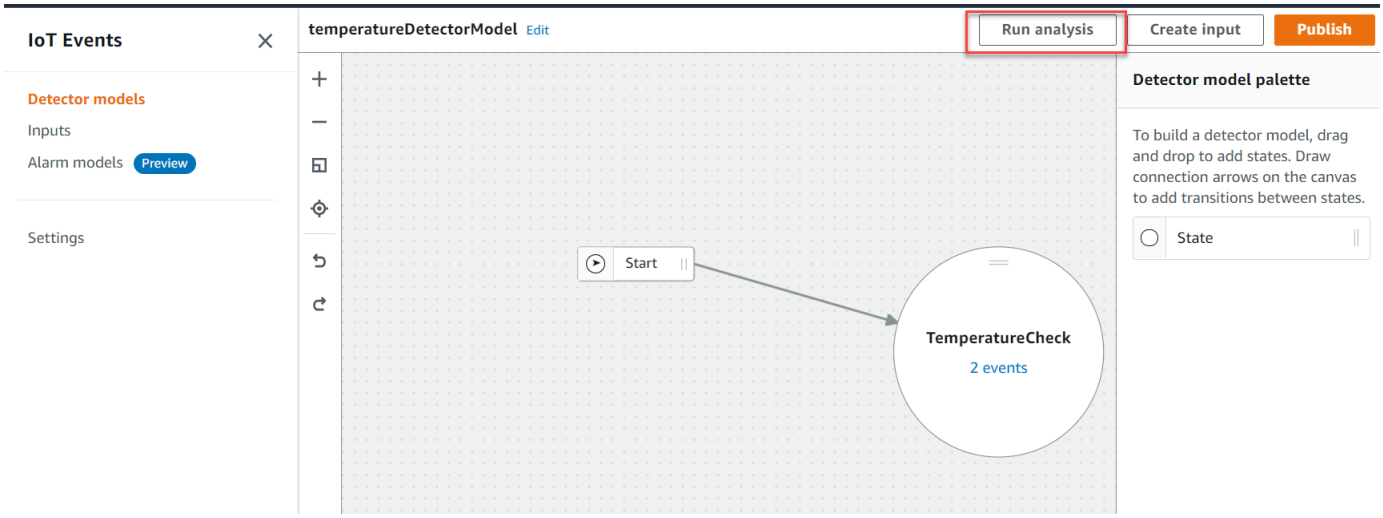
  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Sie Ausdrücke verwenden, um auf eine Eingabe zu verweisen, die nicht existiert. Stellen Sie sicher, dass Ihr Ausdruck auf eine vorhandene Eingabe verweist, und geben Sie den richtigen Eingabenamen ein. Wenn Sie keine Eingabe haben, erstellen Sie zuerst eine.
- Meldung: Die Modelldefinition des Detektors enthält folgende ungültige Angaben InputName: *`input-name`*

  Lösung: Möglicherweise erhalten Sie diese Fehlermeldung, wenn Ihr Detektormodell einen ungültigen Eingabenamen enthält. Stellen Sie sicher, dass Sie den richtigen Eingabenamen eingeben. Der Eingabename muss 1-128 Zeichen lang sein. Gültige Zeichen: a-z, A-Z, 0-9, _ (Unterstrich) und - (Bindestrich).

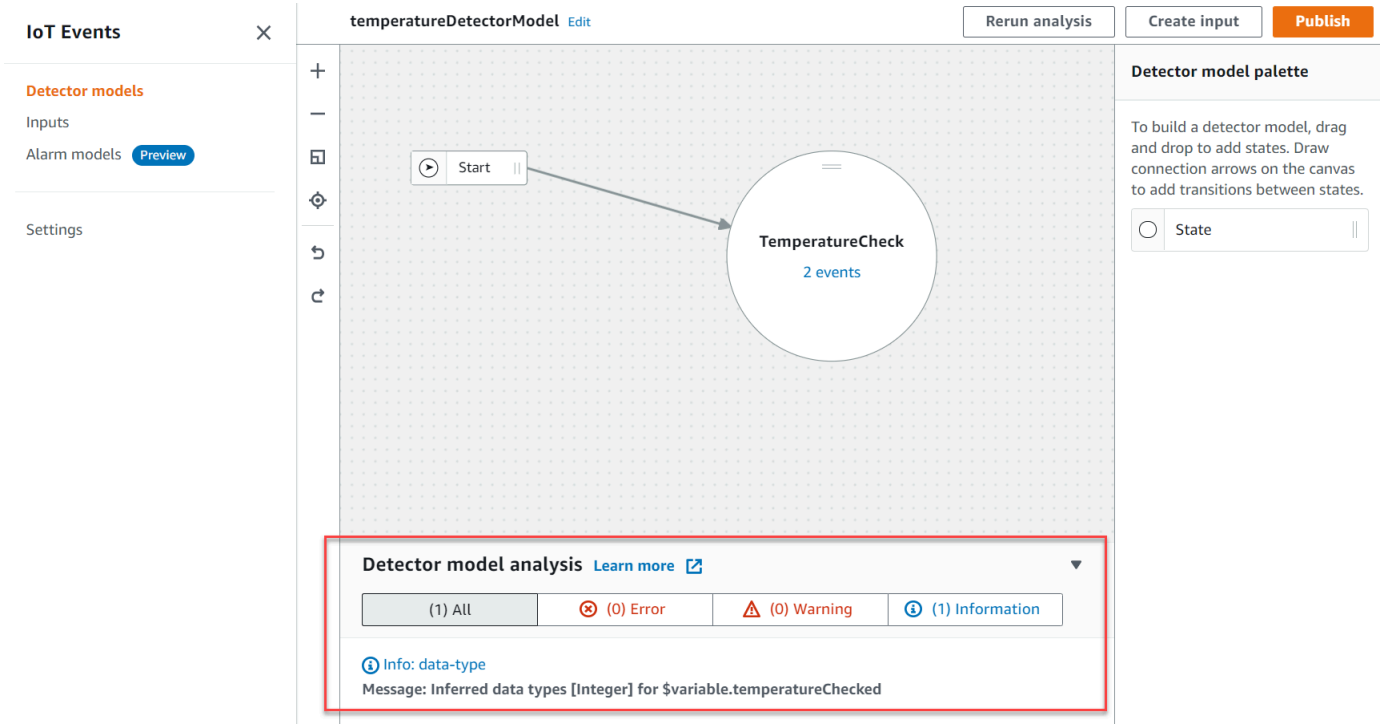
Analysieren eines Detektormodells (Konsole)

In den folgenden Schritten wird die AWS IoT Events Konsole verwendet, um ein Detektormodell zu analysieren.

1. Melden Sie sich an der AWS IoT Events -Konsole an.
2. Wählen Sie im Navigationsbereich die Option Detektormodelle aus.
3. Wählen Sie unter Detektormodelle das Zieldetektormodell aus.
4. Wählen Sie auf der Seite mit dem Meldermodell die Option Bearbeiten aus.
5. Wählen Sie in der oberen rechten Ecke die Option Analyse ausführen aus.



Im Folgenden finden Sie ein Beispiel für ein Analyseergebnis in der AWS IoT Events Konsole.



> **Note**
>
> Nachdem Sie AWS IoT Events mit der Analyse Ihres Detektormodells begonnen haben, haben Sie bis zu 24 Stunden Zeit, um die Analyseergebnisse abzurufen.

Analysieren eines Detektormodells (AWS CLI)

In den folgenden Schritten wird AWS CLI ein Detektormodell analysiert.

1. Führen Sie den folgenden Befehl aus, um eine Analyse zu starten.

```
aws iotevents start-detector-model-analysis --cli-input-json file://file-name.json
```

> **Note**
>
> Ersetzen *file-name* mit dem Namen der Datei, die die Definition des Detektormodells enthält.

Example Definition des Detektormodells

```
{
    "detectorModelDefinition": {
        "states": [
            {
                "stateName": "TemperatureCheck",
                "onInput": {
                    "events": [
                        {
                            "eventName": "Temperature Received",
                            "condition":
 "isNull($input.TemperatureInput.sensorData.temperature)==false",
                            "actions": [
                                {
                                    "iotTopicPublish": {
                                        "mqttTopic": "IoTEvents/Output"
                                    }
                                }
                            ]
                        }
                    ],
                    "transitionEvents": []
                },
                "onEnter": {
                    "events": [
                        {
```

```
                            "eventName": "Init",
                            "condition": "true",
                            "actions": [
                                {
                                    "setVariable": {
                                        "variableName": "temperatureChecked",
                                        "value": "0"
                                    }
                                }
                            ]
                        }
                    ]
                },
                "onExit": {
                    "events": []
                }
            }
        ],
        "initialStateName": "TemperatureCheck"
    }
}
```

Wenn Sie den verwenden AWS CLI , um ein vorhandenes Detektormodell zu analysieren, wählen Sie eine der folgenden Optionen, um die Definition des Detektormodells abzurufen:

- Wenn Sie die AWS IoT Events Konsole verwenden möchten, gehen Sie wie folgt vor:
  1. Wählen Sie im Navigationsbereich die Option Detector models aus.
  2. Wählen Sie unter Detektormodelle das Zieldetektormodell aus.
  3. Wählen Sie unter Aktion die Option Detektormodell exportieren aus, um das Detektormodell herunterzuladen. Das Detektormodell ist in gespeichertJSON.
  4. Öffnen Sie die JSON Modelldatei des Detektors.
  5. Sie benötigen nur das `detectorModelDefinition` Objekt. Entfernen Sie Folgendes:
     - Die erste geschweifte Klammer (`{`) oben auf der Seite
     - Die Linie `detectorModel`
     - Das `detectorModelConfiguration`-Objekt
     - Die letzte geschweifte Klammer (`}`) unten auf der Seite
  6. Speichern Sie die Datei.
- Wenn Sie den verwenden möchten AWS CLI, gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl von einem Terminal aus.

```
aws iotevents describe-detector-model --detector-model-name detector-model-name
```

2. Ersetzen *detector-model-name* mit dem Namen Ihres Detektormodells.
3. Kopieren Sie das `detectorModelDefinition` Objekt in einen Texteditor.
4. Fügen Sie geschweifte Klammern (`{}`) außerhalb von hinzu. `detectorModelDefinition`
5. Speichern Sie die Datei inJSON.

Example Beispielantwort

```
{
    "analysisId": "c1133390-14e3-4204-9a66-31efd92a4fed"
}
```

2. Kopieren Sie die Analyse-ID aus der Ausgabe.
3. Führen Sie den folgenden Befehl aus, um den Status der Analyse abzurufen.

```
aws iotevents describe-detector-model-analysis --analysis-id "analysis-id"
```

> **Note**
>
> Ersetzen *analysis-id* mit der Analyse-ID, die Sie kopiert haben.

Example Beispielantwort

```
{
    "status": "COMPLETE"
}
```

Der Status kann einer der folgenden Werte sein:

- `RUNNING`— AWS IoT Events analysiert Ihr Detektormodell. Dieser Vorgang kann bis zu einer Minute dauern.
- `COMPLETE`— die Analyse Ihres Detektormodells AWS IoT Events abgeschlossen.

- `FAILED`— AWS IoT Events konnte Ihr Detektormodell nicht analysieren. Bitte versuchen Sie es später erneut.

4. Führen Sie den folgenden Befehl aus, um ein oder mehrere Analyseergebnisse des Detektormodells abzurufen.

> **Note**
>
> Ersetzen *`analysis-id`* mit der Analyse-ID, die Sie kopiert haben.

```
aws iotevents get-detector-model-analysis-results --analysis-id "analysis-id"
```

Example Beispielantwort

```
{
    "analysisResults": [
        {
            "type": "data-type",
            "level": "INFO",
            "message": "Inferred data types [Integer] for
 $variable.temperatureChecked",
            "locations": []
        },
        {
            "type": "referenced-resource",
            "level": "ERROR",
            "message": "Detector Model Definition contains reference to Input
 'TemperatureInput' that does not exist.",
            "locations": [
                {
                    "path": "states[0].onInput.events[0]"
                }
            ]
        }
    ]
}
```

> **Note**
>
> Nachdem Sie AWS IoT Events mit der Analyse Ihres Detektormodells begonnen haben, haben Sie bis zu 24 Stunden Zeit, um die Analyseergebnisse abzurufen.

AWS IoT Events befehle

In diesem Kapitel finden Sie ausführliche Informationen zu allen API Vorgängen, einschließlich Beispielanfragen, Antworten und Fehlern für die unterstützten Webdienstprotokolle. AWS IoT Events

AWS IoT Events Aktionen

Sie können AWS IoT Events API Befehle verwenden, um Eingänge und Detektormodelle zu erstellen, zu lesen, zu aktualisieren und zu löschen und ihre Versionen aufzulisten. Weitere Informationen finden Sie AWS IoT Events in der AWS IoT Events APIReferenz unter Aktionen und Datentypen, die von unterstützt werden.

Die AWS IoT Events Abschnitte in der AWS CLI Befehlsreferenz enthalten die AWS CLI Befehle, die Sie zur Verwaltung und Bearbeitung AWS IoT Events verwenden können.

AWS IoT Events Daten

Sie können die AWS IoT Events API Datenbefehle verwenden, um Eingaben an Melder zu senden, Melder aufzulisten und den Status eines Melders anzuzeigen oder zu aktualisieren. Weitere Informationen finden Sie in der AWS IoT Events APIReferenz unter Aktionen und Datentypen, die von AWS IoT Events Data unterstützt werden.

Die AWS IoT Events Datenabschnitte in der AWS CLI Befehlsreferenz enthalten die AWS CLI Befehle, mit denen Sie AWS IoT Events Daten verarbeiten können.

Dokumenthistorie für AWS IoT Events

In der folgenden Tabelle werden die wichtigen Änderungen am AWS IoT Events Entwicklerhandbuch nach dem 17. September 2020 beschrieben. Für weitere Informationen zu Aktualisierungen dieser Dokumentation können Sie einen RSS Feed abonnieren.

Änderung	Beschreibung	Datum
Start in der Region	AWS IoT Events ist jetzt in der Region Asien-Pazifik (Mumbai) verfügbar.	30. September 2021
Start der Region	AWS IoT Events ist jetzt in der Region AWS GovCloud (USA West) verfügbar.	22. September 2021
Führen Sie Analysen durch Ausführen von Analysen zur Fehlerbehebung bei einem Detektormodell durch	AWS IoT Events kann jetzt Ihr Detektormodell analysier en und Analyseergebnisse generieren, die Sie zur Fehlerbehebung bei Ihrem Detektormodell verwenden können.	23. Februar 2021
Start in der Region	AWS IoT Events In China (Peking) eingeführt.	30. September 2020
Verwendung von Ausdrücken	Es wurden Beispiele hinzugefü gt, die Ihnen zeigen, wie man Ausdrücke schreibt.	22. September 2020
Überwachung mit Alarmen	Alarme helfen Ihnen dabei, Ihre Daten auf Änderunge n zu überwachen. Sie können Alarme erstellen, die Benachrichtigungen senden,	1. Juni 2020

wenn ein Schwellenwert überschritten wird.

Frühere Aktualisierungen

In der folgenden Tabelle werden wichtige Änderungen am AWS IoT Events Entwicklerhandbuch vor dem 18. September 2020 beschrieben.

Änderung	Beschreibung	Datum
Die Typvalidierung wurde zur Expressionsreferenz hinzugefügt	Informationen zur Typvalidierung wurden der Ausdrucksreferenz hinzugefügt.	3. August 2020
Es wurde eine Regionswarnung für andere Dienste hinzugefügt	Es wurde eine Warnung zur Auswahl derselben Region für AWS IoT Events und andere AWS Dienste hinzugefügt.	7. Mai 2020
Ergänzungen, Aktualisierungen	• Funktion zur Anpassung der Nutzlast • Neue Ereignisaktionen: Amazon DynamoDB und AWS IoT SiteWise	27. April 2020
Integrierte Funktionen für bedingte Ausdrücke im Detektormodell wurden hinzugefügt	Integrierte Funktionen für bedingte Ausdrücke im Detektormodell wurden hinzugefügt.	10. September 2019
Beispiele für Detektormodelle hinzugefügt	Beispiele für das Detektormodell wurden hinzugefügt.	5. August 2019
Neue Event-Aktionen hinzugefügt	Neue Event-Aktionen hinzugefügt für: • Lambda	19. Juli 2019

Änderung	Beschreibung	Datum
	• Amazon SQS • Kinesis Data Firehose • AWS IoT Events Eingabe	
Ergänzungen, Korrekturen	• Die Beschreibung der `timeout()` Funktion wurde aktualisiert. • Bewährte Methode in Bezug auf Kontoinaktivität hinzugefügt.	11. Juni 2019
Die Berechtigungsrichtlinie und die Debug-Optionen für die Konsole wurden aktualisiert	• Die Richtlinie für Konsolenberechtigungen wurde aktualisiert. • Das Bild der Seite mit den Debug-Optionen für die Konsole wurde aktualisiert.	5. Juni 2019
Aktualisierungen	AWS IoT Events Der Dienst ist jetzt allgemein verfügbar.	30. Mai 2019
Ergänzungen, Aktualisierungen	• Aktualisierte Sicherheitsinformationen. • Ein Beispiel für ein kommentiertes Detektormodell wurde hinzugefügt.	22. Mai 2019
Beispiele und erforderliche Berechtigungen wurden hinzugefügt	Beispiele für SNS Amazon-Nutzlasten hinzugefügt; Ergänzungen zu den erforderlichen Berechtigungen für`CreateDetectorModel` .	17. Mai 2019

Änderung	Beschreibung	Datum
Zusätzliche Sicherheitsinformationen hinzugefügt	Dem Sicherheitsbereich wurden Informationen hinzugefügt.	9. Mai 2019
Limitierte Vorschauversion	Eingeschränkte Vorschauversion der Dokumentation.	28. März 2019

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.