User Guide

AWS IoT Analytics

AWS IoT Analytics: User Guide

Table of Contents

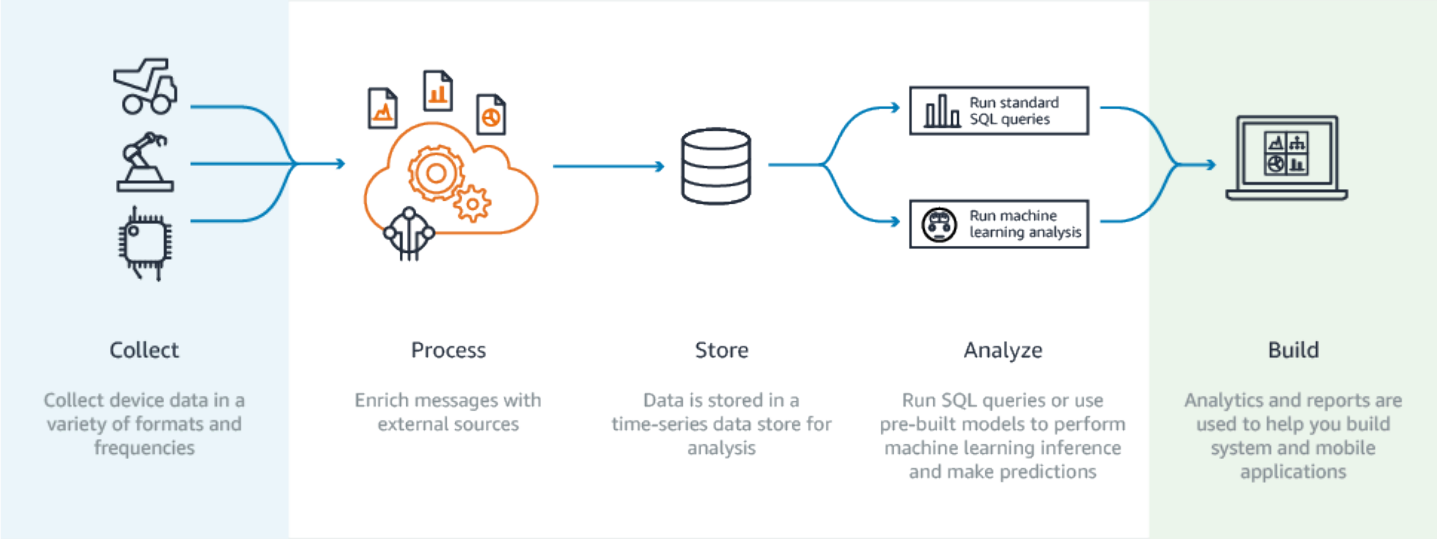
Was ist AWS IoT Analytics?

AWS IoT Analyticsautomatisiert die Schritte, die zur Analyse von Daten von IoT-Geräten erforderlich sind. AWS IoT Analyticsfiltert, transformiert und reichert IoT-Daten an, bevor sie zur Analyse in einem Zeitreihendatenspeicher gespeichert werden. Sie können den Service so einrichten, dass er nur die Daten sammelt, die Sie von Ihren Geräten benötigen, mathematische Transformationen zur Verarbeitung der Daten anwendet und die Daten mit gerätespezifischen Metadaten wie Gerätetyp und Standort erweitert, bevor Sie sie speichern. Anschließend können Sie Ihre Daten analysieren, indem Sie Abfragen mithilfe der integrierten SQL-Abfrage-Engine ausführen oder komplexere Analysen und Inferenzen für maschinelles Lernen durchführen. AWS IoT Analyticsermöglicht erweiterte Datenexploration durch die Integration mit Jupyter Notebook. AWS IoT Analyticsermöglicht auch die Datenvisualisierung durch die Integration mit Amazon QuickSight. Amazon QuickSight ist in den folgenden -Regionen verfügbar.

Herkömmliche Analyse- und Business-Intelligence-Tools sind für die Verarbeitung strukturierter Daten ausgelegt. IoT-Rohdaten stammen häufig von Geräten, die weniger strukturierte Daten (wie Temperatur, Bewegung oder Ton) aufzeichnen. Die Daten von diesen Geräten können daher erhebliche Lücken, beschädigte Nachrichten und falsche Messwerte aufweisen, die vor der Analyse bereinigt werden müssen. Außerdem sind IoT-Daten oft nur im Kontext mit anderen Daten aus externen Quellen aussagekräftig. AWS IoT Analyticsermöglicht es Ihnen, diese Probleme zu lösen und große Mengen an Gerätedaten zu sammeln, Nachrichten zu verarbeiten und zu speichern. Anschließend können Sie die Daten abfragen und analysieren. AWS IoT Analyticsenthält vorgefertigte Modelle für gängige IoT-Anwendungsfälle, sodass Sie Fragen beantworten können, z. B. welche Geräte kurz vor dem Ausfall stehen oder bei welchen Kunden das Risiko besteht, dass sie ihre tragbaren Geräte aufgeben.

Funktionsweise von AWS IoT Analytics

Die folgende Grafik zeigt einen Überblick über die Verwendung vonAWS IoT Analytics.



Schlüsselfunktionen

Erfassen

- Integriert mitAWS IoT Core —AWS IoT Analytics ist vollständig integriert,AWS IoT Core sodass es Nachrichten von verbundenen Geräten empfangen kann, während diese einströmen.
- Verwenden Sie eine Batch-API, um Daten aus einer beliebigen Quelle hinzuzufügen —AWS IoT Analytics kann Daten aus jeder Quelle über HTTP empfangen. Das bedeutet, dass jedes Gerät oder jeder Dienst, der mit dem Internet verbunden ist, Daten senden kannAWS IoT Analytics. Weitere Informationen finden Sie unter BatchPutMessage in der AWS IoT Analytics-API-Referenz.
- Erfassen Sie nur die Daten, die Sie speichern und analysieren möchten — Sie können dieAWS IoT Analytics Konsole verwenden, um den Empfang von Nachrichten von Geräten über MQTT-Themenfilter in verschiedenen Formaten und FrequenzenAWS IoT Analytics zu konfigurieren. AWS IoT Analyticsüberprüft, ob sich die Daten innerhalb bestimmter Parameter befinden, die Sie definieren, und erstellt Kanäle. Anschließend leitet der Service die Kanäle zu geeigneten Pipelines für die Verarbeitung, Transformation und Anreicherung von Nachrichten um.

Prozess

- Bereinigen und filtern —AWS IoT Analytics ermöglicht die Definition vonAWS Lambda Funktionen, die ausgelöst werden, wenn fehlende DatenAWS IoT Analytics erkannt werden, sodass Sie Code ausführen können, um Lücken zu schätzen und zu schließen. Sie können auch maximale und minimale Filter sowie Perzentilschwellenwerte definieren, um Ausreißer in Ihren Daten zu entfernen.

- Transformieren —AWS IoT Analytics kann Nachrichten mithilfe von von Ihnen definierter mathematischer oder bedingter Logik transformieren, sodass Sie gängige Berechnungen wie die Umwandlung von Celsius in Fahrenheit durchführen können.
- Anreichern —AWS IoT Analytics kann Daten mit externen Datenquellen wie einer Wettervorhersage anreichern und die Daten dann an denAWS IoT Analytics Datenspeicher weiterleiten.

Speichern

- Zeitreihendatenspeicher —AWS IoT Analytics speichert die Gerätedaten in einem optimierten Zeitreihendatenspeicher für einen schnelleren Abruf und eine schnellere Analyse. Sie können Zugriffsberechtigungen verwalten, Datenaufbewahrungsrichtlinien implementieren und Ihre Daten an externe Zugriffspunkte exportieren.
- Verarbeitete Daten und Rohdaten speichern —AWS IoT Analytics Speichert die verarbeiteten Daten und speichert auch automatisch die aufgenommenen Rohdaten, sodass Sie sie zu einem späteren Zeitpunkt verarbeiten können.

Analysieren

- Ad-hoc-SQL-Abfragen ausführen —AWS IoT Analytics stellt eine SQL-Abfrage-Engine bereit, mit der Sie Ad-hoc-Abfragen ausführen und schnell Ergebnisse erzielen können. Mit dem Service können Sie Standard-SQL-Abfragen verwenden, um Daten aus dem Datenspeicher zu extrahieren, um Fragen wie die durchschnittliche zurückgelegte Entfernung einer Flotte vernetzter Fahrzeuge oder die Anzahl der Türen in einem intelligenten Gebäude nach 19 Uhr zu beantworten. Diese Abfragen können auch dann wiederverwendet werden, wenn sich die angeschlossenen Geräte, die Flottengröße und die analytischen Anforderungen ändern.
- Zeitreihenanalyse —AWS IoT Analytics unterstützt Zeitreihenanalysen, sodass Sie die Leistung von Geräten im Zeitverlauf analysieren und nachvollziehen können, wie und wo sie verwendet werden, kontinuierlich Gerätedaten überwachen, um Wartungsprobleme vorherzusagen, und Sensoren überwachen können, um Umgebungsbedingungen vorherzusagen und darauf zu reagieren.
- Gehostete Notebooks für anspruchsvolle Analysen und maschinelles Lernen —AWS IoT Analytics beinhaltet Unterstützung für gehostete Notebooks in Jupyter Notebook für statistische Analysen und maschinelles Lernen. Der Service umfasst eine Reihe von Notizbuchvorlagen, die vonAWS uns verfasste Modelle und Visualisierungen für maschinelles Lernen enthalten. Sie können die Vorlagen verwenden, um mit IoT-Anwendungsfällen zu beginnen, die mit der Erstellung von Geräteausfallprofilen, der Prognose von Ereignissen wie geringer Nutzung, die darauf hindeuten könnten, dass der Kunde das Produkt verlässt, oder mit der Segmentierung von Geräten nach Kundennutzungsgrad (z. B. Vielnutzer, Wochenendnutzer)

oder Gerätezustand beginnen. Nachdem Sie ein Notizbuch erstellt haben, können Sie es containerisieren und nach einem von Ihnen angegebenen Zeitplan ausführen. Weitere Informationen finden Sie unter Automatisierung Ihres Workflows.

- Prognose — Sie können die statistische Klassifizierung mithilfe einer Methode durchführen, die als logistische Regression bezeichnet wird. Sie können auch LSTM (Long-Short-Term Memory) verwenden, eine leistungsfähige neuronale Netzwerktechnik zur Prognose der Ausgabe oder des Zustands eines Prozesses, der im Laufe der Zeit variiert. Die vorkonfigurierten Notebook-Vorlagen unterstützen auch den K-Means-Clustering-Algorithmus für die Gerätesegmentierung, der Ihre Geräte in Gruppen ähnlicher Geräte einordnet. Diese Vorlagen werden typischerweise verwendet, um den Gerätezustand und den Gerätestatus zu erfassen, wie z. B. für HLK-Einheiten in einer Schokoladenfabrik oder die Abnutzung der Blätter an einer Windkraftanlage. Auch diese Notizbuchvorlagen können enthalten und nach einem Zeitplan ausgeführt werden.

Baue und visualisiere

- QuickSight Amazon-Integration —AWS IoT Analytics stellt einen Konnektor zu Amazon bereit, QuickSight sodass Sie Ihre Datensätze in einem QuickSight Dashboard visualisieren können.
- Konsolenintegration — Sie können die Ergebnisse Ihrer Ad-hoc-Analyse auch im eingebetteten Jupyter Notebook in der KonsoleAWS IoT Analytics visualisieren.

AWS IoT AnalyticsKomponenten und Konzepte

Channel

Ein Channel erfasst Daten aus einem MQTT-Thema und archiviert die unformatierten, nicht verarbeiteten Nachrichten vor der Veröffentlichung der Daten in einer Pipeline. Sie können Nachrichten auch direkt über die BatchPutMessageAPI an einen Channel senden. Sie werden die unverarbeiteten Nachrichten in einem Amazon Simple Storage Service (Amazon S3) -Bucket gespeichert, den Sie oder SieAWS IoT Analytics verwalten.

Pipeline

Eine Pipeline nimmt Nachrichten aus einem Channel auf und ermöglicht Ihnen, die Nachrichten vor dem Speichern in einem Datastore zu verarbeiten. Die Verarbeitungsschritte, die als Aktivitäten (Pipeline-Aktivitäten) bezeichnet werden, führen Transformationen für Ihre Nachrichten durch, z. B. das Entfernen, Umbenennen oder Hinzufügen von Nachrichtenattributen, das Filtern von Nachrichten basierend auf Attributwerten, das Aufrufen Ihrer Lambda-Funktionen für Nachrichten für eine erweiterte Verarbeitung oder mathematische Transformationen für die Normalisierung von Gerätedaten.

Datastore

Pipelines speichern ihre verarbeiteten Nachrichten in einem Datenspeicher. Ein Datenspeicher ist keine Datenbank, sondern ein skalierbares und abfragbares Repository für Ihre Nachrichten. Sie können mehrere Datenspeicher für Nachrichten von verschiedenen Geräten oder Standorten haben oder für nach Nachrichtenattributen gefilterte Nachrichten, abhängig von der jeweiligen Pipeline-Konfiguration und Ihren Anforderungen. Wie bei unverarbeiteten Kanalnachrichten werden die verarbeiteten Nachrichten eines Datenspeichers in einem Amazon S3 S3-Bucket gespeichert, den Sie oder SieAWS IoT Analytics verwalten.

Dataset

Sie rufen Daten aus einem Datenspeicher ab, indem Sie einen Datensatz erstellen. AWS IoT Analyticsermöglicht es Ihnen, einen SQL-Datensatz oder einen Container-Datensatz zu erstellen.

Nachdem Sie über einen Datensatz verfügen, können Sie Ihre Daten untersuchen und durch die Integration mit Amazon Einblicke in sie gewinnen QuickSight. Durch die Integration mit Jupyter Notebook können Sie auch erweiterte Analysefunktionen ausführen. Jupyter Notebook bietet leistungsstarke datenwissenschaftliche Tools, mit denen maschinelles Lernen und eine Reihe statistischer Analysen durchgeführt werden können. Weitere Informationen finden Sie unter Notebook-Vorlagen.

Sie können Datensatzinhalte an einen Amazon S3 S3-Bucket senden und so die Integration mit Ihren vorhandenen Data Lakes oder den Zugriff über interne Anwendungen und Visualisierungstools ermöglichen. Sie können auch Datensatzinhalte als Eingabe an einen Dienst senden AWS IoT Events, der es Ihnen ermöglicht, Geräte oder Prozesse auf Fehler oder Betriebsänderungen zu überwachen und zusätzliche Aktionen auszulösen, wenn solche Ereignisse eintreten.

SQL-Dataset

Ein SQL-Dataset ist vergleichbar mit einer materialisierten Ansicht aus einer SQL-Datenbank. Sie können einen SQL-Datensatz erstellen, indem Sie eine SQL-Aktion anwenden. SQL-Datasets können im Rahmen eines sich wiederholenden Zeitplans durch Angeben eines Auslösers automatisch generiert werden.

Container-Dataset

Ein Container-Datensatz ermöglicht es Ihnen, Ihre Analysetools automatisch auszuführen und Ergebnisse zu generieren. Weitere Informationen finden Sie unter Automatisierung Ihres Workflows. Darin werden ein SQL-Dataset als Eingabe, ein Docker-Container mit Ihren Analyse-

Tools und erforderlichen Bibliotheksdateien, Eingabe- und Ausgabevariablen und ein optionaler Zeitplanauslöser kombiniert. Die Eingabe- und Ausgabevariablen informieren das ausführbare Abbild darüber, wo die Daten abgerufen und die Ergebnisse gespeichert werden sollen. Der Auslöser kann Ihre Analyse entsprechend eines Zeitplanausdrucks ausführen oder wenn ein SQL-Dataset das Erstellen seiner Inhalte beendet. Die Ausführung, Erstellung und Speicherung der Ergebnisse des Analysetools erfolgt mit Container-Datasets automatisch.

Auslöser

Sie können automatisch ein Dataset erstellen, indem Sie einen Auslöser festlegen. Der Trigger kann ein Zeitintervall sein (z. B. diesen Datensatz alle zwei Stunden erstellen) oder der Zeitpunkt, an dem der Inhalt eines anderen Datensatzes erstellt wurde (erstellen Sie diesen Datensatz beispielsweise, wenn die Erstellung seines Inhalts`myOtherDataset` abgeschlossen ist). Oder Sie können Datensatzinhalte manuell mithilfe der CreateDatasetContentAPI generieren.

Docker-Container

Sie können Ihren eigenen Docker-Container erstellen, um Ihre Analysetools zu verpacken, oder die verfügbaren Optionen SageMaker verwenden. Weitere Informationen finden Sie unter Docker-Container. Sie können Ihren eigenen Docker-Container erstellen, um Ihre Analysetools zu verpacken, oder die von bereitgestellten Optionen verwenden SageMaker. Sie können einen Container in einer Amazon ECR-Registry speichern, die Sie angeben, sodass er für die Installation auf der gewünschten Plattform verfügbar ist. Docker-Container können Ihren benutzerdefinierten Analysecode ausführen, der mit Matlab, Octave, Wise.io, SPSS, R, Fortran, Python, Scala, Java, C++ usw. vorbereitet wurde. Weitere Informationen finden Sie unter Containerisieren von Notebooks.

Delta-Fenster

Delta-Fenster sind eine Reihe von benutzerdefinierten, nicht überschneidenden und zusammenhängenden Zeitintervallen. Delta-Fenster ermöglichen Ihnen, den Dataset-Inhalt mit neuen Daten, die seit der letzten Analyse im Datenspeicher eingetroffen sind, zu erstellen und Analysen für diese Daten durchzuführen. Sie erstellen ein Delta-Fenster, indem Sie das`deltaTime` in den`filters` Teil`queryAction` eines Datensatzes setzen. Weitere Informationen finden Sie in der `CreateDataset`-API. Normalerweise sollten Sie den Datensatzinhalt automatisch erstellen, indem Sie auch einen Zeitintervall-Trigger (`triggers:schedule:expression`) einrichten. Auf diese Weise können Sie Nachrichten filtern, die in einem bestimmten Zeitfenster eingegangen sind, sodass die in Nachrichten aus früheren Zeitfenstern enthaltenen Daten nicht zweimal gezählt werden. Weitere Informationen finden Sie unter Beispiel 6 — Erstellen eines SQL-Datensatzes mit einem Delta-Fenster (CLI).

Zugriff auf AWS IoT Analytics

AWS IoT AnalyticsStellt als Teil von die folgenden Schnittstellen bereitAWS IoT, über die Ihre Geräte Daten generieren und Ihre Anwendungen mit den von ihnen generierten Daten interagieren können:

AWS Command Line Interface (AWS CLI)

Führen Sie Befehle fürAWS IoT Analytics Windows, OS X und Linux aus. Mit diesen Befehlen können Sie Dinge, Zertifikate, Regeln und Richtlinien erstellen und verwalten. Informationen zu den ersten Schritten finden Sie im AWS Command Line Interface-Benutzerhandbuch. Weitere Informationen zu den Befehlen fürAWS IoT finden Sie unter iot in der AWS Command Line InterfaceReferenz.

> **Important**
>
> Verwenden Sie den`aws iotanalytics` Befehl, um mit zu interagierenAWS IoT Analytics. Verwenden Sie den`aws iot` Befehl, um mit anderen Teilen des IoT-Systems zu interagieren.

AWS IoT-API

Erstellen Ihrer IoT-Anwendungen mithilfe von HTTP- oder HTTPS-Anfragen. Mit diesen API-Aktionen können Sie Dinge, Zertifikate, Regeln und Richtlinien erstellen und verwalten. Weitere Informationen finden Sie unter -Aktionen in der AWS IoT-API-Referenz.

AWS-SDKs

Erstellen Sie IhreAWS IoT Analytics Anwendungen mit sprachspezifischen APIs. Diese SDKs umfassen die HTTP- und HTTPS-API und ermöglichen es Ihnen, in jeder der unterstützten Sprachen zu programmieren. Weitere Informationen finden Sie unter AWS SDKs und Tools.

AWS IoTGeräte-SDKs

Erstellen Sie Anwendungen, die auf Ihren Geräten ausgeführt werden und an die Nachrichten gesendetAWS IoT Analytics werden. Weitere Informationen finden Sie unter AWS IoT-SDKs.

AWS IoT Analytics-Konsole

Sie können die Komponenten erstellen, um die Ergebnisse in der AWS IoT AnalyticsKonsole zu visualisieren.

Anwendungsfälle

Prädiktive Wartung

AWS IoT Analyticsbietet Vorlagen zum Erstellen von Modellen für die vorausschauende Wartung und deren Anwendung auf Ihre Geräte. Sie könnenAWS IoT Analytics damit beispielsweise vorhersagen, wann Heiz- und Kühlsysteme bei vernetzten Frachtfahrzeugen voraussichtlich ausfallen werden, sodass die Fahrzeuge umgeleitet werden können, um Transportschäden zu vermeiden. Oder ein Automobilhersteller kann erkennen, welche seiner Kunden abgenutzte Bremsbeläge haben, und sie darauf hinweisen, dass sie sich um die Wartung ihrer Fahrzeuge kümmern sollten.

Proaktive Wiederauffüllung von Vorräten

AWS IoT Analyticsermöglicht die Erstellung von IoT-Anwendungen, mit denen Bestände in Echtzeit überwacht werden können. Beispielsweise kann ein Lebensmittel- und Getränkeunternehmen Daten von Lebensmittelautomaten analysieren und proaktiv Waren nachbestellen, wenn der Vorrat knapp wird.

Bewertung der Prozesseffizienz

MitAWS IoT Analytics können Sie IoT-Anwendungen erstellen, die die Effizienz verschiedener Prozesse ständig überwachen und Maßnahmen ergreifen, um den Prozess zu verbessern. Beispielsweise kann ein Bergbauunternehmen die Effizienz seiner Erztransporter steigern, indem es die Ladung für jede Fahrt maximiert. DamitAWS IoT Analytics kann das Unternehmen die effizienteste Ladung für einen Standort oder einen Lkw im Zeitverlauf ermitteln und dann etwaige Abweichungen von der Ziellast in Echtzeit vergleichen und die wichtigsten Richtlinien zur Verbesserung der Effizienz besser planen.

Intelligente Landwirtschaft

AWS IoT Analyticskann IoT-Gerätedaten mithilfe vonAWS IoT Registrierungsdaten oder öffentlichen Datenquellen mit kontextbezogenen Metadaten anreichern, sodass Ihre Analyse Zeit, Ort, Temperatur, Höhe und andere Umgebungsbedingungen berücksichtigt. Mit dieser Analyse können Sie Modelle erstellen, die empfohlene Aktionen für Ihre Geräte im Feld ausgeben. Um beispielsweise zu bestimmen, wann bewässert werden muss, könnten Bewässerungssysteme die Daten von Feuchtigkeitssensoren mit Daten über Niederschläge anreichern, was eine effizientere Wassernutzung ermöglicht.

Erste Schritte mitAWS IoT Analytics (Konsole)

Verwenden Sie dieses Tutorial, um dieAWS IoT Analytics Ressourcen (auch als Komponenten bezeichnet) zu erstellen, die Sie benötigen, um nützliche Erkenntnisse über Ihre IoT-Gerätedaten zu gewinnen.

Hinweise

- Wenn Sie im folgenden Tutorial Großbuchstaben eingeben,AWS IoT Analytics werden diese automatisch in Kleinbuchstaben geändert.
- DieAWS IoT Analytics Konsole verfügt über eine Einstiegsfunktion mit einem Klick, mit der Sie einen Kanal, eine Pipeline, einen Datenspeicher und einen Datensatz erstellen können. Sie finden diese Funktion, wenn Sie sich bei derAWS IoT Analytics Konsole anmelden.
  - In diesem Tutorial erfahren Sie, wie Sie IhreAWS IoT Analytics Ressourcen erstellen können.

Folgen Sie den nachstehenden Anweisungen, um einenAWS IoT Analytics Kanal, eine Pipeline, einen Datenspeicher und einen Datensatz zu erstellen. Das Tutorial zeigt Ihnen auch, wie Sie dieAWS IoT Core Konsole verwenden, um Nachrichten zu senden, die aufgenommen werdenAWS IoT Analytics.

Themen

Anmelden bei der AWS IoT Analytics-Konsole

Für den Einstieg benötigen Sie einAWS -Konto. Wenn Sie bereits einAWS Konto haben, navigieren Sie zu https://console.aws.amazon.com/iotanalytics/.

Wenn Sie keinAWS -Konto haben, führen Sie die folgenden Schritte zum Erstellen eines Kontos aus.

So erstellen Sie ein AWS-Konto

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

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

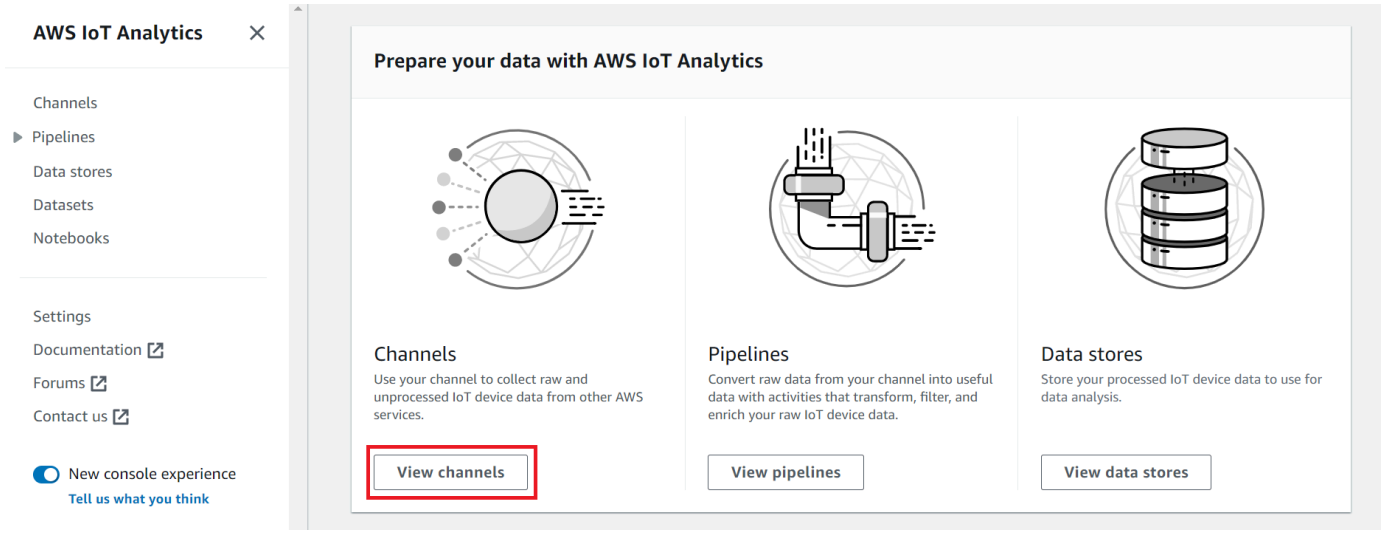
   Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Stammbenutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Methode zur Gewährleistung der Sicherheit sollten Sie den administrativen Zugriff einem administrativen Benutzer zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, die einen Root-Benutzerzugriff erfordern.
3. Melden Sie sich bei der anAWS Management Console und navigieren Sie zu https://console.aws.amazon.com/iotanalytics/.

Erstellen Sie einen Channel

Ein Kanal sammelt und archiviert rohe, unverarbeitete und unstrukturierte IoT-Gerätedaten. Befolgen Sie diese Schritte, um Ihren Channel zu erstellen.

So erstellen Sie einen Channel

1. Wählen Sie unter https://console.aws.amazon.com/iotanalytics/ imAWS IoT Analytics Abschnitt Daten vorbereiten mit die Option Kanäle anzeigen aus.



> **Tip**
>
> Sie können auch Kanäle im Navigationsbereich auswählen.

2. Wählen Sie auf der Seite Channels (Channels) die Option Create channel (Channel erstellen).
3. Geben Sie auf der Seite Kanaldetails angeben die Details zu Ihrem Kanal ein.

   a. Geben Sie einen eindeutigen Kanalnamen ein, den Sie leicht identifizieren können.

   b. (Optional) Fügen Sie für Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Channel hinzu. Mithilfe von Tags können Sie die Ressourcen, für die Sie erstellen, leichter identifizierenAWS IoT Analytics.

   c. Wählen Sie Next (Weiter).
4. AWS IoT Analyticsspeichert Ihre rohen, unverarbeiteten IoT-Gerätedaten in einem Amazon Simple Storage Service (Amazon S3) -Bucket. Sie können Ihren eigenen Amazon S3 S3-Bucket auswählen, auf den Sie zugreifen und ihn verwalten können, oder SieAWS IoT Analytics können den Amazon S3 S3-Bucket für Sie verwalten.

   a. Wählen Sie in diesem Tutorial für Speichertyp die Option Service Managed Storage aus.

   b. Wählen Sie für Wählen Sie aus, wie lange Ihre Rohdaten gespeichert werden sollen, die Option Unbegrenzt.

   c. Wählen Sie Next (Weiter).
5. Geben Sie auf der Seite „Quelle konfigurieren“ Informationen ein, ausAWS IoT Analytics denen Nachrichtendaten gesammelt werden sollenAWS IoT Core.

a. Geben Sie einenAWS IoT Core Themenfilter ein, zum Beispiel`update/environment/dht1`. Später in diesem Tutorial werden Sie diesen Themenfilter verwenden, um Nachrichtendaten an Ihren Kanal zu senden.

b. Wählen Sie im Bereich IAM-Rolle die Option Neu erstellen. Geben Sie im Fenster Neue Rolle erstellen einen Namen für die Rolle ein und wählen Sie dann Rolle erstellen. Dadurch wird automatisch eine Rolle erstellt, an die eine entsprechende Richtlinie angehängt ist.

c. Wählen Sie Next (Weiter).

6. Überprüfe deine Auswahl und wähle dann Kanal erstellen.
7. Vergewissere dich, dass dein neuer Kanal auf der Kanalseite erscheint.

Erstellen Sie einen Datenspeicher

Ein Datenspeicher empfängt und speichert Ihre Nachrichtendaten. Ein Datenspeicher ist keine Datenbank. Stattdessen ist ein Datenspeicher ein skalierbares und abfragebares Repository in einem Amazon S3 S3-Bucket. Sie können mehrere Datenspeicher für Nachrichten von verschiedenen Geräten oder Standorten verwenden. Oder Sie können Nachrichtendaten je nach Ihrer Pipeline-Konfiguration und Ihren Anforderungen filtern.

Befolgen Sie diese Schritte, um einen Datenspeicher zu erstellen.

Um einen Datenspeicher zu erstellen

1. Wählen Sie unter https://console.aws.amazon.com/iotanalytics/ imAWS IoT Analytics Abschnitt Daten vorbereiten mit die Option Datenspeicher anzeigen aus.
2. Wählen Sie auf der Seite Datenspeicher die Option Datenspeicher erstellen aus.
3. Geben Sie auf der Seite Datenspeicherdetails angeben grundlegende Informationen zu Ihrem Datenspeicher ein.

   a. Geben Sie als Datenspeicher-ID eine eindeutige Datenspeicher-ID ein. Sie können diese ID nicht mehr ändern, nachdem Sie sie erstellt haben.

   b. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Datenspeicher hinzuzufügen. Mithilfe von Tags können Sie die Ressourcen, für die Sie erstellen, leichter identifizierenAWS IoT Analytics.

   c. Wählen Sie Next (Weiter).

4. Geben Sie auf der Seite Speichertyp konfigurieren an, wie Ihre Daten gespeichert werden sollen.

   a. Wählen Sie als Speichertyp die Option Service Managed Storage aus.

   b. Wählen Sie unter Konfigurieren Sie, wie lange Sie Ihre verarbeiteten Daten behalten möchten, die Option Unbegrenzt aus.

   c. Wählen Sie Next (Weiter).

5. AWS IoT AnalyticsDatenspeicher unterstützen die Dateiformate JSON und Parquet. Wählen Sie für Ihr Datenspeicher-Datenformat JSON oder Parquet. DateiformateWeitere Informationen zuAWS IoT Analytics unterstützten Dateitypen finden Sie unter.

   Wählen Sie Next (Weiter).

6. (Optional)AWS IoT Analytics unterstützt benutzerdefinierte Partitionen in Ihrem Datenspeicher, sodass Sie bereinigte Daten abfragen können, um die Latenz zu verbessern. Weitere Informationen zu unterstützten benutzerdefinierten Partitionen finden Sie unterBenutzerdefinierte Partitionen.

   Wählen Sie Next (Weiter).

7. Überprüfen Sie Ihre Auswahl und wählen Sie dann Datenspeicher erstellen.

8. Stellen Sie sicher, dass Ihr neuer Datenspeicher auf der Seite Datenspeicher angezeigt wird.

Erstellen Sie eine Pipeline

Sie müssen eine Pipeline erstellen, um einen Kanal mit einem Datenspeicher zu verbinden. Eine einfache Pipeline gibt nur den Kanal an, der die Daten sammelt, und identifiziert den Datenspeicher, an den die Nachrichten gesendet werden. Weitere Informationen finden Sie unter Pipeline-Aktivitäten.

Für dieses Tutorial erstellen Sie eine Pipeline, die nur einen Kanal mit einem Datenspeicher verbindet. Später können Sie Pipeline-Aktivitäten hinzufügen, um diese Daten zu verarbeiten.

Befolgen Sie diese Schritte, um eine Pipeline zu erstellen.

So erstellen Sie eine Pipeline

1. Wählen Sie unter https://console.aws.amazon.com/iotanalytics/ imAWS IoT Analytics Abschnitt Prepare your data with die Option Pipelines anzeigen aus.

> **Tip**
>
> Sie können auch Pipelines im Navigationsbereich auswählen.

2. Wählen Sie auf der Seite Pipelines die Option Pipeline erstellen aus.
3. Geben Sie die Details zu Ihrer Pipeline ein.

   a. Geben Sie unter Setup-Pipeline-ID und -quellen einen Pipeline-Namen ein.

   b. Wählen Sie die Quelle Ihrer Pipeline aus. Dies ist einAWS IoT Analytics Kanal, von dem Ihre Pipeline Nachrichten liest.

   c. Geben Sie die Ausgabe Ihrer Pipeline an. Dies ist der Datenspeicher, in dem Ihre verarbeiteten Nachrichtendaten gespeichert werden.

   d. (Optional) Fügen Sie für Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrer Pipeline hinzu.

   e. Geben Sie auf der Seite Nachrichtenattribute ableiten einen Attributnamen und einen Beispielwert ein, wählen Sie einen Datentyp aus der Liste aus, und klicken Sie dann auf Attribut hinzufügen.

   f. Wiederholen Sie den vorherigen Schritt für so viele Attribute, wie Sie benötigen, und wählen Sie dann Weiter.

   g. Sie werden derzeit keine Pipeline-Aktivitäten hinzufügen. Wählen Sie auf der Seite „Nachrichten anreichern, transformieren und filtern“ die Option Weiter.
4. Überprüfen Sie Ihre Auswahl und wählen Sie dann Pipeline erstellen.
5. Stellen Sie sicher, dass Ihre neue Pipeline auf der Seite Pipelines angezeigt wird.

> **Note**
>
> Sie habenAWS IoT Analytics Ressourcen erstellt, sodass sie Folgendes tun können:
>
> - Erfassen Sie rohe, unverarbeitete Nachrichtendaten von IoT-Geräten mit einem Kanal.
> - Speichern Sie die Nachrichtendaten Ihres IoT-Geräts in einem Datenspeicher.
> - Bereinigen, filtern, transformieren und reichern Sie Ihre Daten mit einer Pipeline an.

Als Nächstes erstellen Sie einenAWS IoT Analytics SQL-Datensatz, um nützliche Erkenntnisse über Ihr IoT-Gerät zu erhalten.

Erstellen Sie ein Dataset

> **Note**
>
> Ein Datensatz ist in der Regel eine Sammlung von Daten, die in tabellarischer Form organisiert sein können oder auch nicht. Im Gegensatz dazuAWS IoT Analytics erstellt Ihr Dataset, indem Sie eine SQL-Abfrage auf Daten in Ihrem Datenspeicher anwenden.

Sie haben jetzt einen Kanal, der unformatierte Nachrichtendaten an eine Pipeline weiterleitet, die Daten in einem Datenspeicher speichert, wo sie abgefragt werden können. Um die Daten abzufragen, erstellen Sie einen Datensatz. Eine Datenmenge enthält SQL-Anweisungen und Ausdrücke, mit denen Sie den Datenspeicher abfragen, sowie einen optionalen Zeitplan, der die Abfrage an einem von Ihnen angegebenen Tag und zu einer von Ihnen angegebenen Uhrzeit wiederholt. Sie können Ausdrücke verwenden, die den CloudWatch Amazon-Zeitplanausdrücken ähneln, um die optionalen Zeitpläne zu erstellen.

So erstellen Sie ein Dataset

1. Wählen Sie in https://console.aws.amazon.com/iotanalytics/ im linken Navigationsbereich Datasets aus.
2. Wählen Sie auf der Seite Datensatz erstellen die Option Create SQL aus.
3. Geben Sie auf der Seite „Datensatzdetails angeben“ die Details Ihres Datensatzes an.
   a. Geben Sie einen Namen für Ihren Dataset ein.
   b. Wählen Sie für Datenspeicherquelle die eindeutige ID aus, die den Datenspeicher identifiziert, den Sie zuvor erstellt haben.
   c. (Optional) Fügen Sie für Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Dataset hinzu.
4. Verwenden Sie SQL-Ausdrücke, um Ihre Daten abzufragen und analytische Fragen zu beantworten. Die Ergebnisse Ihrer Anfrage werden in diesem Datensatz gespeichert.

a. Geben Sie im Feld Autorenabfrage eine SQL-Abfrage ein, die einen Platzhalter verwendet, um bis zu fünf Datenzeilen anzuzeigen.

```
SELECT * FROM my_data_store LIMIT 5
```

Weitere Hinweise zur unterstützten SQL-Funktionalität finden Sie unterSQL-Ausdrücke inAWS IoT Analytics.AWS IoT Analytics

b. Sie können Testabfrage wählen, um zu überprüfen, ob Ihre Eingabe korrekt ist, und die Ergebnisse in einer Tabelle nach der Abfrage anzuzeigen.

> **Note**
>
> - An dieser Stelle des Tutorials ist Ihr Datenspeicher möglicherweise leer. Wenn Sie eine SQL-Abfrage in einem leeren Datenspeicher ausführen, werden keine Ergebnisse zurückgegeben, sodass Sie möglicherweise nur sehen`__dt`.
> - Sie müssen darauf achten, Ihre SQL-Abfrage auf eine angemessene Größe zu beschränken, damit sie nicht über einen längeren Zeitraum ausgeführt wird, da Athena die maximale Anzahl der laufenden Abfragen begrenzt. Aus diesem Grund müssen Sie darauf achten, die SQL-Abfrage auf eine angemessene Größe zu beschränken.
>
>   Wir empfehlen, während des Testens eine`LIMIT` Klausel in Ihrer Abfrage zu verwenden. Nach erfolgreichem Test können Sie diese Klausel entfernen.

5. (Optional) Wenn Sie Datensatzinhalte mithilfe von Daten aus einem bestimmten Zeitraum erstellen, kommen einige Daten möglicherweise nicht rechtzeitig zur Verarbeitung an. Um eine Verzögerung zu berücksichtigen, können Sie einen Offset oder Delta angeben. Weitere Informationen finden Sie unter Verspätete Datenbenachrichtigungen über Amazon CloudWatch Events erhalten.

   Sie werden an dieser Stelle keinen Datenauswahlfilter konfigurieren. Wählen Sie auf der Seite „Datenauswahlfilter konfigurieren“ die Option Weiter.

6. (Optional) Sie können diese Abfrage so planen, dass sie regelmäßig ausgeführt wird, um den Datensatz zu aktualisieren. Datensatzpläne können jederzeit erstellt und bearbeitet werden.

Zu diesem Zeitpunkt planen Sie keine wiederkehrende Ausführung der Abfrage. Wählen Sie daher auf der Seite Abfragezeitplan festlegen die Option Weiter aus.

7. AWS IoT Analyticserstellt Versionen dieses Datensatzinhalts und speichert Ihre Analyseergebnisse für den angegebenen Zeitraum. Wir empfehlen 90 Tage, Sie können sich jedoch dafür entscheiden, Ihre benutzerdefinierte Aufbewahrungsrichtlinie festzulegen. Sie können auch die Anzahl der gespeicherten Versionen Ihres Datensatzinhalts einschränken.

   Sie können den standardmäßigen Aufbewahrungszeitraum für Datensätze auf Unbestimmt festlegen und die Versionierung deaktiviert lassen. Wählen Sie auf der Seite „Die Ergebnisse Ihrer Analysen konfigurieren“ die Option Weiter aus.

8. (Optional) Sie können die Übermittlungsregeln Ihrer Datensatzergebnisse an ein bestimmtes Ziel konfigurieren, z.AWS IoT Events B.

   Sie werden Ihre Ergebnisse an keiner anderen Stelle in diesem Tutorial bereitstellen. Wählen Sie daher auf der Seite „Regeln für die Bereitstellung von Datensatzinhalten konfigurieren“ die Option Weiter aus.

9. Überprüfen Sie Ihre Auswahl und wählen Sie dann Datensatz erstellen.

10. Vergewissern Sie sich, dass Ihr neuer Datensatz auf der Seite Datensätze angezeigt wird.

Nachrichtendaten senden mitAWS IoT

Wenn Sie einen Kanal haben, der Daten an eine Pipeline weiterleitet, die Daten in einem Datenspeicher speichert, wo sie abgefragt werden können, sind Sie bereit, IoT-Gerätedaten zu sendenAWS IoT Analytics. Sie können Daten senden,AWS IoT Analytics indem Sie die folgenden Optionen verwenden:

- Verwenden Sie denAWS IoT Message Broker.
- Verwenden Sie denAWS IoT Analytics BatchPutMessageAPI-Vorgang.

In den folgenden Schritten senden Sie Nachrichtendaten vomAWS IoT Message Broker in derAWS IoT Core Konsole, damit dieser diese Daten aufnehmenAWS IoT Analytics kann.

> **Note**
>
> Beachten Sie beim Erstellen von Themennamen für Ihre Nachrichten:

- Bei den Namen von Themen wird Groß- und Kleinschreibung nicht beachtet. Felder, die benannt sind`example` und sich`EXAMPLE` in derselben Payload befinden, werden als Duplikate betrachtet.
- Themennamen können nicht mit dem$ Charakter beginnen. Themen, die mit beginnen,$ sind reservierte Themen und können nur von verwendet werdenAWS IoT.
- Geben Sie in Ihren Themennamen keine personenbezogenen Daten an, da diese Informationen in unverschlüsselten Mitteilungen und Berichten vorkommen können.
- AWS IoT Corekann keine Nachrichten zwischenAWS Konten oderAWS Regionen senden.

Um Nachrichtendaten zu senden mitAWS IoT

1. Melden Sie sich an der AWS IoT-Konsole an.
2. Wählen Sie im Navigationsbereich Test und dann MQTT-Testclient aus.
3. Wählen Sie auf der Seite des MQTT-Testclients die Option Zu einem Thema veröffentlichen.
4. Geben Sie als Themenname einen Namen ein, der dem Themenfilter entspricht, den Sie bei der Erstellung eines Kanals eingegeben haben. Dieses Beispiel verwendet `update/environment/dht1`.
5. Geben Sie für Message payload den folgenden JSON-Inhalt ein.

   ```
   {
     "thingid": "dht1",
     "temperature": 26,
     "humidity": 29,
     "datetime": "2018-01-26T07:06:01"
   }
   ```

6. (Optional) Wählen Sie Konfiguration hinzufügen, um zusätzliche Nachrichtenprotokolloptionen zu erhalten.
7. Wählen Sie Publish.

   Dadurch wird eine Nachricht veröffentlicht, die von deinem Kanal erfasst wird. Ihre Pipeline leitet die Nachricht dann an Ihren Datenspeicher weiter.

Überprüfen Sie den Fortschritt derAWS IoT Nachrichten

Du kannst überprüfen, ob Nachrichten in deinen Kanal aufgenommen werden, indem du diesen Schritten folgst.

Um den Fortschritt derAWS IoT Nachrichten zu überprüfen

1. Melden Sie sich unter diesem Link an: https://console.aws.amazon.com/iotanalytics/.
2. Wählen Sie im Navigationsbereich Kanäle und dann den Namen des Channels aus, den Sie zuvor erstellt haben.
3. Scrollen Sie auf der Detailseite des Kanals nach unten zum Abschnitt Überwachung und passen Sie dann den angezeigten Zeitrahmen an (1h 3h 12h 1d 3d 1w). Wählen Sie einen Wert wie 1w, um die Daten der letzten Woche anzuzeigen.

Sie können eine ähnliche Funktion verwenden, um die Laufzeit und Fehler der Pipeline-Aktivität auf der Detailseite der Pipeline zu überwachen. In diesem Tutorial haben Sie keine Aktivitäten als Teil der Pipeline angegeben, daher sollten keine Laufzeitfehler auftreten.

Um die Pipeline-Aktivität zu überwachen

1. Wählen Sie im Navigationsbereich Pipelines und dann den Namen der Pipeline aus, die Sie zuvor erstellt haben.
2. Scrollen Sie auf der Detailseite der Pipeline nach unten zum Abschnitt Überwachung und passen Sie dann den angezeigten Zeitrahmen an, indem Sie einen der Zeitrahmenindikatoren auswählen (1h 3h 12h 1d 3d 1w).

Zugriff auf Abfrageergebnisse

Der Inhalt des Datensatzes ist eine Datei, die das Ergebnis Ihrer Anfrage im CSV-Format enthält.

1. Wählen Sie in der linken Navigationsleiste von https://console.aws.amazon.com/iotanalytics/ Dataset aus.
2. Wählen Sie auf der Seite Datensätze den Namen des Datasets aus, das Sie zuvor erstellt haben.
3. Wählen Sie auf der Dataset -Informationsseite in der oberen rechten Ecke die Option Ausführen aus.

4. Um zu überprüfen, ob der Datensatz bereit ist, suchen Sie unter dem Datensatz nach einer Meldung ähnlich wie Sie haben die Abfrage für Ihren Datensatz erfolgreich gestartet. Die Registerkarte „Inhalt des Datensatzes“ enthält die Abfrageergebnisse und zeigt „Erfolgreich“ an.
5. Um eine Vorschau der Ergebnisse Ihrer erfolgreichen Abfrage anzuzeigen, wählen Sie auf der Registerkarte Datensatzinhalt den Abfragenamen aus. Um die CSV-Datei mit den Abfrageergebnissen anzuzeigen oder zu speichern, wählen Sie Herunterladen.

> **Note**
>
> AWS IoT Analyticskann den HTML-Teil eines Jupyter-Notizbuchs auf der Inhaltsseite des Datensatzes einbetten. Weitere Informationen finden Sie unter VisualisierenAWS IoT AnalyticsDaten mit der Konsole.

Ihre Daten erkunden

Sie haben mehrere Möglichkeiten, Ihre Daten zu speichern, zu analysieren und zu visualisieren.

Amazon Simple Storage Service

Sie können Datensatzinhalte an einen Amazon S3 S3-Bucket senden und so die Integration mit Ihren vorhandenen Data Lakes oder den Zugriff über interne Anwendungen und Visualisierungstools ermöglichen. Sehen Sie sich das Feld`contentDeliveryRules::destination::s3DestinationConfiguration` in der CreateDatasetOperation an.

AWS IoT Events

Sie können Dataset als Eingabe an einen Dienst sendenAWS IoT Events, mit dem Sie Geräte oder Prozesse auf Fehler oder Änderungen im Betrieb sowie für das Auslösen von Aktionen, wenn solche Ereignisse auftreten.

Erstellen Sie dazu mithilfe der CreateDatasetOperation einen Datensatz und geben Sie eineAWS IoT Events Eingabe in das Feld an`contentDeliveryRules :: destination :: iotEventsDestinationConfiguration :: inputName`. Sie müssen auch die Rolle`roleArn` einer Rolle angeben, dieAWS IoT Analytics Ausführungsberechtigungen gewährt`iotevents:BatchPutMessage`. Jedes Mal, wenn der Inhalt des Datensatzes erstelltAWS IoT Analytics wird, wird jeder Inhaltseintrag des Datensatzes als Nachricht an die

angegebeneAWS IoT Events Eingabe gesendet. Beispiel: Ihr Dataset enthält den folgenden Inhalt.

```
"what","who","dt"
"overflow","sensor01","2019-09-16 09:04:00.000"
"overflow","sensor02","2019-09-16 09:07:00.000"
"underflow","sensor01","2019-09-16 11:09:00.000"
...
```

AWS IoT AnalyticsSendet dann Nachrichten, die Felder wie die folgenden enthalten.

```
{ "what": "overflow", "who": "sensor01", "dt": "2019-09-16 09:04:00.000" }
```

```
{ "what": "overflow", "who": "sensor02", "dt": "2019-09-16 09:07:00.000" }
```

Sie sollten eineAWS IoT Events Eingabe erstellen, die die Felder erkennt, an denen Sie interessiert sind (eines oder mehrere von`what`,`dt`)`who`, und einAWS IoT Events Detektormodell erstellen, das diese Eingabefelder in Ereignissen verwendet, um Aktionen auszulösen oder interne Variablen festzulegen.

Jupyter Notebook

Jupyter Notebook ist eine Open-Source-Lösung für die Verwendung von Skriptsprachen für die Ad-hoc-Datenexploration und erweiterte Analysen. Sie können tiefer eintauchen und komplexere Analysen anwenden und Methoden des maschinellen Lernens wie K-Means-Clustering und Regressionsmodelle zur Vorhersage auf Ihre IoT-Gerätedaten anwenden.

AWS IoT Analyticsverwendet SageMaker Amazon-Notebook-Instances, um seine Jupyter Notebooks zu hosten. Bevor Sie eine Notebook-Instance erstellen, müssen Sie eine Beziehung zwischenAWS IoT Analytics und Amazon erstellen SageMaker:

1. Navigieren Sie zur SageMaker Konsole und erstellen Sie eine Notebook-Instanz:
   a. Tragen Sie die Details ein und wählen Sie dann Create a new Role (Eine neue Rolle erstellen). Notieren Sie sich den ARN der Rolle.
   b. Erstellen Sie eine Notebook-Instance.
2. Gehen Sie zur IAM-Konsole und ändern Sie die SageMaker Rolle:

a. Öffnen Sie die Rolle. Sie sollte eine verwaltete Richtlinie enthalten.

b. Wählen Sie Inline-Richtlinie hinzufügen und dann für Service die Option IoTAnalytics aus. Wählen Sie Aktionen auswählen aus, geben Sie dann**`GetDatasetContent`** in das Suchfeld ein und wählen Sie sie aus. Wählen Sie Review policy (Richtlinie überprüfen) aus.

c. Überprüfen Sie die Richtlinie auf Richtigkeit, geben Sie einen Namen ein und wählen Sie dann Richtlinie erstellen aus.

Dadurch erhält die neu erstellte Rolle die Berechtigung, einen Datensatz zu lesenAWS IoT Analytics.

1. Kehren Sie zu https://console.aws.amazon.com/iotanalytics/ zurück und wählen Sie im linken Navigationsbereich Notebooks aus. Wählen Sie auf der Seite Notizbücher die Option Notizbuch erstellen aus.
2. Wählen Sie auf der Seite „Vorlage auswählen“ die Option IoTA Blank Template aus.
3. Geben Sie auf der Seite Notizbuch einrichten einen Namen für Ihr Notizbuch ein. Wählen Sie unter Datensatzquelle auswählen den Datensatz aus, den Sie zuvor erstellt haben, und wählen Sie ihn dann aus. Wählen Sie unter Notebook-Instanz auswählen die Notebook-Instance aus, in der Sie sie erstellt haben SageMaker.
4. Nachdem Sie Ihre Auswahl überprüft haben, wählen Sie Notizbuch erstellen.
5. Auf der Seite Notebooks wird Ihre Notebook-Instance in der SageMakerAmazon-Konsole geöffnet.

Notizbuch-Vorlagen

DieAWS IoT Analytics Notizbuchvorlagen enthaltenAWS verfasste Modelle und Visualisierungen für maschinelles Lernen, die Ihnen den Einstieg inAWS IoT Analytics Anwendungsfälle erleichtern. Sie können diese Notizbuchvorlagen verwenden, um mehr zu erfahren, oder sie wiederverwenden, um sie an Ihre IoT-Gerätedaten anzupassen und einen sofortigen Mehrwert zu erzielen.

In derAWS IoT Analytics Konsole finden Sie die folgenden Notizbuchvorlagen:

- Erkennung kontextueller Anomalien — Anwendung der Erkennung kontextueller Anomalien bei der gemessenen Windgeschwindigkeit mit einem Modell des exponentiell gewichteten gleitenden Durchschnitts (PEWMA) von Poisson.

- Prognose der Leistung von Solarmodulen — Anwendung von stückweisen, saisonalen und linearen Zeitreihenmodellen zur Vorhersage der Leistung von Solarmodulen.
- Prädiktive Wartung von Düsentriebwerken — Anwendung multivariater neuronaler Netze mit langem Kurzzeitgedächtnis (LSTM) und logistischer Regression zur Vorhersage von Triebwerksausfällen.
- Segmentierung von Smart-Home-Kunden — Anwendung von K-Means- und Principal Component Analysis (PCA) -Analysen zur Erkennung verschiedener Kundensegmente in Daten zur Smart-Home-Nutzung.
- Intelligente Stauprognose — Anwendung von LSTM zur Vorhersage der Nutzungsraten von Stadtautobahnen.
- Intelligente Luftqualitätsprognose für Städte — Anwendung von LSTM zur Vorhersage der Partikelbelastung in Stadtzentren.

Erste Schritte mit AWS IoT Analytics

In diesem Abschnitt werden die grundlegenden Befehle beschrieben, mit denen Sie Ihre Gerätedaten sammeln, speichern, verarbeiten und abfragenAWS IoT Analytics. Die hier gezeigten Beispiele verwenden dasAWS Command Line Interface (AWS CLI). Weitere Informationen zumAWS CLI finden Sie im AWS Command Line InterfaceBenutzerhandbuch. Weitere Informationen zu den verfügbaren CLI-Befehlen finden Sie unter iot in der AWS Command Line InterfaceReferenz.AWS IoT

Important

Verwenden Sie den`aws iotanalytics` Befehl, umAWS IoT Analytics mit dem zu interagierenAWS CLI. Verwenden Sie den`aws iot` Befehl, um mit anderen Teilen des IoT-Systems zu interagieren, indem Sie die verwendenAWS CLI.

Note

Beachten Sie bei der Eingabe der Namen vonAWS IoT Analytics Entitäten (Kanal, Datensatz, Datenspeicher und Pipeline) in den folgenden Beispielen, dass alle von Ihnen verwendeten Großbuchstaben vom System automatisch in Kleinbuchstaben geändert werden. Die Namen von Entitäten müssen mit einem Kleinbuchstaben beginnen und nur Kleinbuchstaben, Unterstriche und Ziffern enthalten.

Erstellen eines Channels

Ein Kanal erfasst und archiviert unverarbeitete Nachrichten-Rohdaten, bevor diese Daten in einer Pipeline veröffentlicht werden. Eingehende Nachrichten werden an einen Kanal gesendet. Der erste Schritt besteht also darin, einen Kanal für Ihre Daten zu erstellen.

```
aws iotanalytics create-channel --channel-name mychannel
```

Wenn Sie möchten, dassAWS IoT Nachrichten aufgenommen werdenAWS IoT Analytics, können Sie eineAWS IoT Rules Engine-Regel erstellen, um die Nachrichten an diesen Kanal zu senden. Dies wird später in gezeigtErfassen von Daten in AWS IoT Analytics. Eine andere Möglichkeit, die Daten in einen Kanal zu übertragen, besteht darin, denAWS IoT Analytics Befehl zu verwenden`BatchPutMessage`.

So listen Sie die Kanäle auf, die Sie bereits erstellt haben:

```
aws iotanalytics list-channels
```

Um weitere Informationen zu einem Channel anzuzeigen.

```
aws iotanalytics describe-channel --channel-name mychannel
```

Unverarbeitete Kanalnachrichten werden in einem von Ihnen verwalteten oder vonAWS IoT Analytics Ihnen verwalteten Amazon-S3-Bucket gespeichert. Legen Sie die Speichermethode mit dem Parameter `channelStorage` fest. Standardmäßig wird ein serviceverwalteter Amazon S3-Bucket verwendet. Wenn Sie sich dafür entscheiden, Kanalnachrichten in einem von Ihnen verwalteten Amazon S3 S3-Bucket zu speichern, müssen Sie dieAWS IoT Analytics Erlaubnis erteilen, diese Aktionen in Ihrem Namen auf Ihrem Amazon S3 S3-Bucket auszuführen:`s3:GetBucketLocation` (Bucket-Standort überprüfen)`s3:PutObject` (speichern),`s3:GetObject` (lesen),`s3:ListBucket` (erneut verarbeiten).

Example

```
{
    "Version": "2012-10-17",
    "Id": "MyPolicyID",
    "Statement": [
        {
            "Sid": "MyStatementSid",
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::my-iot-analytics-bucket",
                "arn:aws:s3:::my-iot-analytics-bucket/*"
            ]
        }
    ]
```

```
}
```

Wenn Sie Änderungen an den Optionen oder Berechtigungen Ihres vom Kunden verwalteten Kanalspeichers vornehmen, müssen Sie möglicherweise Kanaldaten erneut verarbeiten, um sicherzustellen, dass zuvor aufgenommene Daten in den Datensatzinhalten enthalten sind. Siehe Wiederverarbeitung von Kanaldaten.

Einen Datenspeicher erstellen

Ein Datenspeicher empfängt und speichert Ihre Nachrichten. Es ist keine Datenbank, sondern ein skalierbares und abfragbares Repository Ihrer Nachrichten. Sie können mehrere Datenspeicher erstellen, um Nachrichten zu speichern, die von verschiedenen Geräten oder Standorten stammen, oder Sie können einen einzigen Datenspeicher verwenden, um alle IhreAWS IoT Nachrichten zu empfangen.

```
aws iotanalytics create-datastore --datastore-name mydatastore
```

Um die Datenspeicher aufzulisten, die Sie bereits erstellt haben.

```
aws iotanalytics list-datastores
```

Um weitere Informationen zu einem Datastore anzuzeigen.

```
aws iotanalytics describe-datastore --datastore-name mydatastore
```

Amazon S3 S3-Richtlinien fürAWS IoT AnalyticsRessourcen

Sie können verarbeitete Data Store-Nachrichten in einem Amazon S3 S3-Bucket speichern, das vonAWS IoT Analyticsoder in einem, das du verwaltest. Wenn Sie einen Data Store erstellen, wählen Sie den gewünschten Amazon S3 S3-Bucket mithilfe der`datastoreStorage`API-Parameter. Standardmäßig wird ein serviceverwalteter Amazon S3-Bucket verwendet.

Wenn Sie Data Store-Nachrichten in einem von Ihnen verwalteten Amazon S3 S3-Bucket speichern möchten, müssen SieAWS IoT Analytics-Berechtigung, diese Aktionen in Ihrem Amazon S3 S3-Bucket für Sie auszuführen:

- `s3:GetBucketLocation`

- `s3:PutObject`
- `s3:DeleteObject`

Wenn Sie den Datenspeicher als Quelle für ein SQL-Abfrage-Dataset verwenden, richten Sie eine Amazon S3 S3-Bucket-Richtlinie ein, die Folgendes gewährt:AWS IoT AnalyticsBerechtigung zum Aufrufen von Amazon Athena Athena-Abfragen für den Inhalt Ihres Buckets.

> **Note**
>
> Wir empfehlen Ihnen, zu spezifizierenaws:SourceArnin Ihrer Bucket-Richtlinie, um das Sicherheitsproblem des Confused Deputy zu vermeiden. Dies schränkt den Zugriff ein, indem nur die Anfragen zugelassen werden, die von einem bestimmten Konto stammen. Weitere Informationen zu dem Confused Deputy finden Sie unterthe section called "Dienstübergreifende Confused-Deputy-Prävention".

Es folgt ein Beispiel für eine Bucket-Richtlinie, die diese erforderlichen Berechtigungen erteilt.

```
{
    "Version": "2012-10-17",
    "Id": "MyPolicyID",
    "Statement": [
        {
            "Sid": "MyStatementSid",
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
```

```
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:iotanalytics:us-east-1:123456789012:dataset/DOC-
EXAMPLE-DATASET",
                        "arn:aws:iotanalytics:us-east-1:123456789012:datastore/DOC-
EXAMPLE-DATASTORE"
                    ]
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unterKontenübergreifender Zugriffin derAmazon-Athena-Benutzerhandbuch.

> **Note**
>
> Wenn Sie die Optionen oder Berechtigungen Ihres vom Kunden verwalteten Datenspeichers aktualisieren, müssen Sie möglicherweise Kanaldaten erneut verarbeiten, um sicherzustellen, dass alle zuvor aufgenommenen Daten in den Datensatzinhalten enthalten sind. Weitere Informationen finden Sie unterKanaldaten erneut verarbeiten.

Dateiformate

AWS IoT AnalyticsDatastores unterstützen derzeit JSON- und Parquet -Dateiformate. JSON ist das Standarddateiformat.

- JSON (JavaScript Object Notation)- Ein Textformat, das Name-Wert-Paare und geordnete Wertelisten unterstützt.
- Apache Parquet- Ein säulenares Speicherformat, das zur effizienten Speicherung und Abfrage großer Datenmengen verwendet wird.

So konfigurieren Sie das Dateiformat derAWS IoT AnalyticsDatenspeicher können Sie den`FileFormatConfiguration`-Objekt, wenn Sie den Datenspeicher erstellen.

`fileFormatConfiguration`

Enthält die Konfigurationsinformationen von Dateiformaten.AWS IoT AnalyticsDatastores unterstützen JSON und Parquet.

JSON ist das Standarddateiformat. Sie können nur ein Format angeben. Sie können das Dateiformat nicht ändern, nachdem Sie den Datenspeicher erstellt haben.

`jsonConfiguration`

Enthält die Konfigurationsinformationen des JSON-Formats.

`parquetConfiguration`

Enthält die Konfigurationsinformationen des Parquet-Formats.

`schemaDefinition`

Informationen, die zur Definition eines Schemas benötigt werden.

`columns`

Gibt eine oder mehrere Spalten an, in denen Ihre Daten gespeichert sind.

Jedes Schema kann bis zu 100 Spalten enthalten. Jede Spalte kann bis zu 100 verschachtelte Typen enthalten.

`name`

Der Name der Spalte.

Längenabhängigkeiten: 1-255 Zeichen.

`type`

Die Art der Daten. Weitere Informationen zu dem unterstützten Datentyp finden Sie unterGängige DatentypenimAWS GlueEntwicklerhandbuchaus.

Längenbeschränkungen: 1-131072 Zeichen.

AWS IoT Analyticsunterstützt alle Datentypen, die auf derDatentypen in Amazon AthenaSeite, außer für`DECIMAL(`*`precision`*`, `*`scale`*`)-`*`precision`*aus.

Erstellen eines Datenspeichers (Konsole)

Die folgende Anleitung zeigt, wie Sie einen Datenspeicher erstellen, der Daten im Parquet -Format speichert.

So erstellen Sie einen Datenspeicher

1. Melden Sie sich beim anhttps://console.aws.amazon.com/iotanalytics/aus.
2. Klicken Sie im Navigationsbereich aufDatastoresaus.
3. Auf derDatastores-Seite wählenDatenspeicher erstellenaus.
4. Auf derGeben Sie Datenspeicherdetails angeben Sie grundlegende Informationen zu Ihrem Datenspeicher ein.

   a. FürID des DatenspeichersGeben Sie eine eindeutige Datenspeicher-ID ein. Sie können diese ID nicht ändern, nachdem Sie sie erstellt haben.

   b. (Optional) FürTags, wählenNeues Tag hinzufügenum ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Datenspeicher hinzuzufügen. Tags können Ihnen helfen, Ihre -Ressourcen zu identifizieren, für die Sie erstellenAWS IoT Analyticsaus.

   c. Wählen Sie Next (Weiter).
5. Auf derKonfigurieren des Speichertypsgeben Sie an, wie Ihre Daten gespeichert werden sollen.

   a. FürSpeichertyp, wählenService verwalteter Speicheraus.

   b. FürKonfigurieren Sie, wie lange Sie Ihre verarbeiteten Daten speichern möchten, wählenAuf unbestimmte Zeitaus.

   c. Wählen Sie Next (Weiter).
6. Auf derDatenformat konfigurierendefinieren Sie die Struktur und das Format Ihrer Datensätze.

   a. FürKlassifizierung, wählenParquetaus. Sie können dieses Format nicht ändern, nachdem Sie den Datenspeicher erstellt haben.

   b. FürInferenzquelle, wählenJSON-Zeichenfolgefür Ihren Datenspeicher.

   c. FürZeichenfolgeGeben Sie Ihr Schema im JSON-Format ein, z. B. im folgenden Beispiel.

   ```
   {
       "device_id": "0001",
       "temperature": 26,
       "humidity": 29,
       "datetime": "2018-01-26T07:06:01"
   }
   ```

   d. Klicken Sie aufSchema ableitenaus.

e. UNDERKonfigurieren des Parquet-, bestätigen Sie, dass das Format Ihrem JSON-Beispiel entspricht. Wenn das Format nicht übereinstimmt, aktualisieren Sie das Parkett-Schema manuell.

- Wenn Sie möchten, dass Ihr Schema mehr Spalten anzeigen soll, wählen SieFügen Sie neue Spalte hinzuGeben Sie einen Spaltennamen ein und wählen Sie dann den Datentyp aus.

> **Note**
>
> Standardmäßig können Sie 100 Spalten für Ihr Schema haben. Weitere Informationen finden Sie unter AWS IoT Analytics-Kontingente.

- Sie können den Datentyp für eine vorhandene Spalte ändern. Weitere Informationen zu den unterstützten Datentypen finden Sie unterGängige DatentypenimAWS GlueEntwicklerhandbuchaus.

> **Note**
>
> Nachdem Sie Ihren Datenspeicher erstellt haben, können Sie den Datentyp für eine vorhandene Spalte nicht mehr ändern.

- Um eine vorhandene Spalte zu entfernen, wählen SieSpalte entfernenaus.

f. Wählen Sie Next (Weiter).

7. (Optional)AWS IoT Analyticsunterstützt benutzerdefinierte Partitionen in Ihrem Datenspeicher, sodass Sie beschnittete Daten abfragen können, um die Latenz zu verbessern. Weitere Informationen zu unterstützten benutzerdefinierten Partitionen finden Sie unterBenutzerdefinierte Partitionenaus.

   Wählen Sie Next (Weiter).

8. Auf derÜberprüfen und erstellenÜberprüfen Sie Ihre Auswahl und wählen Sie dannDatenspeicher erstellenaus.

> **Important**
>
> Sie können die Datenspeicher-ID, das Dateiformat oder den Datentyp für eine Spalte nicht ändern, nachdem Sie den Datenspeicher erstellt haben.

9. Stellen Sie sicher, dass Ihr neuer Datenspeicher auf derDatastoresangezeigten.

Benutzerdefinierte Partitionen

AWS IoT Analyticsunterstützt die Datenpartitionierung, damit Sie die Daten in Ihrem Datenspeicher organisieren können. Wenn Sie Datenpartitionierung zum Organisieren von Daten verwenden, können Sie beschnittene Daten abfragen. Dies verringert die pro Abfrage gescannte Datenmenge und verbessert die Latenz.

Sie können Ihre Daten nach Nachrichtendatenattributen oder Attributen partitionieren, die durch Pipeline-Aktivitäten hinzugefügt wurden.

Aktivieren Sie zunächst die Datenpartitionierung in einem Datenspeicher. Geben Sie eine oder mehrere Datenpartitionsdimensionen an und verbinden Sie Ihren partitionierten Datenspeicher mit einemAWS IoT AnalyticsPipeline. Schreiben Sie dann Abfragen, die die`WHERE`-Klausel zur Optimierung der Leistung.

Erstellen eines Datenspeichers (Konsole)

Das folgende Verfahren zeigt, wie Sie einen Datenspeicher mit einer benutzerdefinierten Partition erstellen.

So erstellen Sie einen Datenspeicher

1. Melden Sie sich an der AWS IoT Analytics-Konsole an.
2. Wählen Sie im Navigationsbereich und dann ausDatastoresaus.
3. Auf derDatastores-Seite, wählen SieErstellen eines Datenspeichersaus.
4. Auf derGeben Sie die Datenspeicherdetailsgeben Sie grundlegende Informationen zu Ihrem Datenspeicher ein.

    a. FürDatenspeicher-IDGeben Sie eine eindeutige Datenspeicher-ID ein. Sie können diese ID nicht ändern, nachdem Sie sie erstellt haben.

    b. (Optional) FürTags, wählenNeues Tag hinzufügenum Ihrem Datenspeicher ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) hinzuzufügen. Tags können Ihnen helfen, Ressourcen zu identifizieren, für die Sie erstellenAWS IoT Analyticsaus.

    c. Wählen Sie Next (Weiter).
5. Auf derKonfigurieren des Speichertypsgeben Sie an, wie Ihre Daten gespeichert werden sollen.

a. FürSpeichertyp, wählenService verwalteter Speicheraus.

b. FürKonfigurieren Sie, wie lange Sie Ihre verarbeiteten Daten speichern möchten, wählenAuf unbestimmte Zeitaus.

c. Wählen Sie Next (Weiter).

6. Auf derKonfigurieren des Datenformatsdefinieren Sie die Struktur und das Format Ihrer Datensätze.

a. Für Ihr Datenspeicher-DatenformatKlassifizierung, wählenJSONoderParquetaus. Weitere Informationen zuAWS IoT Analyticsunterstützte Dateitypen finden Sie unterDateiformateaus.

> **Note**
>
> Sie können dieses Format nicht ändern, nachdem Sie den Datenspeicher erstellt haben.

b. Wählen Sie Next (Weiter).

7. Erstellen Sie benutzerdefinierte Partitionen für diesen Datenspeicher.

a. FürFügen Sie Datenpartitionen hinzu, WÄHLEN SIEAktivieren vonaus.

b. FürDatenpartitionsquelle, geben Sie grundlegende Informationen über die Quelle Ihrer Partition an.

Klicken Sie aufBeispiel für eine Quelle, und wählen SieAWS IoT AnalyticsKanal, der Nachrichten für diesen Datenspeicher sammelt.

c. FürAttribute für Nachrichtenbeispielewählen Sie die Nachrichtenattribute aus, die Sie zum Partitionieren Ihres Datenspeichers verwenden möchten. Fügen Sie dann Ihre Auswahl als Attribut-Partitionsdimensionen oder Timestamp-Partitionsdimensionen unterAktionenaus.

> **Note**
>
> Sie können Ihrem Datenspeicher nur eine Zeitstempelpartition hinzufügen.

d. FürBenutzerdefinierte Datenspeicher-PartitionsdimensionenDefinieren Sie grundlegende Informationen über Ihre Partitionsdimensionen. Jedes Nachrichtenbeispielattribut, das Sie im vorherigen Schritt ausgewählt haben, wird zu den Dimensionen Ihrer Partition. Passen Sie jede Dimension mit diesen Optionen an:

- Partitionstyp- Geben Sie an, ob diese Partitionsdimension eineAttribute (Attribut)oder einZeitstempelPartitionstyp.
- AttributnameundBemaßungsname- StandardmäßigAWS IoT Analyticsverwendet den Namen des Nachrichtenbeispielattributs, das Sie als Bezeichner für Ihre Attributpartitionsdimension ausgewählt haben. Bearbeiten Sie den Attributnamen, um den Namen Ihrer Partitionsdimension anzupassen. Sie können den Dimensionsnamen im`WHERE`-Klausel zur Optimierung der Abfrageleistung.
  - Dem Namen einer Partitionsattribut-Dimension wird das Präfix`__partition_`aus.
  - Für Zeitstempel-PartitionstypenAWS IoT Analyticserstellt die folgenden vier Dimensionen mit Namen`__year`,`__month`,`__day`,`__hour`aus.
- Bestellen- Ordnen Sie Ihre Partitionsdimensionen neu an, um die Latenz für Ihre Abfragen zu verbessern.

FürZeitstempelformat, geben Sie das Format Ihrer Zeitstempelpartition an, indem Sie den aufgenommenen Zeitstempel aus Ihren Nachrichtendaten abgleichen. Sie können eine vonAWS IoT Analyticslistet Formatoptionen auf, oder geben Sie eine an, die dem Format Ihrer Daten entspricht. Weitere Informationen zur AngabeFormatierer für Datumszeitaus.

Um eine neue Dimension hinzuzufügen, die kein Nachrichtenattribut ist, wählen SieFügen Sie neue Partitionen hinzuaus.

e. Wählen Sie Next (Weiter).

8. Auf derÜberprüfen und erstellen-Seite, überprüfen Sie Ihre Auswahl und wählen Sie dannErstellen eines Datenspeichersaus.

> **Important**
>
> - Sie können die Datenspeicher-ID nicht ändern, nachdem Sie den Datenspeicher erstellt haben.
> - Um vorhandene Partitionen zu bearbeiten, müssen Sie einen anderen Datenspeicher erstellen und die Daten über eine Pipeline erneut verarbeiten.

9. Stellen Sie sicher, dass Ihr neuer Datenspeicher auf derDatastoresangezeigten.

Erstellen einer Pipeline

Eine Pipeline nimmt Nachrichten aus einem Channel auf und ermöglicht Ihnen, die Nachrichten vor dem Speichern in einem Datastore zu verarbeiten und zu filtern. Um einen Kanal mit einem Datenspeicher zu verbinden, müssen Sie eine Pipeline erstellen. Die einfachste mögliche Pipeline enthält keine Aktivitäten außer die Angabe des Kanals, der die Daten erfasst, und die Identifikation des Datenspeichers, an den die Nachrichten gesendet werden. Informationen zu komplizierteren Pipelines finden Sie unter Pipeline-Aktivitäten.

Wir empfehlen, mit einer Pipeline zu beginnen, die nichts anderes tut, als einen Kanal mit einem Datenspeicher zu verbinden. Nachdem Sie dann bestätigt haben, dass Rohdaten in den Datenspeicher eingespeist werden, können Sie weitere Pipeline-Aktivitäten zur Verarbeitung dieser Daten einführen.

Führen Sie den folgenden Befehl aus, um eine Pipeline zu erstellen.

```
aws iotanalytics create-pipeline --cli-input-json file://mypipeline.json
```

Die`mypipeline.json` Datei enthält den folgenden Inhalt.

```
{
    "pipelineName": "mypipeline",
    "pipelineActivities": [
        {
            "channel": {
                "name": "mychannelactivity",
                "channelName": "mychannel",
                "next": "mystoreactivity"
            }
        },
        {
            "datastore": {
                "name": "mystoreactivity",
                "datastoreName": "mydatastore"
            }
        }
    ]
}
```

Führen Sie den folgenden Befehl aus, um Ihre vorhandenen Pipelines aufzulisten.

```
aws iotanalytics list-pipelines
```

Führen Sie den folgenden Befehl aus, um die Konfiguration einer einzelnen Pipeline anzuzeigen.

```
aws iotanalytics describe-pipeline  --pipeline-name mypipeline
```

Erfassen von Daten in AWS IoT Analytics

Wenn Sie über einen Kanal verfügen, der Daten an eine Pipeline weiterleitet, die Daten in einem Datenspeicher speichert, wo sie abgefragt werden können, können Sie Nachrichtendaten an diese sendenAWS IoT Analytics. Hier zeigen wir zwei Methoden, um Daten einzugebenAWS IoT Analytics. Sie können eine Nachricht mit demAWS IoT Message Broker senden oder dieAWS IoT Analytics`BatchPutMessage` API verwenden.

Themen

DenAWS IoT Message Broker verwenden

Um denAWS IoT Message Broker zu verwenden, erstellen Sie eine Regel mithilfe derAWS IoT Rules Engine. Die Regel leitet Nachrichten mit einem bestimmten Thema weiterAWS IoT Analytics. Zunächst müssen Sie für diese Regel jedoch eine Rolle erstellen, die die erforderlichen Berechtigungen gewährt.

Erstellen einer IAM-Rolle

UmAWS IoT Nachrichten an einenAWS IoT Analytics Channel weiterleiten zu lassen, richten Sie eine Regel ein. Zunächst müssen Sie jedoch eine IAM-Rolle erstellen, die dieser Regel die Berechtigung erteilt, Nachrichtendaten an einenAWS IoT Analytics Kanal zu senden.

Führen Sie den folgenden -Befehl aus, um die Rolle zu erstellen.

```
aws iam create-role --role-name myAnalyticsRole --assume-role-policy-document file://
arpd.json
```

Der Inhalt der`arpd.json` Datei sollte wie folgt aussehen.

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

Hängen Sie dann ein Richtliniendokument an die Rolle an.

```
aws iam put-role-policy --role-name myAnalyticsRole --policy-name myAnalyticsPolicy --
policy-document file://pd.json
```

Der Inhalt der`pd.json` Datei sollte wie folgt aussehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotanalytics:BatchPutMessage",
            "Resource": [
               "arn:aws:iotanalytics:us-west-2:your-account-number:channel/mychannel"
            ]
        }
    ]
}
```

EineAWS IoT Regel erstellen

Erstelle eineAWS IoT Regel, die Nachrichten an deinen Kanal sendet.

```
aws iot create-topic-rule --rule-name analyticsTestRule --topic-rule-payload file://
rule.json
```

Der Inhalt der`rule.json` Datei sollte wie folgt aussehen.

```
{
    "sql": "SELECT * FROM 'iot/test'",
    "ruleDisabled": false,
    "awsIotSqlVersion": "2016-03-23",
    "actions": [ {
        "iotAnalytics": {
            "channelName": "mychannel",
            "roleArn": "arn:aws:iam::your-account-number:role/myAnalyticsRole"
        }
    } ]
}
```

Ersetzen Sie `iot/test` durch das MQTT-Thema der Nachrichten, die weitergeleitet werden sollen. Ersetzen Sie den Kanalnamen und die Rolle durch die in den vorigen Abschnitten erstellten.

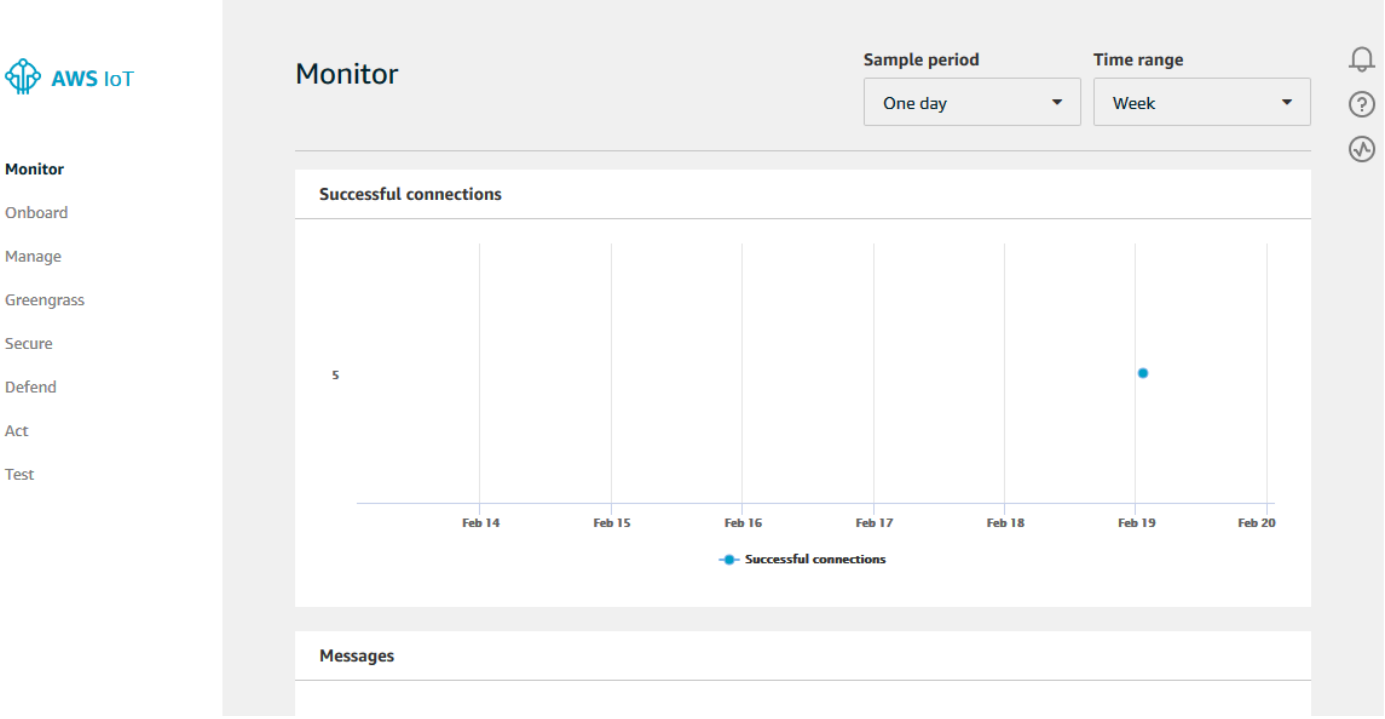
Senden von MQTT-Nachrichten anAWS IoT Analytics

Nachdem Sie eine Regel mit einem Channel, einen Channel mit einer Pipeline und eine Pipeline mit einem Datenspeicher verknüpft haben, werden alle Daten, die der Regel entsprechen, nunAWS IoT Analytics an den Datenspeicher weitergeleitet und können abgefragt werden. Um dies zu testen, können Sie dieAWS IoT Konsole verwenden, um eine Nachricht zu senden.

> **Note**
>
> Die Feldnamen der Nachrichten-Payloads (Daten), an die Sie sendenAWS IoT Analytics.
>
> - Dürfen nur alphanumerische Zeichen und Unterstriche (_) enthalten. Andere Sonderzeichen sind nicht zulässig.
> - Mit einem alphabetischen Zeichen oder einzelnen Unterstrich (_) beginnen müssen.
> - Keine Bindestriche (-) enthalten können.
> - In Begriffen mit regulären Ausdrücken: "`^[A-Za-z_]([A-Za-z0-9]*|[A-Za-z0-9][A-Za-z0-9_]*)$`“.
> - Darf nicht mehr als 255 Zeichen enthalten
> - Die Groß- und Kleinschreibung berücksichtigen. Felder, die benannt sind`foo` und sich`F00` in derselben Payload befinden, werden als Duplikate betrachtet.

Beispielsweise sind `{"temp_01": 29}` und `{"_temp_01": 29}` gültig, aber `{"temp-01": 29}`, `{"01_temp": 29}` und `{"__temp_01": 29}` sind ungültig in Nachrichtennutzlasten.

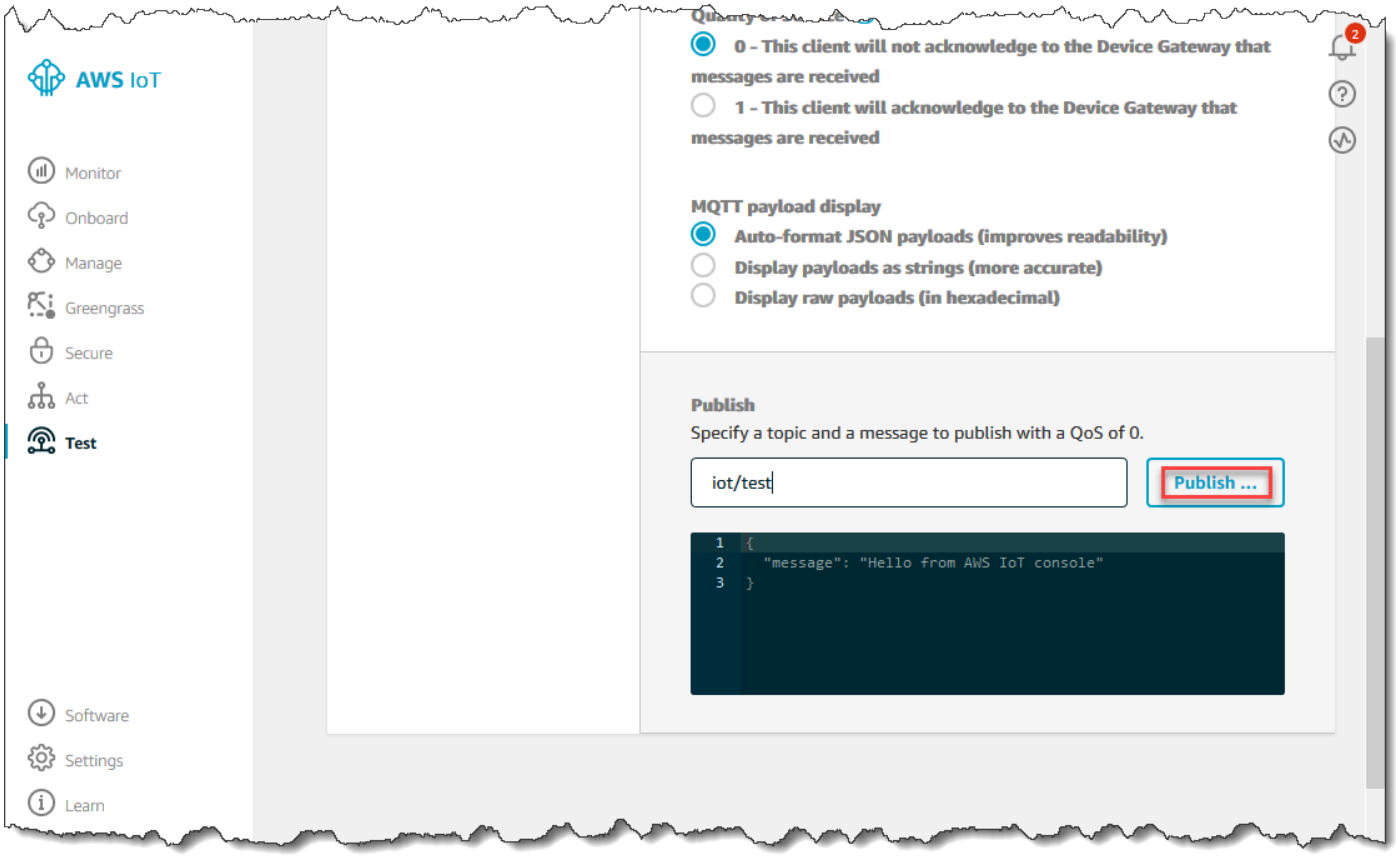
1. Wählen Sie in der AWS IoT-Konsole im linken Navigationsbereich die Option Test.



2. Geben Sie auf der Seite "MQTT client" im Abschnitt Publish unter Specify a topic die Zeichenfolge **`iot/test`** ein. Stellen Sie im Abschnitt Nachrichten-Payload sicher, dass die folgenden JSON-Inhalte vorhanden sind, oder geben Sie sie ein, falls nicht.

```
{
    "message": "Hello from the IoT console"
}
```

3. Wählen Sie Publish to topic (An Thema veröffentlichen).



Dadurch wird eine Nachricht veröffentlicht, die an den zuvor erstellten Datenspeicher weitergeleitet wird.

Die BatchPutMessage API verwenden

Eine andere Möglichkeit, Nachrichtendaten abzurufen,AWS IoT Analytics besteht darin, den`BatchPutMessage` API-Befehl zu verwenden. Für diese Methode musst du keineAWS IoT Regel einrichten, um Nachrichten mit einem bestimmten Thema an deinen Kanal weiterzuleiten. Es erfordert jedoch, dass das Gerät, das seine Daten/Nachrichten an den Kanal sendet, in der Lage ist, Software auszuführen, die mit demAWS SDK erstellt wurde, oder denAWS CLI to call verwenden kann`BatchPutMessage`.

1. Erstellen Sie eine Datei`messages.json`, die die zu sendenden Nachrichten enthält (in diesem Beispiel wird nur eine Nachricht gesendet).

```
[
    { "messageId": "message01", "payload": "{ \"message\": \"Hello from the CLI
\" }" }
```

```
]
```

2. Führen Sie den Befehl `batch-put-message` aus.

```
aws iotanalytics batch-put-message  --channel-name mychannel  --messages file://
messages.json --cli-binary-format raw-in-base64-out
```

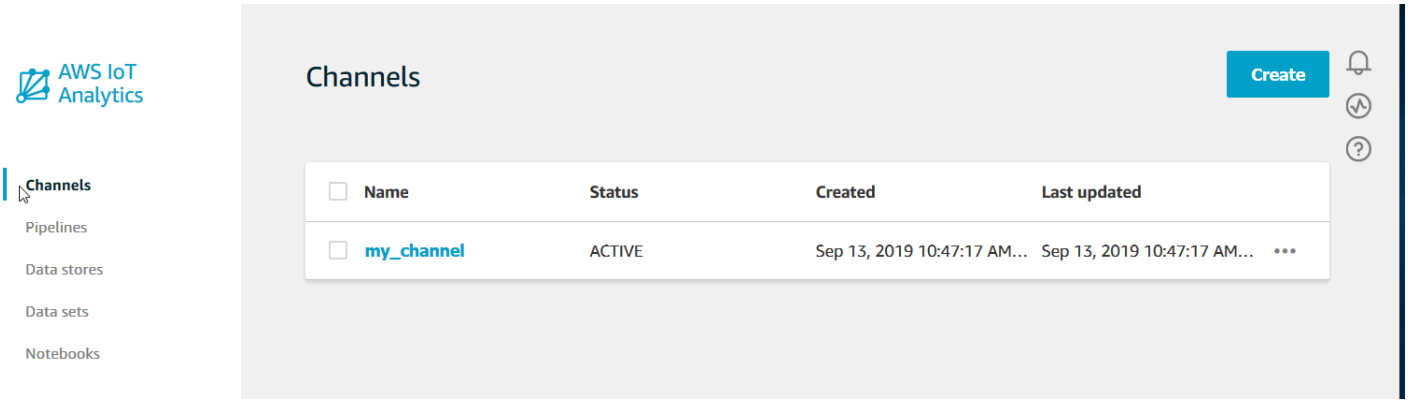
Wenn keine Fehler vorliegen, wird die folgende Ausgabe angezeigt.

```
{
    "batchPutMessageErrorEntries": []
}
```

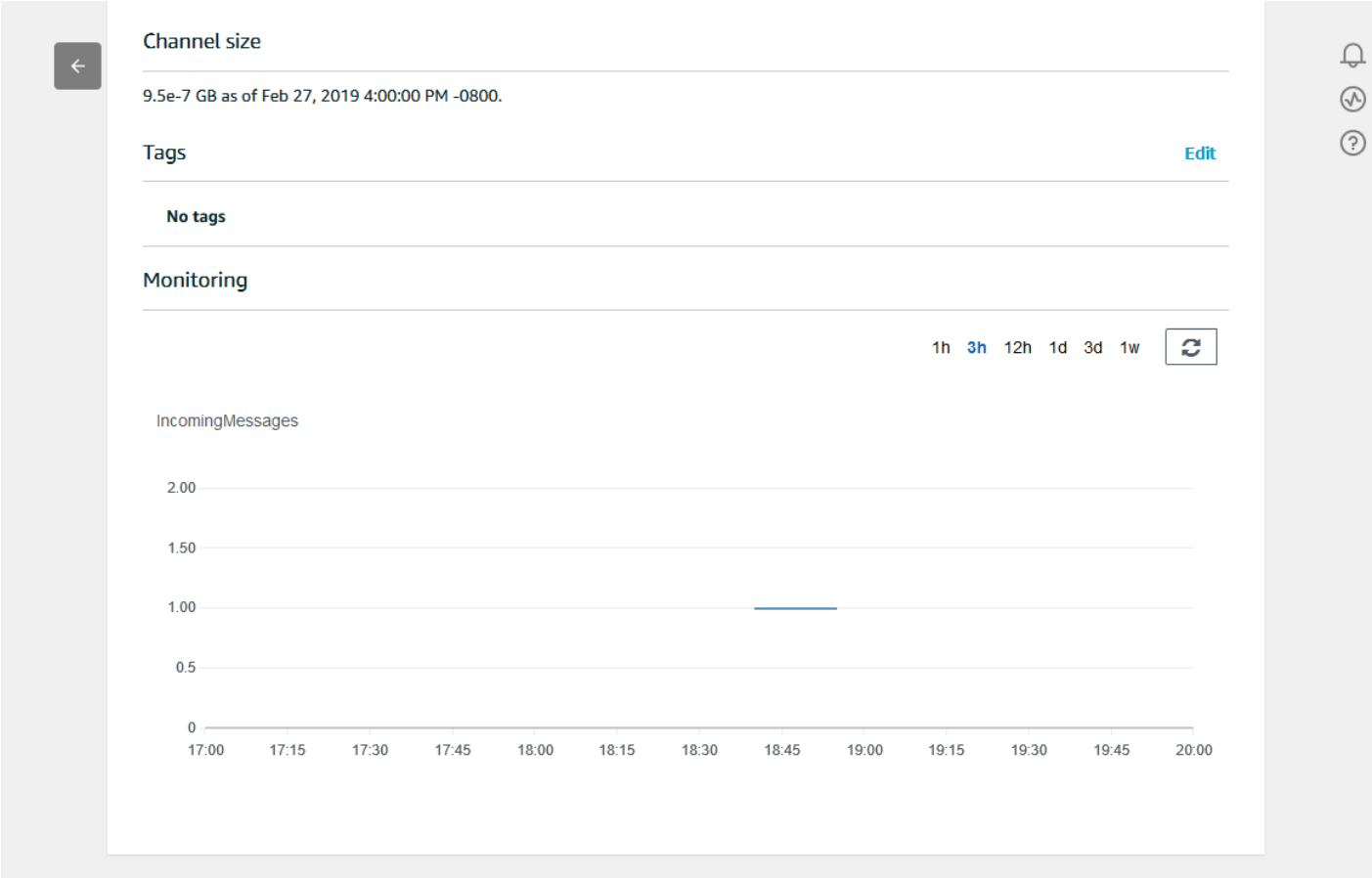
Überwachen der aufgenommenen Daten

Mithilfe derAWS IoT Analytics Konsole kannst du überprüfen, ob die von dir gesendeten Nachrichten in deinen Kanal aufgenommen werden.

1. Wählen Sie in der AWS IoT AnalyticsKonsole im linken Navigationsbereich Prepare und (falls erforderlich) Channel und dann den Namen des Kanals aus, den Sie zuvor erstellt haben.

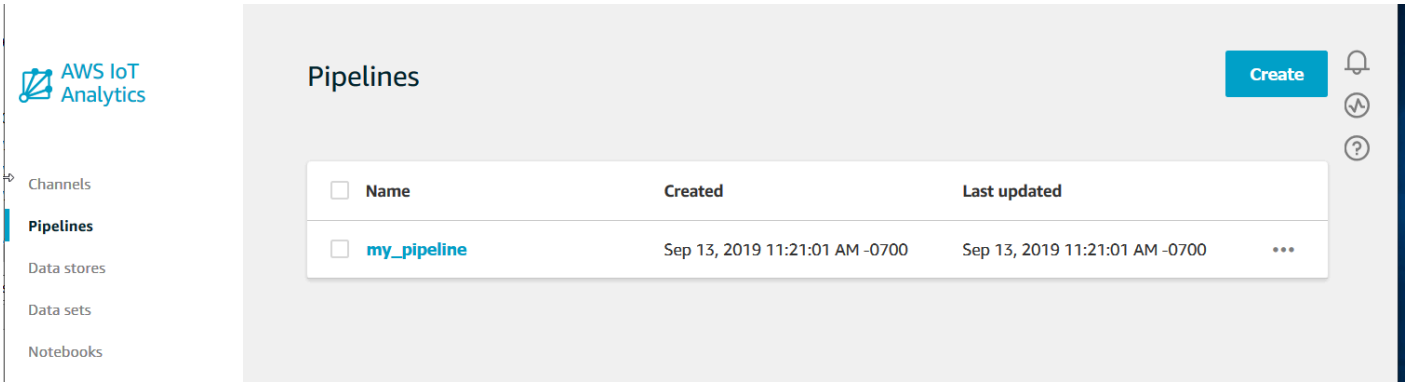


2. Blättern Sie auf der Detailseite des Kanals nach unten zum Abschnitt Monitoring (Überwachung). Passen Sie den angezeigten Zeitraum nach Bedarf über die Indikatoren (1h 3h 12h 1d 3d 1w (1 Std 3 Std 12 Std 1 T 3 T 1 W)) an. Sie sollten eine grafische Linie sehen, die die Anzahl der Nachrichten anzeigt, die während des angegebenen Zeitrahmens in diesen Kanal aufgenommen wurden.

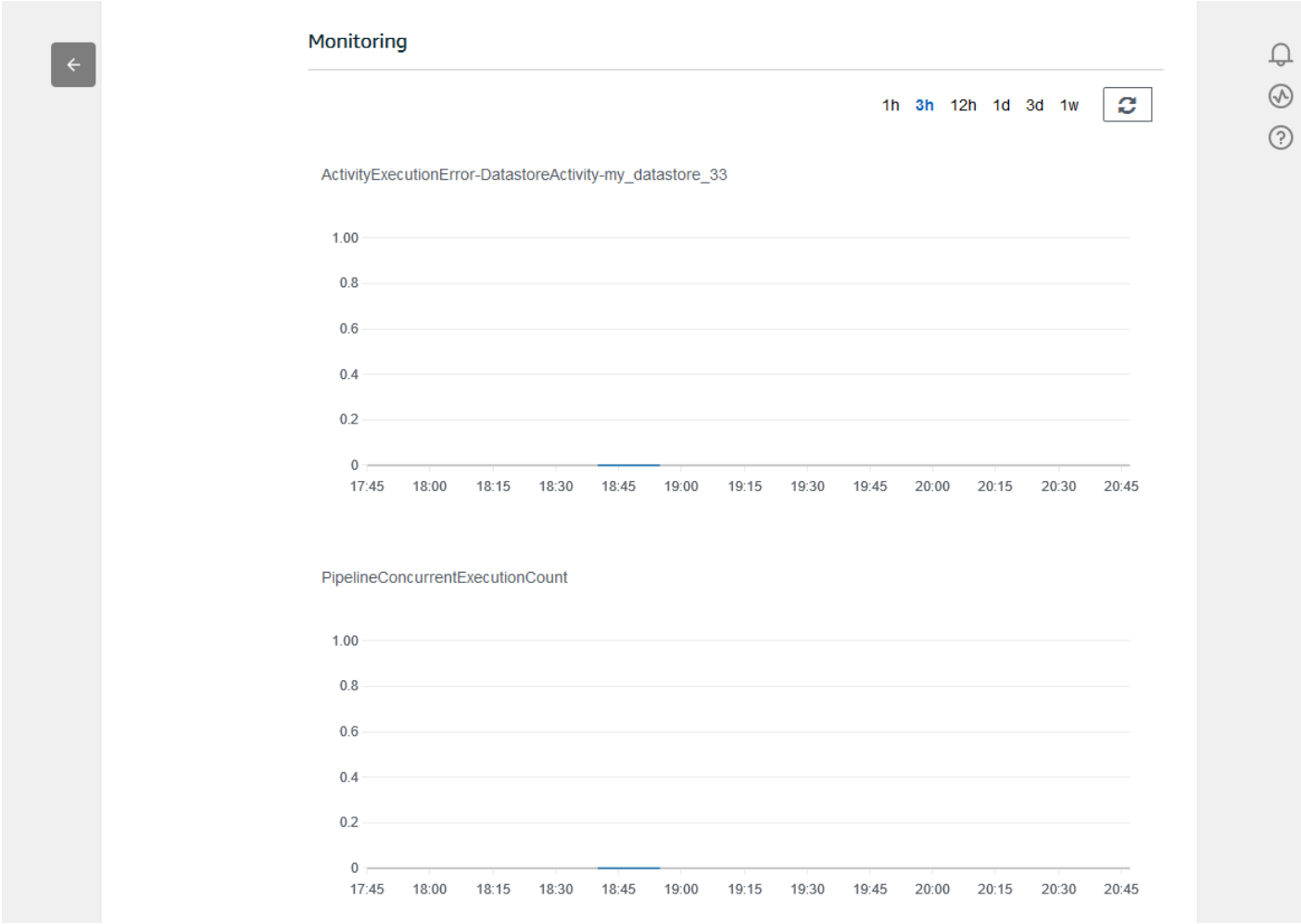


Es gibt eine ähnliche Überwachungsfunktion für die Ausführungen von Pipeline-Aktivitäten. Sie können Fehler bei der Aktivitätsausführung auf der Detailseite der Pipeline überwachen. Wenn Sie keine Aktivitäten als Teil Ihrer Pipeline angegeben haben, sollten 0 Ausführungsfehler angezeigt werden.

1. Wählen Sie in der AWS IoT AnalyticsKonsole im linken Navigationsbereich Prepare und dann Pipelines und dann den Namen einer Pipeline aus, die Sie zuvor erstellt haben.



2. Blättern Sie auf der Detailseite der Pipeline nach unten zum Abschnitt Monitoring (Überwachung). Passen Sie den angezeigten Zeitraum nach Bedarf über die Indikatoren (1h 3h 12h 1d 3d 1w (1 Std 3 Std 12 Std 1 T 3 T 1 W)) an. Sie sollten eine grafische Linie sehen, die die Anzahl der Fehler bei der Ausführung von Pipeline-Aktivitäten während des angegebenen Zeitrahmens angibt.



Dataset erstellen

Sie rufen Daten aus einem Datenspeicher ab, indem Sie ein SQL-Dataset oder ein Container-Dataset erstellen. AWS IoT Analyticskann die Daten abfragen, um analytische Fragen zu beantworten. Obwohl ein Datenspeicher keine Datenbank ist, verwenden Sie SQL-Ausdrücke, um die Daten abzufragen und Ergebnisse zu erzeugen, die in einer Datenmenge gespeichert werden.

Themen

- Abfragen von Daten
- Zugriff auf die abgefragten Daten

Abfragen von Daten

Um die Daten abzufragen, erstellen Sie einen Datensatz. Ein Datensatz enthält das SQL, das Sie für die Abfrage des Datenspeichers verwenden, sowie einen optionalen Zeitplan, der die Abfrage an einem von Ihnen ausgewählten Tag und zu einer Uhrzeit wiederholt. Sie erstellen die optionalen Zeitpläne mithilfe von Ausdrücken, die CloudWatch Amazon-Zeitplanausdrücken ähneln.

Führen Sie den folgenden Befehl aus, um ein Dataset zu erstellen.

```
aws iotanalytics create-dataset --cli-input-json file://mydataset.json
```

Wo die`mydataset.json` Datei den folgenden Inhalt enthält.

```
{
    "datasetName": "mydataset",
    "actions": [
        {
            "actionName":"myaction",
            "queryAction": {
                "sqlQuery": "select * from mydatastore"
            }
        }
    ]
}
```

Führen Sie den folgenden Befehl aus, um den Datast-Inhalt zu erstellen, indem Sie die Abfrage ausführen.

```
aws iotanalytics create-dataset-content --dataset-name mydataset
```

Warten Sie ein paar Minuten, bis der Datast-Inhalt erstellt wird, bevor Sie fortfahren.

Zugriff auf die abgefragten Daten

Das Ergebnis der Abfrage ist der Inhalt Ihres Datensatzes, gespeichert als Datei, im CSV-Format. Die Datei wird Ihnen über Amazon S3 bereitgestellt. Das folgende Beispiel zeigt, wie Sie überprüfen können, ob Ihre Ergebnisse bereit sind, und die Datei herunterladen.

Führen Sie den Befehl `get-dataset-content` aus.

```
aws iotanalytics get-dataset-content --dataset-name mydataset
```

Wenn Ihr Datensatz Daten enthält, dann hat die Ausgabe von`get-dataset-content`,`"state": "SUCCEEDED"` in dem`status` Feld, wie in diesem Beispiel das folgende Beispiel.

```
{
    "timestamp": 1508189965.746,
    "entries": [
        {
          "entryName": "someEntry",
          "dataURI": "https://aws-iot-analytics-datasets-f7253800-859a-472c-aa33-
e23998b31261.s3.amazonaws.com/results/f881f855-c873-49ce-abd9-b50e9611b71f.csv?X-Amz-"

        }
    ],
    "status": {
      "state": "SUCCEEDED",
      "reason": "A useful comment."
    }
}
```

`dataURI` ist eine signierte URL für die Ausgabeergebnisse. Sie ist für einen kurzen Zeitraum (einige Stunden) gültig. Abhängig von Ihrem Workflow empfiehlt es sich, immer `get-dataset-content` aufzurufen, bevor Sie auf den Inhalt zugreifen, da der Aufruf dieses Befehls eine neue signierte URL erzeugt.

AWS IoT AnalyticsDaten untersuchen

Sie haben mehrere Möglichkeiten, IhreAWS IoT Analytics Daten zu speichern, zu analysieren und zu visualisieren.

Themen auf dieser Seite:

- Amazon S3
- AWS IoT Events
- Amazon QuickSight
- Jupyter Notebook

Amazon S3

Sie können den Inhalt von Datensätzen an einen Amazon Simple Storage Service (Amazon S3) -Bucket senden und so die Integration mit Ihren vorhandenen Data Lakes oder den Zugriff über interne Anwendungen und Visualisierungstools ermöglichen. Sehen Sie das Feld`contentDeliveryRules::destination::s3DestinationConfiguration` in CreateDataset.

AWS IoT Events

Datast-Inhalte können als Eingabe an ein Datastore gesendet werdenAWS IoT Events, um Geräte oder Prozesse auf Fehler oder Änderungen im Betrieb zu überwachen und zusätzliche Aktionen auszuführen, wenn solche Ereignisse auftreten.

Erstellen Sie dazu einen Datensatz mit einerAWS IoT Events Eingabe in das Feld CreateDatasetund geben Sie diese an`contentDeliveryRules :: destination :: iotEventsDestinationConfiguration :: inputName`. Sie müssen auch die`roleArn` einer Rolle angeben, die dieAWS IoT Analytics Berechtigung zur Ausführung von „iotevents:BatchPutMessage“ gewährt. Jedes Mal, wenn der Inhalt des Datensatzes erstelltAWS IoT Analytics wird, wird jeder Inhaltseintrag des Datensatzes als Nachricht an die angegebeneAWS IoT Events Eingabe gesendet. Beispiel: Ihr Dataset enthält:

```
"what","who","dt"
"overflow","sensor01","2019-09-16 09:04:00.000"
"overflow","sensor02","2019-09-16 09:07:00.000"
"underflow","sensor01","2019-09-16 11:09:00.000"
...
```

sendetAWS IoT Analytics dann Nachrichten mit Feldern wie diesen:

```
{ "what": "overflow", "who": "sensor01", "dt": "2019-09-16 09:04:00.000" }
```

```
{ "what": "overflow", "who": "sensor02", "dt": "2019-09-16 09:07:00.000" }
```

und Sie sollten eineAWS IoT Events Eingabe erstellen, die die Felder erkennt, an denen Sie interessiert sind (eines oder mehrere von`what`,`who`,`dt`), und einAWS IoT Events Detektormodell erstellen, das diese Eingabefelder in Ereignissen verwendet, um Aktionen auszulösen oder interne Variablen festzulegen.

Amazon QuickSight

AWS IoT Analyticsbietet eine direkte Integration mit Amazon QuickSight. Amazon QuickSight ist ein schneller Geschäftsanalyse-Service, um Visualisierungen zu erstellen, Ad-hoc-Analysen auszuführen und schnell geschäftliche Erkenntnisse anhand Ihrer Daten zu gewinnen. Amazon QuickSight ermöglicht Unternehmen die Skalierung auf Hunderttausende von Benutzern und bietet eine reaktionsschnelle Leistung mithilfe einer robusten In-Memory-Engine (SPICE). Amazon QuickSight ist in diesen Regionen verfügbar.

Jupyter Notebook

AWS IoT AnalyticsDatensätze können auch direkt von Jupyter Notebook verwendet werden, um erweiterte Analysen und Datenerkundungen durchzuführen. Jupyter Notebook ist eine Open-Source-Lösung. Sie können unter http://jupyter.org/install.html installieren und herunterladen. Eine zusätzliche Integration mit SageMaker einer von Amazon gehosteten Notebook-Lösung ist ebenfalls verfügbar.

Aufbewahrung mehrerer Versionen von Datensätzen

Sie können wählen, wie viele Versionen Ihres Datensatzinhalts aufbewahrt werden sollen und für wie lange, indem Sie Werte für die`retentionPeriod and versioningConfiguration` Datensatzfelder angeben, wenn Sie die CreateDatasetund UpdateDatasetAPIs aufrufen:

```
...
"retentionPeriod": {
  "unlimited": "boolean",
  "numberOfDays": "integer"
},
"versioningConfiguration": {
  "unlimited": "boolean",
  "maxVersions": "integer"
},
...
```

Die Einstellungen dieser beiden Parameter bestimmen zusammen, wie viele Versionen von Datensatzinhalten aufbewahrt werden, und zwar auf folgende Weise und für wie lange.

	retentionPeriod [nicht angegeben]	retentionPeriod: unbegrenzt = TRUE, numberOfDays = nicht gesetzt	retentionPeriod: unbegrenzt = FALSCH, numberOfDays = X
versioningConfiguration: [nicht angegeben]	Nur die neueste Version sowie die neueste, erfolgreich ausgeführte Version (sofern abweichend) werden 90 Tage lang beibehalten.	Nur die neueste Version sowie die neueste, erfolgreich ausgeführte Version (sofern abweichend) werden unbegrenzt lang beibehalten.	Nur die neueste Version sowie die neueste, erfolgreich ausgeführte Version (sofern abweichend) werden X Tage lang beibehalten.
versioningConfiguration: unlimited = WAHR, maxVersions nicht festgelegt	Alle Versionen der letzten 90 Tage werden beibehalten, unabhängig von der Anzahl der Versionen.	Es gibt keine Begrenzung für die Anzahl der beibehaltenen Versionen.	Alle Versionen aus der letzten X Tage werden beibehalten, unabhängig von der Anzahl der Versionen.
versioningConfiguration: unlimited = FALSCH, maxVersions = Y	Es werden nicht mehr als Y Versionen der letzten 90 Tage beibehalten.	Bis zu Y Versionen werden beibehalten, unabhängig davon, wie alt sie sind.	Es werden nicht mehr als Y Versionen der letzten X Tage aufbewahrt.

Nachrichten-Nutzlast-Syntax

Die Feldnamen der Nachrichten-Payloads (Daten), an die Sie sendenAWS IoT Analytics:

- Darf nur alphanumerische Zeichen und Unterstriche (_) enthalten; weitere Sonderzeichen sind nicht zulässig
- Mit einem alphabetischen Zeichen oder einzelnen Unterstrich (_) beginnen müssen.
- Keine Bindestriche (-) enthalten können.

- In Begriffen mit regulären Ausdrücken: "`^[A-Za-z_]([A-Za-z0-9]*|[A-Za-z0-9][A-Za-z0-9_]*)$`“.
- Nicht länger als 255 Zeichen sein dürfen.
- Die Groß- und Kleinschreibung berücksichtigen. Felder mit den Namen „foo“ und „FOO“ in derselben Payload werden als Duplikate betrachtet.

Beispielsweise sind `{"temp_01": 29}` und `{"_temp_01": 29}` gültig, aber `{"temp-01": 29}`, `{"01_temp": 29}` und `{"__temp_01": 29}` sind ungültig in Nachrichtennutzlasten.

Arbeiten mitAWS IoT SiteWiseDaten

AWS IoT SiteWiseist ein verwalteter Service, mit dem Sie Daten von Industrieanlagen skalierbar erfassen, modellieren, analysieren und visualisieren können. Der Service bietet ein Framework zum Modellieren von Komponenten, zum Erstellen von Darstellungen Ihrer industriellen Geräte, Prozesse und Einrichtungen.

mitAWS IoT SiteWiseMithilfe von Komponentenmodellen können Sie definieren, welche Industrieanlagen verwendet und wie diese zu komplexen Metriken verarbeitet werden sollen. Sie können Asset-Modelle für die Erfassung und Verarbeitung von Daten imAWSCloud. Weitere Informationen finden Sie im .AWS IoT SiteWise-Benutzerhandbuch.

AWS IoT Analyticsist in integriert.AWS IoT SiteWisedamit Sie SQL-Abfragen ausführen und planen könnenAWS IoT SiteWiseDATA. So starten Sie mit der AbfrageAWS IoT SiteWisedata, erstellen Sie einen Datenspeicher, indem Sie die Verfahren unterKonfigurieren der SpeichereinstellungenimAWS IoT SiteWise-Benutzerhandbuchaus. Führen Sie anschließend die -Schritte unter ausErstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (Konsole)oder inErstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (AWS CLI)um einAWS IoT AnalyticsDatensatz und führen Sie eine SQL-Abfrage für Ihre industriellen Daten aus.

Themen

- Erstellen einesAWS IoT AnalyticsDataset mitAWS IoT SiteWiseDaten
- Zugriff auf Datensatzinhalte
- Tutorial: AbfragenAWS IoT SiteWisedata inAWS IoT Analytics

Erstellen einesAWS IoT AnalyticsDataset mitAWS IoT SiteWiseDaten

Importieren in &S3;AWS IoT AnalyticsEin Dataset enthält SQL-Anweisungen und -Ausdrücke, mit denen Sie Daten in Ihrem Datenspeicher abfragen, zusammen mit einem optionalen Zeitplan, der die Abfrage zu einem von Ihnen angegebenen Tag und einer von Ihnen angegebenen Uhrzeit wiederholt. Sie können Ausdrücke verwenden, die ähnlich sindAmazon CloudWatch Zeitplanausdrückeum die optionalen Zeitpläne zu erstellen.

> **Note**
>
> Ein Datensatz ist normalerweise eine Sammlung von Daten, die möglicherweise tabellarisch organisiert sind oder nicht. Im Gegensatz dazuAWS IoT Analyticserstellt Ihren Datensatz, indem Sie eine SQL-Abfrage auf Daten in Ihrem Datenspeicher anwenden.

Führen Sie als Einstieg in die Erstellung eines Datasets für IhreAWS IoT SiteWiseDATA.

Themen

- Erstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (Konsole)
- Erstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (AWS CLI)

Erstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (Konsole)

Gehen Sie wie folgt vor, um einen Datensatz imAWS IoT AnalyticsKonsole für IhreAWS IoT SiteWiseDATA.

So erstellen Sie ein Dataset

1. In derhttps://console.aws.amazon.com/iotanalytics/, auf derlinker Navigationsbereich, wählenDatensätzeaus.
2. Auf derErstellen eines Datasets-Seite wählenErstellen Sie SQLaus.
3. Auf derFestlegen von Dataset-Details-Seite geben Sie die Details Ihres Datasets an.
   a. Geben Sie einen Namen für Ihren Dataset ein.
   b. FürDatenspeicher-Quelle, wählen Sie die eindeutige ID, mit der SieAWS IoT SiteWiseDatenspeicher.

c. (Optional) FürTags, fügen Sie ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Dataset hinzu.

4. Verwenden Sie SQL-Ausdrücke, um Ihre Daten abzufragen und analytische Fragen zu beantworten.

   a. In derAnfrage des Autorseine SQL-Abfrage ein, die einen Platzhalter verwendet, um bis zu fünf Datenzeilen anzuzeigen.

   ```
   SELECT * FROM my_iotsitewise_datastore.asset_metadata LIMIT 5
   ```

   Weitere Informationen zu den unterstützten SQL-Funktionen unterAWS IoT Analytics, finden Sie unterSQL-Ausdrücke inAWS IoT Analyticsaus. Oder finden Sie unterTutorial: AbfragenAWS IoT SiteWisedata inAWS IoT Analyticsfür Beispiele für statistische Abfragen, die einen Einblick in Ihre Daten geben können.

   b. Sie können wählenTestabfrageum zu überprüfen, ob Ihre Eingabe korrekt ist, und um die Ergebnisse in einer Tabelle nach der Abfrage anzuzeigen.

   > **Note**
   >
   > Da es sich beiAmazon Athena begrenzt die maximale Anzahl laufender Abfragen, sollten Sie Ihre SQL-Abfrage auf eine angemessene Größe beschränken, damit sie über einen längeren Zeitraum nicht ausgeführt wird.

5. (Optional) Wenn Sie Datensatzinhalte mit Daten aus einem bestimmten Zeitraum erstellen, kommen einige Daten möglicherweise nicht rechtzeitig zur Verarbeitung an. Um eine Verzögerung zuzulassen, können Sie einen Offset oder ein Delta angeben. Weitere Informationen finden Sie unter Verspätete Datenbenachrichtigungen über Amazon CloudWatch Events erhalten.

   Nach dem Konfigurieren eines Datenauswahlfilters auf derKonfigurieren des Datenauswahlfilters-Seite wählenWeiteraus.

6. (Optional) Auf derSeite „Abfrageplan festlegen“können Sie planen, dass diese Abfrage regelmäßig ausgeführt wird, um das Dataset zu aktualisieren. Dataset-Zeitpläne können jederzeit erstellt und bearbeitet werden.

> **Note**
>
> DATA ausAWS IoT SiteWisenimmt inAWS IoT Analyticsalle sechs Stunden. Wir empfehlen, eine Frequenz von sechs Stunden oder mehr auszuwählen.

Wählen und Option fürHäufigkeitund danach wählen SieWeiteraus.

7. AWS IoT Analyticserstellt Versionen dieses Datensatz-Inhalts und speichert Ihre Analyseergebnisse für den angegebenen Zeitraum. Wir empfehlen 90 Tage, Sie können sich jedoch dafür entscheiden, Ihre benutzerdefinierte Aufbewahrungsrichtlinie festzulegen. Sie können auch die Anzahl der gespeicherten Versionen Ihres Datensatz-Inhalts einschränken.

   Nachdem Sie Ihre Optionen auf derKonfigurieren Sie die Ergebnisse Ihres Datensatzes-Seite wählenWeiteraus.

8. (Optional) Sie können die Lieferregeln Ihrer Datensatzergebnisse an ein bestimmtes Ziel konfigurieren, z.AWS IoT Eventsaus.

   Nachdem Sie Ihre Optionen auf derKonfigurieren von Regeln für die Bereitstellung von Datensätzen-Seite wählenWeiteraus.

9. Überprüfen Sie Ihre Auswahl und klicken Sie dann aufErstellen eines Datasetsaus.

10. Stellen Sie sicher, dass Ihr neuer Datensatz auf derDatensätzeangezeigten.

Erstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (AWS CLI)

Führen Sie Folgendes ausAWS CLIBefehle zum Abfragen IhresAWS IoT SiteWiseDATA.

Die hier gezeigten Beispiele verwenden dieAWS Command Line Interface(AWS CLI) enthalten. Weitere Informationen über dieAWS CLI, finden Sie unterAWS Command Line Interface-Benutzerhandbuchaus. Weitere Informationen zu den CLI-Befehlen fürAWS IoT Analytics, finden Sie unteriotAnalyticsimAWS Command Line Interface--Referenzaus.

So erstellen Sie ein Dataset

1. Führen Sie Folgendes aus`create-dataset`Befehl zum Erstellen eines Datasets.

```
aws iotanalytics create-dataset --cli-input-json file://my_dataset.json
```

Wobei gilt der`my_dataset.json`-Datei enthält den folgenden Inhalt.

```
{
    "datasetName": "my_dataset",
    "actions": [
        {
            "actionName":"my_action",
            "queryAction": {
                "sqlQuery": "SELECT * FROM my_iotsitewise_datastore.asset_metadata
 LIMIT 5"
            }
        }
    ]
}
```

Weitere Informationen zu den unterstützten SQL-Funktionen unterAWS IoT Analytics, finden Sie unterSQL-Ausdrücke inAWS IoT Analyticsaus. Oder finden Sie unterTutorial: AbfragenAWS IoT SiteWisedata inAWS IoT Analyticsfür Beispiele für statistische Abfragen, die einen Einblick in Ihre Daten geben können.

2. Führen Sie Folgendes aus`create-dataset-content`Befehl, um Ihren Datensatzinhalt durch Ausführen Ihrer Abfrage zu erstellen.

```
aws iotanalytics create-dataset-content --dataset-name my_dataset
```

Zugriff auf Datensatzinhalte

Das Ergebnis der SQL-Abfrage ist Ihr Dataset-Inhalt, der als Datei im CSV-Format gespeichert wird. Die Datei wird Ihnen über Amazon S3 bereitgestellt. Die folgenden Schritte zeigen, wie Sie überprüfen können, ob Ihre Ergebnisse bereit sind, und die Datei herunterladen.

Themen

- Zugriff auf Dataset-Inhalte inAWS IoT Analytics(Konsole)
- Zugriff auf Dataset-Inhalte inAWS IoT Analytics(AWS CLI)

Zugriff auf Dataset-Inhalte inAWS IoT Analytics(Konsole)

Wenn Ihr Dataset Daten enthält, können Sie Ihre SQL-Abfrageergebnisse in einer Vorschau anzeigen und herunterladenAWS IoT Analyticsconsole.

Zugriff auf IhreAWS IoT AnalyticsErgebnisse des Datensatzes

1. In der -Konsole, auf derDatensätzeWählen Sie den Namen des Datasets aus, auf den Sie zugreifen möchten.
2. Wählen Sie auf der Seite Dataset-Zusammenfassung die OptionInhalt-Tab.
3. In derInhalt von Dataset-Inhaltenwählen Sie den Namen der Abfrage, für die Sie eine Vorschau der Ergebnisse anzeigen möchten, oder laden Sie eine CSV-Datei der Ergebnisse herunter.

Zugriff auf Dataset-Inhalte inAWS IoT Analytics(AWS CLI)

Wenn Ihr Dataset Daten enthält, können Sie Ihre SQL-Abfrageergebnisse in der Vorschau anzeigen und herunterladen.

Die hier gezeigten Beispiele verwenden dieAWS Command Line Interface(AWS CLI) enthalten. Weitere Informationen über dieAWS CLI, finden Sie unterAWS Command Line Interface-Benutzerhandbuchaus. Weitere Informationen zu den CLI-Befehlen, die fürAWS IoT Analytics, finden Sie unteriotAnalyticsimAWS Command Line Interface--Referenzaus.

Zugriff auf IhreAWS IoT AnalyticsErgebnisse des Datasets (AWS CLI)

1. Führen Sie Folgendes aus`get-dataset-content`, um das Ergebnis Ihrer Abfrage anzuzeigen.

```
aws iotanalytics get-dataset-content --dataset-name my_iotsitewise_dataset
```

2. Wenn Ihr Dataset Daten enthält, wird die Ausgabe von`get-dataset-content`, hat`"state": "SUCCEEDED"`im`status`-Feld, wie im folgenden Beispiel.

```
{
    "timestamp": 1508189965.746,
    "entries": [
        {
          "entryName": "my_entry_name",
          "dataURI": "https://aws-iot-analytics-datasets-f7253800-859a-472c-aa33-
e23998b31261.s3.amazonaws.com/results/f881f855-c873-49ce-abd9-b50e9611b71f.csv?X-
Amz-"
```

```
        }
    ],
    "status": {
      "state": "SUCCEEDED",
      "reason": "A useful comment."
    }
}
```

3. Die Ausgabe vonget-dataset-contentBeinhaltet einedataURI, was eine signierte URL für die Ausgabeergebnisse ist. Sie ist für einen kurzen Zeitraum (einige Stunden) gültig. Besuchen Sie dasdataURIURL für den Zugriff auf Ihre SQL-Abfrageergebnisse.

> **Note**
>
> Abhängig von Ihrem Workflow empfiehlt es sich, immer `get-dataset-content` aufzurufen, bevor Sie auf den Inhalt zugreifen, da der Aufruf dieses Befehls eine neue signierte URL erzeugt.

Tutorial: AbfragenAWS IoT SiteWisedata inAWS IoT Analytics

In diesem Tutorial wird gezeigt, wie SieAWS IoT SiteWisedata inAWS IoT Analytics. Das Tutorial verwendet Daten aus einer Demo inAWS IoT SiteWisedas liefert einen Beispieldatensatz für einen Windpark.

> **Important**
>
> Die Ressourcen, die in dieser Demo erstellt und genutzt werden, werden Ihnen in Rechnung gestellt.

Themen

Voraussetzungen

Für dieses Tutorial benötigen Sie folgende Ressourcen:

- Sie benötigen einAWSAccount mit dem Sie beginnenAWS IoT SiteWiseundAWS IoT Analytics. Wenn dies nicht der Fall ist, folgen Sie den Schritten inErstellen einesAWSKonto.
- Ein Entwicklungscomputer mit Windows, macOS, Linux oder Unix für den Zugriff auf die AWS Management Console. Weitere Informationen finden Sie unter Erste Schritte mit AWS Management Console.
- AWS IoT SiteWiseDaten, die definierenAWS IoT SiteWisemodelliert und Anlagen und streamt Daten, die Daten von Windparkgeräten darstellen. Gehen Sie folgendermaßen vor, um Ihre Daten zu erstellenErstellen derAWS IoT SiteWiseDemoin derAWS IoT SiteWiseBenutzerhandbuch.
- DeinAWS IoT SiteWiseDemo-Windparkausrüstungsdaten in einem vorhandenen Datenspeicher, den Sie verwalten. Weitere Informationen, wie Sie einen Datenspeicher für Ihren erstellen könnenAWS IoT SiteWiseDaten, siheSpeichereinstellungen konfigurierenin derAWS IoT SiteWiseBenutzerhandbuch.

> **Note**
>
> DeinAWS IoT SiteWiseMetadaten erscheinen in IhremAWS IoT SiteWiseDatenspeicher kurz nach der Erstellung; es kann jedoch bis zu sechs Stunden dauern, bis Ihre Rohdaten angezeigt werden. In der Zwischenzeit können Sie einAWS IoT AnalyticsDatenmenge erstellen und Abfragen zu Ihren Metadaten ausführen.

Nächster Schritt

Daten laden und verifizieren

Daten laden und verifizieren

Die Daten, die Sie in diesem Tutorial abfragen, sind ein Beispielsatz vonAWS IoT SiteWiseDaten, die Windkraftanlagen in einem Windpark modellieren.

> **Note**
>
> In diesem Tutorial werden Sie drei Tabellen in Ihrem Datenspeicher abfragen:
>
> - `raw`- Enthält unverarbeitete Rohdaten für jedes Asset.

- `asset_metadata`- Enthält allgemeine Informationen zu jedem Asset.
- `asset_hierarchy_metadata`- Enthält Informationen zu den Beziehungen zwischen Assets.

So führen Sie die SQL-Abfragen in diesem Lernprogramm aus

1. Führen Sie die Schritte unterErstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (Konsole)oderErstellen Sie ein Dataset mitAWS IoT SiteWiseDATA (AWS CLI)Erstellen einesAWS IoT Analyticsdatensatz für IhrAWS IoT SiteWisedata.
2. Gehen Sie wie folgt vor, um Ihre Datensatzabfrage während dieses Lernprogramms zu aktualisieren.

   a. In derAWS IoT AnalyticsKonsole, in derDatensätzewählen Sie den Namen des Datensatzes, den Sie auf der vorherigen Seite erstellt haben.

   b. Wählen Sie auf der DatensatzzusammenfassungsseiteBearbeitenum Ihre SQL-Abfrage zu bearbeiten.

   c. Um die Ergebnisse im Anschluss an die Abfrage in einer Tabelle anzuzeigen, wählen SieTestabfrage.

   Alternativ können Sie Folgendes ausführen`update-dataset`Befehl zum Ändern der SQL-Abfrage mit demAWS CLI.

   ```
   aws iotanalytics update-dataset --cli-input-json file://update-query.json
   ```

   Inhalt von `update-query.json`:

   ```
   {
       "datasetName": "my_dataset",
       "actions": [
           {
               "actionName": "myDatasetUpdateAction",
               "queryAction": {
                   "sqlQuery": "SELECT * FROM my_iotsitewise_datastore.asset_metadata
    LIMIT 3"
               }
           }
       ]
   ```

```
}
```

3. In derAWS IoT AnalyticsKonsole oder mit derAWS CLI, führen Sie die folgende Abfrage Ihrer Daten durch, um zu überprüfen, ob Ihre`asset_metadata`Tabelle wurde erfolgreich geladen.

   ```
   SELECT COUNT(*) FROM my_iotsitewise_datastore.asset_metadata
   ```

   Ebenso können Sie überprüfen, ob Ihr`asset_hierarchy_metadata`und`raw`Tische sind nicht leer.

Nächster Schritt

[Erkundung von Daten](#)

Erkundung von Daten

Nach IhremAWS IoT SiteWiseDaten werden erstellt und in einen Datenspeicher geladen, Sie können eineAWS IoT AnalyticsDatenmenge erstellen und SQL-Abfragen ausführenAWS IoT Analyticsum Erkenntnisse über Ihr Vermögen zu gewinnen. Die folgenden Abfragen veranschaulichen, wie Sie Ihre Daten untersuchen können, bevor Sie statistische Abfragen ausführen.

So untersuchen Sie Ihre Daten mit SQL-Abfragen

1. Zeigen Sie eine Stichprobe von Spalten und Werten in jeder Tabelle an, z. B. in der Rohtabelle.

   ```
   SELECT * FROM my_iotsitewise_datastore.raw LIMIT 5
   ```

2. Verwenden von`SELECT DISTINCT`um Ihr`asset_metadata`und listen Sie die (eindeutigen) Namen IhrerAWS IoT SiteWiseAssetins.

   ```
   SELECT DISTINCT assetname FROM my_iotsitewise_datastore.asset_metadata ORDER BY
    assetname
   ```

3. So listen Sie Informationen zu Eigenschaften für eine bestimmteAWS IoT SiteWiseAsset, benutze das`WHERE`Klausel.

   ```
   SELECT assetpropertyname,
        assetpropertyunit,
        assetpropertydatatype
   FROM my_iotsitewise_datastore.asset_metadata
   ```

```
WHERE assetname = 'Demo Turbine Asset 2'
```

4. mitAWS IoT Analyticskönnen Sie Daten aus zwei oder mehr Tabellen in Ihrem Datenspeicher verknüpfen, wie im folgenden Beispiel.

   ```
   SELECT * FROM my_iotsitewise_datastore.raw AS raw
   JOIN my_iotsitewise_datastore.asset_metadata AS asset_metadata
   ON raw.seriesId = asset_metadata.timeseriesId
   ```

   Um alle Beziehungen zwischen Ihren Assets anzuzeigen, verwenden Sie die`JOIN`-Funktionalität in der folgenden Abfrage.

   ```
   SELECT DISTINCT parent.assetName as "Parent name",
       child.assetName AS "Child name"
   FROM (
       SELECT sourceAssetId AS parent,
              targetAssetId AS child
       FROM my_iotsitewise_datastore.asset_hierarchy_metadata
       WHERE associationType = 'CHILD'
   )
   AS relations
   JOIN my_iotsitewise_datastore.asset_metadata AS child
       ON relations.child = child.assetId
   JOIN my_iotsitewise_datastore.asset_metadata AS parent
       ON relations.parent = parent.assetId
   ```

Nächster Schritt

Ausführen von statistischen Abfragen

Ausführen von statistischen Abfragen

Jetzt haben Sie IhreAWS IoT SiteWiseDaten können Sie statistische Abfragen durchführen, die wertvolle Einblicke in Ihre Industrieanlagen liefern. Die folgenden Abfragen veranschaulichen einige der Informationen, die Sie abrufen können.

So führen Sie statistische Abfragen ausAWS IoT SiteWiseDemo-Windparkdaten

1. Führen Sie den folgenden SQL-Befehl aus, um die neuesten Werte aller Eigenschaften mit numerischen Werten für ein bestimmtes Asset (Demo Turbine Asset 4) zu ermitteln.

```
SELECT assetName,
    assetPropertyName,
    assetPropertyUnit,
    max_by(value, timeInSeconds) AS Latest
FROM (
    SELECT *,
        CASE assetPropertyDataType
        WHEN 'DOUBLE' THEN
        cast(doubleValue AS varchar)
        WHEN 'INTEGER' THEN
        cast(integerValue AS varchar)
        WHEN 'STRING' THEN
        stringValue
        WHEN 'BOOLEAN' THEN
        cast(booleanValue AS varchar)
        ELSE NULL
        END AS value
    FROM my_iotsitewise_datastore.asset_metadata AS asset_metadata
    JOIN my_iotsitewise_datastore.raw AS raw
        ON raw.seriesId = asset_metadata.timeSeriesId
    WHERE startYear=2021
        AND startMonth=7
        AND startDay=8
        AND assetName='Demo Turbine Asset 4'
)
GROUP BY assetName, assetPropertyName, assetPropertyUnit
```

2. Verknüpfen Sie beide Metadatentabellen und Ihre Rohtabelle, um die maximalen Windgeschwindigkeitseigenschaften für alle Assets zusätzlich zu ihren übergeordneten Assets zu ermitteln.

```
SELECT child_assets_data_set.parentAssetId,
        child_assets_data_set.childAssetId,
        asset_metadata.assetPropertyId,
        asset_metadata.assetPropertyName,
        asset_metadata.timeSeriesId,
        raw_data_set.max_speed
FROM (
   SELECT sourceAssetId AS parentAssetId,
        targetAssetId AS childAssetId
    FROM my_iotsitewise_datastore.asset_hierarchy_metadata
    WHERE associationType = 'CHILD'
```

```
)
AS child_assets_data_set
JOIN mls_demo.asset_metadata AS asset_metadata
    ON asset_metadata.assetId = child_assets_data_set.childAssetId
JOIN (
    SELECT seriesId, MAX(doubleValue) AS max_speed
    FROM my_iotsitewise_datastore.raw
    GROUP BY seriesId
)
AS raw_data_set
ON raw_data_set.seriesId = asset_metadata.timeseriesid
WHERE assetPropertyName = 'Wind Speed'
ORDER BY max_speed DESC
```

3. Führen Sie den folgenden SQL-Befehl aus, um den Durchschnittswert einer bestimmten Eigenschaft (Windgeschwindigkeit) für ein Asset (Demo Turbine Asset 2) zu ermitteln. Du musst ersetzen`my_bucket_id`mit der ID Ihres -Buckets.

```
SELECT AVG(doubleValue) as "Average wind speed"
FROM my_iotsitewise_datastore.raw
WHERE seriesId =
    (SELECT timeseriesId
    FROM my_iotsitewise_datastore.asset_metadata as asset_metadata
    WHERE asset_metadata.assetname = 'Demo Turbine Asset 2'
            AND asset_metadata.assetpropertyname = 'Wind Speed')
```

Nächster Schritt

Bereinigen Ihrer Tutorialressourcen

Bereinigen Ihrer Tutorialressourcen

Bereinigen Ihrer Ressourcen, nachdem Sie das Tutorial abgeschlossen haben, bereinigen Ihrer Ressourcen, um Gebühren zu vermeiden.

So löschen Sie IhrAWS IoT SiteWiseDemo

DieAWS IoT SiteWisedemo löscht sich nach einer Woche von selbst. Wenn Sie mit der Verwendung der Demo-Ressourcen fertig sind, können Sie die Demo früher löschen. Gehen Sie folgendermaßen vor, um die Demo manuell zu löschen.

1. Navigieren Sie zur AWS CloudFormation-Konsole.

2. Wählen Sie IoTSiteWiseDemoAssets aus der Liste der Stacks aus.
3. Wählen Sie Löschen. Wenn Sie den Stack löschen, werden alle für die Demo erstellten Ressourcen gelöscht.
4. Geben Sie im Bestätigungsdialogfeld einLöschen.

   Das Löschen des Stacks dauert etwa 15 Minuten. Wenn die Demo nicht gelöscht werden kann, wählen Sie oben rechts erneut Löschen aus. Wenn es erneut nicht möglich ist, die Demo zu löschen, führen Sie die Schritte in der AWS CloudFormation-Konsole aus, um die Ressourcen zu überspringen, die nicht gelöscht werden konnten, und versuchen Sie es erneut.

So löschen Sie Ihren Datenspeicher

- Um Ihren verwalteten Datenspeicher zu löschen, führen Sie den CLI-Befehl aus`delete-datastore`, wie im folgenden Beispiel.

  ```
  aws iotanalytics delete-datastore --datastore-name my_IotSiteWise_datastore
  ```

So löschen Sie IhrAWS IoT AnalyticsDatensatz

- Um Ihre Datenmenge zu löschen, führen Sie den CLI-Befehl aus`delete-dataset`, wie im folgenden Beispiel. Sie müssen den Inhalt der Datenmenge nicht löschen, bevor Sie diesen Vorgang ausführen.

  ```
  aws iotanalytics delete-dataset --dataset-name my_dataset
  ```

  > **Note**
  >
  > Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Pipeline-Aktivitäten

Die einfachste funktionale Pipeline verbindet einen Kanal mit einem Datenspeicher, wodurch sie zu einer Pipeline mit zwei Aktivitäten wird: einer `channel`-Aktivität und einer `datastore`-Aktivität. Sie können eine leistungsfähigere Verarbeitung der Nachrichten erreichen, indem Sie Ihrer Pipeline zusätzliche Aktivitäten hinzufügen.

Sie können dasRunPipelineActivityOperation, um die Ergebnisse der Ausführung einer Pipeline-Aktivität auf einer von Ihnen bereitgestellten Nachrichtennutzlast zu simulieren. Dies könnte hilfreich sein, wenn Sie Ihre Pipeline-Aktivitäten entwickeln und debuggen. RunPipelineActivity Beispielzeigt, wie es verwendet wird.

Kanal-Aktivität

Die erste Aktivität in einer Pipeline muss`channel`Aktivität, die die Quelle der zu verarbeitenden Nachrichten bestimmt.

```
{
    "channel": {
        "name": "MyChannelActivity",
        "channelName": "mychannel",
        "next": "MyLambdaActivity"
    }
}
```

Datastore-Aktivität

Die `datastore`-Aktivität, die angibt, wo die verarbeiteten Daten gespeichert werden, ist die letzte Aktivität.

```
{
    "datastore": {
        "name": "MyDatastoreActivity",
        "datastoreName": "mydatastore"
    }
}
```

AWS LambdaAktivität

Sie können ein**lambda**Aktivitätum eine komplexe Verarbeitung von Nachrichten durchzuführen. Beispielsweise können Sie Nachrichten mit Daten aus der Ausgabe externer API-Vorgänge anreichern oder anhand der Logik von Amazon DynamoDB nach Nachrichten filtern. Sie können diese Pipelineaktivität jedoch nicht verwenden, um zusätzliche Nachrichten hinzuzufügen oder vorhandene Nachrichten zu entfernen, bevor Sie einen Datenspeicher aufrufen.

DieAWS LambdaFunktion, die in einem**lambda**Aktivitätmuss ein Array von JSON-Objekten empfangen und zurückgeben. Ein Beispiel finden Sie unter the section called “Beispiel 1 für Lambda-Funktion”.

ErteiltAWS IoT AnalyticsUm Ihre Lambda-Funktion aufrufen zu können, müssen Sie eine Richtlinie hinzufügen. Führen Sie beispielsweise den folgenden -CLI-Befehl aus und ersetzen*exampleFunctionName*Ersetzen Sie durch den Namen Ihrer Lambda-Funktion*123456789012*mit deinemAWSKonto-ID und verwenden Sie den Amazon-Ressourcennamen (ARN) der Pipeline, die die angegebene Lambda-Funktion aufruft.

```
aws lambda add-permission --function-name exampleFunctionName --
action lambda:InvokeFunction --statement-id iotanalytics --principal
 iotanalytics.amazonaws.com --source-account 123456789012 --source-arn
 arn:aws:iotanalytics:us-east-1:123456789012:pipeline/examplePipeline
```

Der Befehl gibt Folgendes zurück:

```
{
    "Statement": "{\"Sid\":\"iotanalyticsa\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"iotanalytics.amazonaws.com\"},\"Action\":
\"lambda:InvokeFunction\",\"Resource\":\"arn:aws:lambda:aws-region:aws-
account:function:exampleFunctionName\",\"Condition\":{\"StringEquals\":
{\"AWS:SourceAccount\":\"123456789012\"},\"ArnLike\":{\"AWS:SourceArn\":
\"arn:aws:iotanalytics:us-east-1:123456789012:pipeline/examplePipeline\"}}}"
}
```

Weitere Informationen finden Sie unterVerwenden ressourcenbasierter Richtlinien fürAWS Lambdain derAWS Lambda-Entwicklerhandbuch.

Beispiel 1 für Lambda-Funktion

In diesem Beispiel fügt die Lambda-Funktion Informationen hinzu, die auf Daten in der ursprünglichen Nachricht basieren. Ein Gerät veröffentlicht eine Nachricht mit einer Nutzlast ähnlich dem folgenden Beispiel.

```
{
  "thingid": "00001234abcd",
  "temperature": 26,
  "humidity": 29,
  "location": {
    "lat": 52.4332935,
    "lon": 13.231694
  },
  "ip": "192.168.178.54",
  "datetime": "2018-02-15T07:06:01"
}
```

Und das Gerät hat die folgende Pipeline-Definition.

```
{
    "pipeline": {
        "activities": [
            {
                "channel": {
                    "channelName": "foobar_channel",
                    "name": "foobar_channel_activity",
                    "next": "lambda_foobar_activity"
                }
            },
            {
                "lambda": {
                    "lambdaName": "MyAnalyticsLambdaFunction",
                    "batchSize": 5,
                    "name": "lambda_foobar_activity",
                    "next": "foobar_store_activity"
                }
            },
            {
                "datastore": {
                    "datastoreName": "foobar_datastore",
                    "name": "foobar_store_activity"
```

```
                }
            }
        ],
        "name": "foobar_pipeline",
        "arn": "arn:aws:iotanalytics:eu-west-1:123456789012:pipeline/foobar_pipeline"
    }
}
```

Die folgende Lambda-Python-Funktion (`MyAnalyticsLambdaFunction`) fügt der Nachricht die GMaps-URL und die Temperatur in Fahrenheit hinzu.

```
import logging
import sys

# Configure logging
logger = logging.getLogger()
logger.setLevel(logging.INFO)
streamHandler = logging.StreamHandler(stream=sys.stdout)
formatter = logging.Formatter('%(asctime)s - %(name)s - %(levelname)s - %(message)s')
streamHandler.setFormatter(formatter)
logger.addHandler(streamHandler)

def c_to_f(c):
    return 9.0/5.0 * c + 32

def lambda_handler(event, context):
    logger.info("event before processing: {}".format(event))
    maps_url = 'N/A'

    for e in event:
        #e['foo'] = 'addedByLambda'
        if 'location' in e:
            lat = e['location']['lat']
            lon = e['location']['lon']
            maps_url = "http://maps.google.com/maps?q={},{}".format(lat,lon)

        if 'temperature' in e:
            e['temperature_f'] = c_to_f(e['temperature'])

        logger.info("maps_url: {}".format(maps_url))
        e['maps_url'] = maps_url

    logger.info("event after processing: {}".format(event))
```

```
    return event
```

Beispiel 2 für Lambda-Funktion

Eine nützliche Technik zum Komprimieren und Serialisieren von Nachrichtennutzlasten, um die Übermittlungs- und Speicherkosten zu reduzieren. In diesem zweiten Beispiel geht die Lambda-Funktion davon aus, dass die Nachrichtennutzlast ein JSON-Original darstellt, das komprimiert und dann als Zeichenfolge base64-codiert (serialisiert) wurde. Es gibt das ursprüngliche JSON zurück.

```
import base64
import gzip
import json
import logging
import sys

# Configure logging
logger = logging.getLogger()
logger.setLevel(logging.INFO)
streamHandler = logging.StreamHandler(stream=sys.stdout)
formatter = logging.Formatter('%(asctime)s - %(name)s - %(levelname)s - %(message)s')
streamHandler.setFormatter(formatter)
logger.addHandler(streamHandler)

def decode_to_bytes(e):
    return base64.b64decode(e)

def decompress_to_string(binary_data):
    return gzip.decompress(binary_data).decode('utf-8')

def lambda_handler(event, context):
    logger.info("event before processing: {}".format(event))

    decompressed_data = []

    for e in event:
        binary_data = decode_to_bytes(e)
        decompressed_string = decompress_to_string(binary_data)

        decompressed_data.append(json.loads(decompressed_string))

    logger.info("event after processing: {}".format(decompressed_data))
```

```
    return decompressed_data
```

AddAttributes Aktivität

Eine `addAttributes`-Aktivität fügt Attribute basierend auf vorhandenen Attributen in der Nachricht hinzu. Auf diese Weise können Sie die Form der Nachricht ändern, bevor sie gespeichert wird. Verwenden Sie beispielsweise `addAttributes`, um Daten aus verschiedenen Generationen von Gerätefirmware zu normalisieren.

Betrachten Sie folgende Eingabemeldung.

```
{
    "device": {
        "id": "device-123",
        "coord": [ 47.6152543, -122.3354883 ]
    }
}
```

Die`addAttributes`Die Aktivität sieht wie folgt aus.

```
{
    "addAttributes": {
        "name": "MyAddAttributesActivity",
        "attributes": {
            "device.id": "id",
            "device.coord[0]": "lat",
            "device.coord[1]": "lon"
        },
        "next": "MyRemoveAttributesActivity"
    }
}
```

Diese Aktivität verschiebt die Geräte-ID auf die Stammebene und extrahiert den Wert in`coord`Array und stuft sie zu Attributen der obersten Ebene herauf`lat`und`lon`. Als Ergebnis dieser Aktivität wird die Eingabenachricht in das folgende Beispiel transformiert.

```
{
    "device": {
        "id": "device-123",
        "coord": [ 47.6, -122.3 ]
```

```
    },
    "id": "device-123",
    "lat": 47.6,
    "lon": -122.3
}
```

Das ursprüngliche Geräteattribut ist nach wie vor vorhanden. Wenn Sie es entfernen möchten, können Sie die `removeAttributes`-Aktivität verwenden.

RemoveAttributes Aktivität

Eine `removeAttributes`-Aktivität entfernt Attribute von einer Nachricht. Zum Beispiel angesichts der Botschaft, die das Ergebnis der`addAttributes`aktivität.

```
{
    "device": {
        "id": "device-123",
        "coord": [ 47.6, -122.3 ]
    },
    "id": "device-123",
    "lat": 47.6,
    "lon": -122.3
}
```

Um diese Nachricht zu normalisieren, sodass sie nur die erforderlichen Daten auf Stammebene enthält, verwenden Sie Folgendes:`removeAttributes`aktivität.

```
{
    "removeAttributes": {
        "name": "MyRemoveAttributesActivity",
        "attributes": [
            "device"
        ],
        "next": "MyDatastoreActivity"
    }
}
```

Daraus ergibt sich, dass die folgende Nachricht entlang der Pipeline fließt.

```
{
```

```
    "id": "device-123",
    "lat": 47.6,
    "lon": -122.3
}
```

SelectAttributes Aktivität

Die Aktivität `selectAttributes` erstellt eine neue Nachricht nur unter Verwendung der angegebenen Attribute aus der ursprünglichen Nachricht. Alle anderen Attribute werden verworfen. `selectAttributes` erstellt nur neue Attribute unter dem Stamm der Nachricht. Für die folgende Nachricht:

```
{
    "device": {
        "id": "device-123",
        "coord": [ 47.6152543, -122.3354883 ],
        "temp": 50,
        "hum": 40
    },
    "light": 90
}
```

und diese Aktivität:

```
{
    "selectAttributes": {
        "name": "MySelectAttributesActivity",
        "attributes": [
            "device.temp",
            "device.hum",
            "light"
        ],
        "next": "MyDatastoreActivity"
    }
}
```

Das Ergebnis ist die folgende Nachricht, die durch die Pipeline fließt.

```
{
    "temp": 50,
```

```
    "hum": 40,
    "light": 90
}
```

Auch hier gilt, dass `selectAttributes` nur Objekte auf Stammebene erstellen kann.

Filtern von Aktivitäten

Eine `filter`-Aktivität filtert eine Nachricht basierend auf ihren Attributen. Der in dieser Aktivität verwendete Ausdruck sieht aus wie ein SQL`WHERE`-Klausel, die einen booleschen Wert zurückgeben muss.

```
{
    "filter": {
        "name": "MyFilterActivity",
        "filter": "temp > 40 AND hum < 20",
        "next": "MyDatastoreActivity"
    }
}
```

DeviceRegistryEnrich Aktivität

Die`deviceRegistryEnrich`ermöglicht es Ihnen, Daten aus demAWS IoT-Geräte-Registry für Ihre Nachrichtennutzlast. Betrachten wir beispielsweise die folgende Nachricht:

```
{
    "temp": 50,
    "hum": 40,
    "device" {
        "thingName": "my-thing"
    }
}
```

und eine `deviceRegistryEnrich`-Aktivität, die wie folgt aussieht:

```
{
    "deviceRegistryEnrich": {
        "name": "MyDeviceRegistryEnrichActivity",
        "attribute": "metadata",
        "thingName": "device.thingName",
```

```
        "roleArn": "arn:aws:iam::<your-account-number>:role:MyEnrichRole",
        "next": "MyDatastoreActivity"
    }
}
```

Die Ausgabemeldung sieht jetzt wie in diesem Beispiel aus.

```
{
    "temp" : 50,
    "hum" : 40,
    "device" {
        "thingName" : "my-thing"
    },
    "metadata" : {
        "defaultClientId": "my-thing",
        "thingTypeName": "my-thing",
        "thingArn": "arn:aws:iot:us-east-1:<your-account-number>:thing/my-thing",
        "version": 1,
        "thingName": "my-thing",
        "attributes": {},
        "thingId": "aaabbbccc-dddeeef-gghh-jjkk-llmmnnoopp"
    }
}
```

Sie müssen eine Rolle im Feld `roleArn` der Aktivitätsdefinition festlegen, die über die entsprechenden Berechtigungen verfügt. Die Rolle muss über eine Berechtigungsrichtlinie verfügen, die wie im folgenden Beispiel aussieht.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeThing"
            ],
            "Resource": [
                "arn:aws:iot:<region>:<account-id>:thing/<thing-name>"
            ]
        }
    ]
}
```

und eine Vertrauensrichtlinie, die wie folgt aussieht:

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

DeviceShadowEnrich Aktivität

EIN`deviceShadowEnrich`Aktivität fügt Informationen aus demAWS IoT-Geräteschatten-Service für eine Nachricht. Betrachten wir beispielsweise die folgende Nachricht:

```
{
    "temp": 50,
    "hum": 40,
    "device": { "thingName": "my-thing" }
}
```

und die folgende `deviceShadowEnrich`-Aktivität:

```
{
    "deviceShadowEnrich": {
        "name": "MyDeviceShadowEnrichActivity",
        "attribute": "shadow",
        "thingName": "device.thingName",
        "roleArn": "arn:aws:iam::<your-account-number>:role:MyEnrichRole",
        "next": "MyDatastoreActivity"
    }
}
```

Das Ergebnis ist eine Meldung, die wie das folgende Beispiel aussieht.

```
{
    "temp": 50,
    "hum": 40,
    "device": {
        "thingName": "my-thing"
    },
    "shadow": {
        "state": {
            "desired": {
                "attributeX": valueX, ...
            },
            "reported": {
                "attributeX": valueX, ...
            },
            "delta": {
                "attributeX": valueX, ...
            }
        },
        "metadata": {
            "desired": {
                "attribute1": {
                    "timestamp": timestamp
                }, ...
            },
            "reported": ": {
                "attribute1": {
                    "timestamp": timestamp
                }, ...
            }
        },
        "timestamp": timestamp,
        "clientToken": "token",
        "version": version
    }
}
```

Sie müssen eine Rolle im Feld `roleArn` der Aktivitätsdefinition festlegen, die über die entsprechenden Berechtigungen verfügt. Die Rolle muss über eine Berechtigungsrichtlinie verfügen, die wie folgt aussieht.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:GetThingShadow"
            ],
            "Resource": [
                "arn:aws:iot:<region>:<account-id>:thing/<thing-name>"
            ]
        }
    ]
}
```

und eine Vertrauensrichtlinie, die wie folgt aussieht:

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

Mathematische Aktivität

Eine `math`-Aktivität berechnet einen arithmetischen Ausdruck unter Verwendung der Attribute der Nachricht. Der Ausdruck muss eine Zahl zurückgeben. Beispielsweise angesichts der folgenden Eingangsnachricht:

```
{
    "tempF": 50,
}
```

nach der Verarbeitung durch die folgende `math` Aktivität:

```
{
    "math": {
        "name": "MyMathActivity",
        "math": "(tempF - 32) / 2",
        "attribute": "tempC",
        "next": "MyDatastoreActivity"
    }
}
```

die resultierende Nachricht sieht wie folgt aus:

```
{
    "tempF" : 50,
    "tempC": 9
}
```

Operatoren und Funktionen für Mathematische Aktivitäten

Sie können die folgenden Operatoren in einer `math`-Aktivität verwenden:

+	Addition
-	Subtraktion
*	Multiplikation
/	Division
%	Modulo

Sie können die folgenden Funktionen in einer `math`-Aktivität verwenden:

- abs(Decimal)
- acos(Decimal)
- asin(Decimal)

- atan(Decimal)
- atan2(Decimal, Decimal)
- ceil(Decimal)
- cos(Decimal)
- cosh(Decimal)
- exp(Decimal)
- ln(Decimal)
- log(Decimal)
- mod(Decimal, Decimal)
- power(Decimal, Decimal)
- round(Decimal)
- sign(Decimal)
- sin(Decimal)
- sinh(Decimal)
- sqrt(Decimal)
- tan(Decimal)
- tanh(Decimal)
- trunc (Dezimal, Integer)

abs(Decimal)

Gibt den absoluten Wert einer Zahl zurück.

Beispiele:`abs(-5)`gibt 5 zurück.

Argumenttyp	Ergebnis
`Int`	`Int`, der absolute Wert des Arguments
`Decimal`	`Decimal`, der absolute Wert des Arguments
`Boolean`	`Undefined` .

Argumenttyp	Ergebnis
`String`	`Decimal`. Das Ergebnis ist der absolute Wert des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` .
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

acos(Decimal)

Gibt den umgekehrten Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`acos(0)` = 1.5707963267948966

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Boolean`	`Undefined` .
`String`	`Decimal`(mit doppelter Genauigkeit) der umgekehrte Kosinus des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann,

Argumenttyp	Ergebnis
	ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

asin(Decimal)

Gibt den umgekehrten Sinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`asin(0)` = 0.0

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Sinus des Arguments. Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre

Argumenttyp	Ergebnis
	Ergebnisse werden als `Undefined` zurückgegeben.
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

atan(Decimal)

Gibt den umgekehrten Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`atan(0)` = 0.0

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Tangens des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Tangens des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der umgekehrte Tangens des Arguments . Wenn die Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` .

Argumenttyp	Ergebnis
	Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

atan2(Decimal, Decimal)

Gibt den Winkel im Bogenmaß zwischen der positiven x-Achse und dem Punkt (x, y) an, der in den beiden Argumenten definiert ist. Der Winkel ist positiv für Winkel gegen den Uhrzeigersinn (obere Halbebene, y > 0) und negativ für Winkel im Uhrzeigersinn`Decimal`Argumente werden vor der Anwendung der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`atan(1, 0)` = 1.5707963267948966

Argumenttyp	Argumenttyp	Ergebnis
`Int` / `Decimal`	`Int` / `Decimal`	`Decimal`(mit doppelter Genauigkeit), der Winkel zwischen der X-Achse und dem angegebenen (x, y) Punkt
`Int` / `Decimal` / `String`	`Int` / `Decimal` / `String`	`Decimal`, der umgekehrt e Tangens des beschrieb enen Punkts. Wenn eine Zeichenfolge nicht konvertiert werden kann, ist das Ergebnis `Undefined` .
Anderer Wert	Anderer Wert	`Undefined` .

ceil(Decimal)

Rundet den angegebenen `Decimal`-Wert auf den nächsten `Int`-Wert auf.

Beispiele:

`ceil(1.2)` = 2

`ceil(11.2)` = -1

Argumenttyp	Ergebnis
`Int`	`Int`, der Argumentwert
`Decimal`	`Int`wird der String konvertiert in`Decimal`und auf den nächsten aufgerundet`Int`. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
Anderer Wert	`Undefined` .

cos(Decimal)

Gibt den Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`cos(0)` = 1

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.

Argumenttyp	Ergebnis
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der Kosinus des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

cosh(Decimal)

Gibt den hyperbolischen Kosinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`cosh(2.3)` = 5,037220649268761

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments. Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.

Argumenttyp	Ergebnis
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Kosinus des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` . Imaginäre Ergebnisse werden als `Undefined` zurückgegeben.
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

exp(Decimal)

Rückgabewerteauf das Dezimalargument angehoben.`Decimal`Argumente werden vor der Anwendung der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`exp(1)` = 1

Argumenttyp	Ergebnis
`Int`	`Decimal`(mit doppelter Genauigkeit), e^Argument.
`Decimal`	`Decimal`(mit doppelter Genauigkeit), e^argument
`String`	`Decimal`(mit doppelter Genauigkeit), e^Argument. Wenn das Symbol`String`kann nicht in ein umgewandelt werden`Decimal`, das Ergebnis von`Undefined` .

Argumenttyp	Ergebnis
Anderer Wert	`Undefined` .

ln(Decimal)

Gibt den natürlichen Logarithmus des Arguments zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`ln(e)` = 1

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der natürliche Logarithmus des Arguments
`Decimal`	`Decimal`(mit doppelter Genauigkeit), das natürliche Protokoll des Arguments
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der natürliche Logarithmus des Arguments Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

log(Decimal)

Gibt den Logarithmus des Arguments zur Basis 10 zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`log(100)` = 2.0

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der Logarithmus des Arguments zur Basis 10 Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
Array	`Undefined` .
Objekt	`Undefined` .
Null	`Undefined` .
Undefined	`Undefined` .

mod(Decimal, Decimal)

Gibt den Rest der Division des ersten Arguments des zweiten Arguments zurück. Sie können auch`%`als Infix-Operator für dieselbe Modulo-Funktionalität.

Beispiele:`mod(8, 3)` = 3

Linker Operand	Rechter Operand	Ausgabe
`Int`	`Int`	`Int`, das erste Argument modulo des zweiten Arguments.
`Int` / `Decimal`	`Int` / `Decimal`	`Decimal`, das erste Argument modulo des zweiten Arguments.
`String` / `Int` / `Decimal`	`String` / `Int` / `Decimal`	Wenn alle Strings konvertiert werden in`Decimals`, das Ergebnis, wenn das erste Argument modulo das zweite Argument ist. Andernfalls `Undefined` .
Anderer Wert	Anderer Wert	`Undefined` .

power(Decimal, Decimal)

Gibt das erste Argument, potenziert mit dem zweiten Argument, zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`power(2, 5)` = 32,0

Argumenttyp 1	Argumenttyp 2	Ausgabe
`Int` / `Decimal`	`Int` / `Decimal`	Ein `Decimal`-Wert (mit doppelter Genauigkeit), das erste Argument, potenziert mit dem zweiten Argument
`Int` / `Decimal` / `String`	`Int` / `Decimal` / `String`	Ein `Decimal`-Wert (mit doppelter Genauigkeit), das erste Argument, potenziert mit dem zweiten Argument

Argumenttyp 1	Argumenttyp 2	Ausgabe
		Beliebige Strings werden konvertiert in`Decimals`. Wenn `String`-Werte nicht in `Decimal`-Werte umgewandelt werden können, ist das Ergebnis `Undefined` .
Anderer Wert	Anderer Wert	`Undefined` .

round(Decimal)

Runden den angegebenen `Decimal`-Wert auf den nächsten `Int`-Wert. Wenn der `Decimal`-Wert genau in der Mitte zwischen zwei `Int`-Werten liegt (z. B. 0,5), wird der `Decimal`-Wert aufgerundet.

Beispiele:

`Round(1.2)` = 1

`Round(1.5)` = 2

`Round(1.7)` = 2

`Round(-1.1)` = -1

`Round(-1.5)` = -2

Argumenttyp	Ergebnis
`Int`	Das Argument
`Decimal`	`Decimal` wird auf den nächsten `Int`-Wert abgerundet.
`String`	`Decimal` wird auf den nächsten `Int`-Wert abgerundet. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .

Argumenttyp	Ergebnis
Anderer Wert	`Undefined` .

sign(Decimal)

Gibt das Vorzeichen der angegebenen Zahl zurück. Wenn das Vorzeichen des Arguments positiv ist, wird 1 zurückgegeben. Wenn das Vorzeichen des Arguments negativ ist, wird -1 zurückgegeben. Wenn das Argument 0 ist, wird 0 zurückgegeben.

Beispiele:

`sign(-7)` = -1

`sign(0)`= 0

`sign(13)` = 1

Argumenttyp	Ergebnis
`Int`	`Int`, das Vorzeichen des `Int`-Werts
`Decimal`	`Int`, das Vorzeichen des `Decimal`-Werts
`String`	`Int`, das Vorzeichen des `Decimal`-Werts Die Zeichenfolge, wenn sie in eine konvertie rt wird`Decimal`Wert und das Zeichen der`Decimal`Wert wird zurückgegeben. Wenn der `String`-Wert nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
Anderer Wert	`Undefined` .

sin(Decimal)

Gibt den Sinus einer Zahl im Bogenmaß zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`sin(0)` = 0.0

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der Sinus des Arguments.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der Sinus des Arguments.
`Boolean`	`Undefined` .
`String`	`Decimal`, der Sinus des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
`Array`	`Undefined` .
`Object`	`Undefined` .
`Null`	`Undefined` .
`Undefined`	`Undefined` .

sinh(Decimal)

Gibt den hyperbolischen Sinus einer Zahl zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet. Das Ergebnis ist ein `Decimal`-Wert mit doppelter Genauigkeit.

Beispiele:`sinh(2.3)` = 4,936961805545957

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Sinus des Arguments.

Argumenttyp	Ergebnis
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Sinus des Arguments.
`Boolean`	`Undefined` .
`String`	`Decimal`, der hyperbolische Sinus des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
`Array`	`Undefined` .
`Object`	`Undefined` .
`Null`	`Undefined` .
`Undefined`	`Undefined` .

sqrt(Decimal)

Gibt die Quadratwurzel einer Zahl zurück. `Decimal`-Argumente werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`sqrt(9)` = 3.0

Argumenttyp	Ergebnis
`Int`	Die Quadratwurzel des Arguments.
`Decimal`	Die Quadratwurzel des Arguments.
`Boolean`	`Undefined` .
`String`	Die Quadratwurzel des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .

Argumenttyp	Ergebnis
`Array`	`Undefined` .
`Object`	`Undefined` .
`Null`	`Undefined` .
`Undefined`	`Undefined` .

tan(Decimal)

Gibt den Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`tan(3)` = -0,1425465430742778

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments.
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments.
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der Tangens des Arguments. Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
`Array`	`Undefined` .
`Object`	`Undefined` .
`Null`	`Undefined` .
`Undefined`	`Undefined` .

tanh(Decimal)

Gibt den hyperbolischen Tangens einer Zahl im Bogenmaß zurück. `Decimal`-Werte werden vor dem Anwenden der Funktion auf doppelte Genauigkeit gerundet.

Beispiele:`tanh(2.3)` = 0.9800963962661914

Argumenttyp	Ergebnis
`Int`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments
`Decimal`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments
`Boolean`	`Undefined` .
`String`	`Decimal` (mit doppelter Genauigkeit), der hyperbolische Tangens des Arguments Wenn die Zeichenfolge nicht in einen `Decimal`-Wert konvertiert werden kann, ist das Ergebnis `Undefined` .
`Array`	`Undefined` .
`Object`	`Undefined` .
`Null`	`Undefined` .
`Undefined`	`Undefined` .

trunc (Dezimal, Integer)

Schneidet das erste Argument auf die Anzahl von `Decimal`-Stellen ab, die vom zweiten Argument festgelegt wurden. Wenn das zweite Argument kleiner ist als Null, wird es auf Null festgelegt. Wenn das zweite Argument größer ist als 34, wird es auf 34 festgelegt. Nachgestellte Nullen werden aus dem Ergebnis entfernt.

Beispiele:

`trunc(2.3, 0)` = 2

`trunc(2.3123, 2)`= 2,31

`trunc(2.888, 2)`= 2,88

`trunc(2.00, 5)` = 2

Argumenttyp 1	Argumenttyp 2	Ergebnis
`Int`	`Int`	Der Quellwert
`Int` / `Decimal` / `String`	`Int` / `Decimal`	Das erste Argument wird auf die Länge abgeschnitten, die vom zweiten Argument beschrieben wird. Wenn das zweite Argument kein `Int`-Wert ist, wird es auf den nächsten `Int`-Wert abgerundet. Strings werden konvertiert in`Decimal`values. Wenn die Konvertierung der Zeichenfolge fehlschlägt, ist das Ergebnis `Undefined` .
Anderer Wert		Undefined

RunPipelineActivity

Hier finden Sie ein Beispiel dafür, wie Sie die verwenden`RunPipelineActivity`Befehl zum Testen einer Pipeline-Aktivität. In diesem Beispiel testen wir eine Mathematische Aktivität.

1. Erstellen eines`maths.json`-Datei, die die Definition der Pipeline-Aktivität enthält, die Sie testen möchten.

```
{
    "math": {
        "name": "MyMathActivity",
```

```
        "math": "((temp - 32) * 5.0) / 9.0",
        "attribute": "tempC"
    }
}
```

2. Erstellen einer Dateipayloads.json-Datei, die die Beispiel-Payloads enthält, die zum Testen der Pipeline-Aktivität verwendet werden.

```
[
    "{\"humidity\": 52, \"temp\": 68 }",
    "{\"humidity\": 52, \"temp\": 32 }"
]
```

3. Rufen Sie dieRunPipelineActivitiesOperation über die Befehlszeile.

```
aws iotanalytics run-pipeline-activity  --pipeline-activity file://maths.json  --
payloads file://payloads.json --cli-binary-format raw-in-base64-out
```

   Daraus ergeben sich folgende Ergebnisse.

```
{
    "logResult": "",
    "payloads": [
        "eyJodW1pZGl0eSI6NTIsInRlbXAiOjY4LCJ0ZW1wQyI6MjB9",
        "eyJodW1pZGl0eSI6NTIsInRlbXAiOjMyLCJ0ZW1wQyI6MH0="
    ]
}
```

   Die in den Ergebnissen aufgeführten Nutzlasten sind im Base64-Format codierte Zeichenfolgen. Wenn diese Strings dekodiert werden, erhalten Sie die folgenden Ergebnisse.

```
{"humidity":52,"temp":68,"tempC":20}
{"humidity":52,"temp":32,"tempC":0}
```

Wiederaufarbeitung von Channel-Nachrichten

AWS IoT Analyticsermöglicht es Ihnen, Kanaldaten neu zu verarbeiten. Dies kann in den folgenden Fällen nützlich sein:

- Wenn Sie bereits übernommene Daten wiedergeben möchten, anstatt von Neuem zu starten.
- Sie aktualisieren eine Aktualisierung einer Pipeline und möchten vorhandene Daten abrufen up-to-date mit den Änderungen.
- Sie möchten Daten einschließen, die aufgenommen wurden, bevor Sie Änderungen an den vom Kunden verwalteten Speicheroptionen, Berechtigungen für Channels oder am Datenspeicher vorgenommen haben.

Parameter

Wenn Sie Channel-Nachrichten über die Pipeline mit erneut verarbeitenAWS IoT Analyticsauswählen, müssen Sie die folgenden Informationen angeben:

`StartPipelineReprocessing`

Startet mit der erneuten Verarbeitung von Channel-Nachrichten über die Pipeline.

`ChannelMessages`

Gibt eine oder mehrere Sätze von Channel-Nachrichten an, die Sie erneut verarbeiten möchten.

Wenn Sie das`channelMessages`-Objekt müssen Sie nicht einen Wert für angeben`startTime`und`endTime`aus.

`s3Paths`

Gibt einen oder mehrere Schlüssel an, die die Amazon Simple Storage Service (Amazon S3) -Objekte identifizieren, die Ihre Channel-Nachrichten speichern. Sie müssen den vollständigen Pfad für den Schlüssel verwenden.

Beispiel-Pfad:`00:00:00/1582940490000_1582940520000_123456789012_mychannel_0_2118.0.`

Type: Zeichenfolgen-Array

Beschränkungen für Array-Elemente: 1-100 Elemente.

Längenbeschränkungen: 1-1024 Zeichen.

`endTime`

Die Endzeit (ausschließlich) der Channel-Daten, die erneut verarbeitet werden.

Wenn Sie einen Wert für die`endTime`-Parameter dürfen Sie nicht den`channelMessages`-Objekt.

Type: Zeitstempel

`startTime`

Die Startzeit (einschließlich) der Rohnachrichtendaten, die erneut verarbeitet werden.

Wenn Sie einen Wert für die`startTime`-Parameter dürfen Sie nicht den`channelMessages`-Objekt.

Type: Zeitstempel

`pipelineName`

Der Name der Pipeline, für die die erneute Verarbeitung gestartet werden soll.

Type: String (Zeichenfolge)

Längenbeschränkungen: 1-128 Zeichen.

Erneute Verarbeitung von Channel-Nachrichten (Konsole)

Dieses Tutorial zeigt Ihnen, wie Sie die Kanaldaten, die im angegebenen Amazon S3 S3-Objekt im AWS IoT Analyticsconsole.

Bevor Sie beginnen, stellen Sie sicher, dass die Channel-Nachrichten, die Sie erneut verarbeiten möchten, in einem vom Kunden verwalteten Amazon S3 S3-Bucket gespeichert werden.

1. Melden Sie sich an der AWS IoT Analytics-Konsole an.
2. Wählen Sie im Navigationsbereich und dann aus.Pipelinesaus.
3. Wählen Sie Ihre Zielpipeline aus.
4. Klicken Sie aufNachrichten erneut verarbeitenvonAktionenaus.

5. Auf derWiederaufbereitung von Pipelineangehören, wählen SieS3-ObjektezumNachrichten erneut verarbeitenaus.

   DieAWS IoT Analyticsconsole bietet auch die folgenden Optionen:

   - Alle verfügbaren Produktreihen- Verarbeiten Sie alle gültigen Daten im Kanal erneut.
   - Letzte 120 Tage- Verarbeiten Sie Daten, die in den letzten 120 Tagen eingetroffen sind, erneut.
   - Letzte 90 Tage- Erneute Verarbeitung von Daten, die in den letzten 90 Tagen angekommen sind.
   - Letzte 30 Tage- Erneute Verarbeitung von Daten, die in den letzten 30 Tagen angekommen sind.
   - Benutzerdefinierter Bereich- Verarbeiten Sie Daten, die im angegebenen Zeitraum eingetroffen sind, erneut. Sie können einen beliebigen Zeitraum wählen.
6. Geben Sie den Schlüssel des Amazon S3 S3-Gehorchts ein, der Ihre Channel-Nachrichten speichert.

   Um den Schlüssel zu finden, gehen Sie wie folgt vor:

   a. Rufen Sie aufAmazon S3-Konsoleaus.
   b. Wählen Sie das Amazon-S3-Ziel-Objekt aus.
   c. UnterEigenschaften, imÜbersicht über Objekte, kopieren Sie den Schlüssel.
7. Klicken Sie aufMit der Wiederaufbereitung beginnenaus.

Kanalnachrichten erneut verarbeiten (API)

Wenn Sie die`StartPipelineReprocessing`API, beachten Sie Folgendes:

- Die`startTime`und`endTime`Parameter geben an, wann die Rohdaten übernommen wurden, dies sind jedoch grobe Schätzungen. Sie können auf die nächste ganze Stunde runden. Die`startTime`ist inklusive, aber der`endTime`ist exklusiv.
- Der Befehl startet die erneute Verarbeitung asynchron und liefert eine sofortige Rückgabe.
- Es gibt keine Garantie dafür, dass erneut verarbeitete Nachrichten in der Reihenfolge ihres ursprünglichen Eingangs verarbeitet werden. Sie ist ungefähr die gleiche, aber nicht exakt dieselbe.
- Sie können bis zu 1000 machen`StartPipelineReprocessing`API fordert alle 24 Stunden an, dieselben Channel-Nachrichten über eine Pipeline erneut zu verarbeiten.

- Die erneute Verarbeitung Ihrer Rohdaten verursacht zusätzliche Kosten.

Weitere Informationen finden Sie im .StartPipelineReprocessingAPI, inAWS IoT Analytics-API-Referenzaus.

Abbrechen von Aktivitäten zur Kanalwiederaufbereitung

Um eine Wiederverarbeitungsaktivität der Pipeline abzubrechen, verwenden Sie dieCancelPipelineReprocessingAPI oder wählenErneute Verarbeitung abbrechenauf derAktivitätenangezeigter imAWS IoT Analyticsconsole. Wenn Sie die Wiederaufbereitung abbrechen, werden die restlichen Daten nicht wiederverarbeitet. Sie müssen eine weitere Wiederverarbeitungsanfrage starten.

Verwenden derDescribePipelineAPI, um den Status der erneuten Verarbeitung zu überprüfen. Sehen Sie die`reprocessingSummaries`Feld in der Antwort.

Automatisieren Sie Ihren Workflow

AWS IoT Analyticsbietet erweiterte Datenanalyse fürAWS IoT. Sie können IoT-Daten mit Datenanalyse- und Machine-Learning-Tools automatisch sammeln, verarbeiten, speichern und analysieren. Sie können Container ausführen, die Ihren eigenen benutzerdefinierten Analysecode oder Jupyter Notebook hosten, oder benutzerdefinierte Code-Container von Drittanbietern verwenden, sodass Sie vorhandene Analysetools nicht neu erstellen müssen. Sie können Eingabedaten mit den folgenden Funktionen aus einem Datenspeicher abrufen und in einen automatisierten Workflow einspeisen:

Dataset-Inhalte im Rahmen eines sich wiederholenden

Planen Sie die automatische Erstellung von Datensatzinhalten, indem Sie beim Aufruf einen Trigger angeben`CreateDataset`(`triggers:schedule:expression`) enthalten. Daten, die sich in einem Datenspeicher befinden, werden zum Erstellen des Datensatzinhalts verwendet. Sie wählen die gewünschten Felder mit einer SQL-Abfrage aus (`actions:queryAction:sqlQuery`) enthalten.

Definieren Sie ein nicht überlappendes, zusammenhängendes Zeitintervall, um sicherzustellen, dass der Inhalt des neuen Datensatzes nur die Daten enthält, die seit dem letzten Mal eingetroffen sind. Verwenden der`actions:queryAction:filters:deltaTime`und`:offsetSeconds`Felder zur Angabe des Delta-Zeitintervalls. Geben Sie dann einen Trigger an, um den Inhalt der Datenmenge zu erstellen, wenn das Zeitintervall abgelaufen ist. Siehe the section called “Beispiel 6 — Erstellen einer SQL-Datenmenge mit einem Delta-Fenster (CLI)”.

Datensatz-Inhalt nach Abschluss eines anderen Datensatzes erstellen

Die Erstellung neuer Datensatz-Inhalte auslösen, wenn die Inhaltserstellung eines anderen Datensatzes`triggers:dataset:name`.

Automatisches Ausführen Ihrer Analyseanwendungen

Containerisieren Sie Ihre eigenen, benutzerdefinierten Datenanalyseanwendungen und lösen Sie sie aus, wenn der Inhalt eines anderen Datensatzes erstellt wird. Auf diese Weise können Sie Ihre Anwendung mit Daten aus dem Inhalt eines Datensatzes versorgen, der nach einem wiederkehrenden Zeitplan erstellt wurde. Sie können die Ergebnisse Ihrer Analyse automatisch aus Ihrer Anwendung heraus bearbeiten. (`actions:containerAction`)

Datensatz-Inhalt nach Abschluss eines anderen Datensatzes erstellen

Die Erstellung neuer Datensatz-Inhalte auslösen, wenn die Inhaltserstellung eines anderen Datensatzes`triggers:dataset:name`.

Automatisches Ausführen Ihrer Analyseanwendungen

Containerisieren Sie Ihre eigenen, benutzerdefinierten Datenanalyseanwendungen und lösen Sie sie aus, wenn der Inhalt eines anderen Datensatzes erstellt wird. Auf diese Weise können Sie Ihre Anwendung mit Daten aus dem Inhalt eines Datensatzes versorgen, der nach einem wiederkehrenden Zeitplan erstellt wurde. Sie können die Ergebnisse Ihrer Analyse automatisch aus Ihrer Anwendung heraus bearbeiten. (`actions:containerAction`)

Anwendungsfälle

Automatisieren Sie die Messung der Produktqualität um OpEx

Sie verfügen über ein System mit einem intelligenten Ventil, das Druck, Luftfeuchtigkeit und Temperatur misst. Das System sammelt Ereignisse regelmäßig und auch dann, wenn bestimmte Ereignisse eintreten, z. B. wenn ein Wert geöffnet und geschlossen wird. mitAWS IoT Analyticskönnen Sie eine Analyse automatisieren, die nicht überlappende Daten aus diesen periodischen Fenstern aggregiert und KPI-Berichte zur Endproduktqualität erstellt. Nach der Verarbeitung jeder Charge messen Sie die Gesamtproduktqualität und senken Ihre Betriebskosten durch maximiertes Auflagenvolumen.

Automatisieren der Analyse einer Geräteflotte

Sie führen alle 15 Minuten Analysen (Algorithmus, Data Science oder ML für KPI) für Daten aus, die von Hunderten von Geräten generiert wurden. Mit jedem Analysezyklus wird der Status für den nächsten Analyselauf generiert und gespeichert. Für jede Ihrer Analysen möchten Sie nur die Daten verwenden, die in einem angegebenen Zeitfenster empfangen wurden. mitAWS IoT AnalyticsSie können Ihre Analysen orchestrieren und den KPI und den Bericht für jeden Lauf erstellen und dann die Daten für future Analysen speichern.

Automatisieren der Anomalieerkennung

AWS IoT Analyticsermöglicht es Ihnen, Ihren Workflow zur Erkennung von Anomalien zu automatisieren, den Sie manuell alle 15 Minuten für neue Daten ausführen müssen, die in einem Datenspeicher eingetroffen sind. Sie können auch ein Dashboard automatisieren, das die Gerätenutzung und die wichtigsten Benutzer innerhalb eines bestimmten Zeitraums anzeigt.

Prognostizieren von Ergebnissen bei industriellen Verfahren

Sie haben industrielle Produktionslinien. Verwendung der an gesendeten DatenAWS IoT Analytics, einschließlich verfügbarer Prozessmessungen, können Sie die analytischen Workflows operationalisieren, um Prozessergebnisse vorherzusagen. Die Daten für das Modell können in einer M x N-Matrix angeordnet werden, wobei jede Zeile Daten von verschiedenen Zeitpunkten enthält, an denen Laborproben entnommen werden.AWS IoT Analyticshilft Ihnen, Ihren analytischen Workflow zu operationalisieren, indem Delta-Fenster erstellt und Ihre Data-Science-Tools verwendet werden, um KPIs zu erstellen und den Zustand der Messgeräte zu speichern.

Verwenden eines Docker-Containers

Dieser Abschnitt enthält Informationen zur Erstellung eines eigenen Docker-Containers. Es stellt ein Sicherheitsrisiko dar, wenn Sie Docker-Container von Drittanbietern wiederverwenden: Diese Container können beliebigen Code mit Ihren Benutzerberechtigungen ausführen. Stellen Sie sicher, dass Sie dem Autor von Drittanbieter-Containern vertrauen, bevor Sie ihn verwenden.

Hier werden die Schritte zum Einrichten von regelmäßigen Datenanalysen von Daten beschrieben, die seit der letzten Ausführung der Analyse angekommen sind:

1. Erstellen Sie einen Docker-Container, der Ihre Datenanwendung sowie alle erforderlichen Bibliotheken oder andere Abhängigkeiten enthält.

   Die IotAnalytics Die Jupyter-Erweiterung bietet eine Containerisierungs-API zur Unterstützung des Containerisierungsprozesses. Sie können auch Images Ihrer eigenen Kreation ausführen, in denen Sie Ihr Anwendungs-Toolset erstellen oder zusammenstellen, um die gewünschte Datenanalyse oder Berechnung durchzuführen.AWS IoT Analyticsermöglicht es Ihnen, die Quelle der Eingabedaten für die containerisierte Anwendung und das Ziel für die Ausgabedaten des Docker-Containers anhand von Variablen zu definieren. (Benutzerdefinierte Docker-Container-Eingabe-/Ausgabevariablenenthält weitere Informationen über die Verwendung von Variablen mit einem benutzerdefinierten Container.)
2. Laden Sie den Container in eine Amazon ECR-Registry hoch.
3. Erstellen eines Datenspeichers zum Empfangen und Speichern von Nachrichten (Daten) von Geräten (`iotanalytics: CreateDatastore`)
4. Erstellen Sie einen Kanal, in dem die Nachrichten gesendet werden (`iotanalytics: CreateChannel`) enthalten.

5. Erstellen Sie eine Pipeline, um den Kanal mit dem Datenspeicher zu verbinden (`iotanalytics: CreatePipeline`) enthalten.
6. Erstellen Sie eine IAM-Rolle, die die Berechtigung zum Senden von Nachrichtendaten an eineAWS IoT Analytics-Kanal (`iam: CreateRole`.)
7. Erstellen Sie eine IoT-Regel, die eine SQL-Abfrage verwendet, um einen Kanal mit der Quelle der Nachrichtendaten zu verbinden (`iot: CreateTopicRule`Feld`topicRulePayload:actions:iotAnalytics`) enthalten. Wenn ein Gerät eine Nachricht mit dem entsprechenden Thema über MQTT sendet, wird sie an Ihren Kanal weitergeleitet. Oder Sie können verwenden`iotanalytics: BatchPutMessage`um Nachrichten direkt in einen Kanal von einem Gerät zu senden, dasAWSSDK oderAWS CLI.
8. Erstellen Sie eine SQL-Datenmenge, deren Erstellung durch einen Zeitplan ausgelöst wird (`iotanalytics: CreateDataset,`Feld`actions: queryAction:sqlQuery`) enthalten.

   Außerdem geben Sie einen Vorfilter an, der auf die Nachrichtendaten angewendet werden soll, um die Nachrichten auf die zu beschränken, die seit der letzten Ausführung der Aktion angekommen sind. (Feld.`actions:queryAction:filters:deltaTime:timeExpression`gibt einen Ausdruck, mit dem der Zeitpunkt einer Nachricht bestimmt werden kann. while field`actions:queryAction:filters:deltaTime:offsetSeconds`gibt eine mögliche Latenz beim Eintreffen einer Nachricht an.)

   Der Vorfilter bestimmt zusammen mit dem Trigger-Zeitplan Ihr Delta-Fenster. Jede neue SQL-Datenmenge wird anhand von Nachrichten erstellt, die seit der letzten Erstellung der SQL-Datenmenge empfangen wurden. (Was ist mit der ersten Erstellung der SQL-Datenmenge? Eine Schätzung, wann der Datensatz zum letzten Mal erstellt worden wäre, wird basierend auf dem Zeitplan und dem Vorfilter vorgenommen.)
9. Erstellen Sie einen weiteren Datensatz, der durch die Erstellung des ersten (CreateDatasetFeld`trigger:dataset`) enthalten. Für diesen Datensatz geben Sie eine Container-Aktion an (Feld`actions:containerAction`), das auf den Docker-Container verweist, den Sie im ersten Schritt erstellt haben, und Informationen enthält, die für die Ausführung benötigt werden. Hier legen Sie auch Folgendes fest:

   - Die ARN des in Ihrem Konto gespeicherten Docker-Containers (`image`.)
   - den ARN der Rolle, die dem System die Berechtigung zum Zugriff auf benötigte Ressourcen erteilt, damit die Container-Aktion ausgeführt werden kann (`executionRoleArn`)

- Die Konfiguration der Ressource, die die Container-Aktion ausführt (`resourceConfiguration`.)
- Der Typ der Datenverarbeitungsressource, die zur Ausführung der Container-Aktion verwendet wird (`computeType`mit möglichen Werten:`ACU_1 [vCPU=4, memory=16GiB] or ACU_2 [vCPU=8, memory=32GiB]`) enthalten.
- Die Größe (GB) des persistenten Speichers, der der Ressourcen-Instance zur Verfügung steht, um die Container-Aktion auszuführen (`volumeSizeInGB`) enthalten.
- Die Werte der Variablen, die im Kontext der Ausführung der Anwendung verwendet werden (im Wesentlichen Parameter, die an die Anwendung übergeben werden) (`variables`) enthalten.

  Diese Variablen werden ersetzt, wenn ein Container ausgeführt wird. Auf diese Weise können Sie denselben Container mit verschiedenen Variablen (Parametern) ausführen, die zum Zeitpunkt der Erstellung des Datensatzinhalts bereitgestellt werden. Die IotAnalytics Die Jupyter-Erweiterung vereinfacht diesen Prozess, indem sie die Variablen in einem Notebook automatisch erkennt und sie als Teil des Containerisierungsprozesses zur Verfügung stellt. Sie können die erkannten Variablen auswählen oder benutzerdefinierte Variablen hinzufügen. Vor der Ausführung eines Containers ersetzt das System jede dieser Variablen mit dem zum Zeitpunkt der Ausführung aktuellen Wert.
- Eine der Variablen ist der Name des Datensatzes, dessen neuester Inhalt als Eingabe für die Anwendung verwendet wird (dies ist der Name des Datensatzes, den Sie im vorherigen Schritt erstellt haben) (`datasetContentVersionValue:datasetName`) enthalten.

Mit der SQL-Abfrage und dem Delta-Fenster zum Generieren der Datenmenge und dem Container mit Ihrer AnwendungAWS IoT Analyticserstellt ein geplantes Produktions-Dataset, das in dem Intervall ausgeführt wird, das Sie für die Daten aus dem Delta-Fenster angegeben haben, um die gewünschte Ausgabe zu erzeugen

Sie können Ihre Produktions-Dataset-Anwendung anhalten und fortsetzen, wann immer Sie dies wünschen. Wenn Sie Ihre Anwendung für Produktionsdatensätze fortsetzen,AWS IoT Analyticsholt standardmäßig alle Daten ab, die seit der letzten Ausführung eingetroffen sind, aber noch nicht analysiert wurden. Sie können auch konfigurieren, wie Sie Ihr Produktions-Dataset (Auftragsfensterlänge) fortsetzen möchten, indem Sie eine Reihe aufeinanderfolgender Durchläufe ausführen. Alternativ können Sie Ihre Produktions-Dataset-Anwendung fortsetzen, indem Sie nur die neu eingetroffenen Daten erfassen, die in die angegebene Größe Ihres Delta-Fensters passen.

Bitte beachten Sie die folgenden Einschränkungen beim Erstellen oder Definieren eines Datensatzes, der durch die Erstellung eines anderen Datensatzes ausgelöst wird:

- Nur Container-Datasets können von SQL-Datensätzen ausgelöst werden.
- Eine SQL-Datenmenge kann maximal 10 Container-Datasets auslösen.

Beim Erstellen einer Container-Datenmenge, die von einer SQL-Datenmenge ausgelöst wird, können die folgenden Fehler zurückgegeben werden:

- "Triggering dataset can only be added on a container dataset" (Auslöser-Dataset kann nur auf ein Container-Dataset hinzugefügt werden.)
- "There can only be one triggering dataset" (Es kann nur ein Auslöser-Dataset geben.)

  Dieser Fehler tritt auf, wenn Sie versuchen, eine Container-Datenmenge zu definieren, die von zwei verschiedenen SQL-Datenmengen ausgelöst wird.
- „Der auslösende Datensatz <dataset-name>kann nicht durch einen Container-Datensatz ausgelöst werden“

  Dieser Fehler tritt auf, wenn Sie versuchen, eine andere Container-Datenmenge zu definieren, die von einer anderen Container-Datenmenge ausgelöst
- „<N>Datensätze sind bereits vom <dataset-name>Datensatz abhängig.“

  Dieser Fehler tritt auf, wenn Sie versuchen, eine andere Container-Datenmenge zu definieren, die von einer SQL-Datenmenge ausgelöst wird, die bereits 10 Container-Datasets aus
- "Exactly one trigger type should be provided" (Sie müssen genau einen Auslösertyp angeben.)

  Dieser Fehler tritt auf, wenn Sie versuchen, eine Datenmenge zu definieren, die sowohl von einem Zeitplanauslöser als auch von einem Datensatz-Trigger

Benutzerdefinierte Eingabe-/Ausgabevariablen für Docker-Container

In diesem Abschnitt wird gezeigt, wie ein Programm, das durch Ihr benutzerdefiniertes Docker-Image ausgeführt wird, Eingabevariablen lesen und die Ausgabe hochladen kann.

Params-Datei

Die Eingabevariablen und die Ziele, zu denen Sie die Ausgabe hochladen möchten, werden in einer JSON-Datei gespeichert. Sie finden sie unter `/opt/ml/input/data/iotanalytics/params` auf der Instance, die Ihr Docker-Image ausführt. Hier ist ein Beispiel für den Inhalt dieser Datei.

```
{
   "Context": {
       "OutputUris": {
           "html": "s3://aws-iot-analytics-dataset-xxxxxxx/notebook/results/
iotanalytics-xxxxxxx/output.html",
           "ipynb": "s3://aws-iot-analytics-dataset-xxxxxxx/notebook/results/
iotanalytics-xxxxxxx/output.ipynb"
       }
   },
   "Variables": {
       "source_dataset_name": "mydataset",
       "source_dataset_version_id": "xxxx",
       "example_var": "hello world!",
       "custom_output": "s3://aws-iot-analytics/dataset-xxxxxxx/notebook/results/
iotanalytics-xxxxxxx/output.txt"
   }
}
```

Zusätzlich zum Namen und zur Versions-ID Ihres Datasets enthält der Abschnitt `Variables` auch die Variablen, die im Aufruf `iotanalytics:CreateDataset` festgelegt werden – in diesem Beispiel wurde der Variable `example_var` der Wert `hello world!` zugeteilt. Eine benutzerdefinierte Ausgabe-URI wurde auch in der Variable `custom_output` angegeben. Das Feld `OutputUris` enthält Standard-Speicherorte, zu denen der Container seine Ausgabe hochladen kann – in diesem Beispiel wurden die Standard-Ausgabe-URIs sowohl für ipynb als auch für die HTML-Ausgabe angegeben.

Eingabevariablen.

Das von Ihrem Docker-Image gestartete Programm kann die Variablen aus der `params`-Datei lesen. Hier ist ein Beispielprogramm, das die`params`Datei, analysiert sie und gibt den Wert der`example_var`Variable.

```
import json

with open("/opt/ml/input/data/iotanalytics/params") as param_file:
    params = json.loads(param_file.read())
example_var = params["Variables"]["example_var"]
```

```
print(example_var)
```

Hochladen der Ausgabe

Das von Ihrem Docker-Image gestartete Programm speichert seine Ausgabe möglicherweise auch an einem Amazon S3 S3-Speicherort. Die Ausgabe muss mit einem“ geladen werdenbucket-owner-full-control„Zugriffskontrollliste. Die Zugriffsliste gewährtAWS IoT AnalyticsDienstkontrolle über die hochgeladene Ausgabe. In diesem Beispiel erweitern wir das vorherige, um den Inhalt von hochzuladen`example_var`an den Amazon-S3-Speicherort, der von`custom_output`in der`params`file.

```
import boto3
import json
from urllib.parse import urlparse

ACCESS_CONTROL_LIST = "bucket-owner-full-control"

with open("/opt/ml/input/data/iotanalytics/params") as param_file:
    params = json.loads(param_file.read())
example_var = params["Variables"]["example_var"]

outputUri = params["Variables"]["custom_output"]
# break the S3 path into a bucket and key
bucket = urlparse(outputUri).netloc
key = urlparse(outputUri).path.lstrip("/")

s3_client = boto3.client("s3")
s3_client.put_object(Bucket=bucket, Key=key, Body=example_var, ACL=ACCESS_CONTROL_LIST)
```

Berechtigungen

Sie müssen zwei -Rollen erstellen. Eine Rolle gewährt die Berechtigung zum Starten einer SageMaker -Instanz, um ein Notebook zu containerisieren. Eine weitere Rolle ist erforderlich, um einen Container auszuführen.

Sie können die erste Rolle automatisch oder manuell erstellen. Wenn du dein neues erstellst SageMakerInstanz mit demAWS IoT Analyticsconsole haben Sie die Möglichkeit, automatisch eine neue Rolle zu erstellen, die alle für die Ausführung erforderlichen Berechtigungen gewährt SageMaker Instanzen und Containerisierung von Notebooks. Sie können auch

eine Rolle mit diesen Berechtigungen manuell erstellen. Erstellen Sie dazu eine Rolle mit dem`AmazonSageMakerFullAccess`Richtlinie angehängt und die folgende Richtlinie hinzugefügt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:BatchDeleteImage",
        "ecr:BatchGetImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::iotanalytics-notebook-containers/*"
    }
  ]
}
```

Sie müssen die zweite Rolle manuell erstellen, die die Berechtigung zum Ausführen eines Containers gewährt. Sie müssen dies auch dann tun, wenn Sie das`AWS IoT Analytics`Konsole, um die erste Rolle automatisch zu erstellen. Erstellen Sie eine Rolle mit der folgenden Richtlinie und Vertrauensrichtlinie.

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

```
                "s3:GetBucketLocation",
                "s3:PutObject",
                "s3:GetObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::aws-*-dataset-*/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotanalytics:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "ecr:BatchCheckLayerAvailability",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie.

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

Verwendung der CreateDataset API via Java und dasAWS CLI

Erstellt ein Dataset Ein Dataset speichert Daten, die aus einem Datenspeicher abgerufen wurden, indem ein`queryAction`(eine SQL-Abfrage) oder ein`containerAction`(Ausführen einer containerisierten Anwendung). Dieser Vorgang erstellt das Grundgerüst einer Datenmenge. Die Datenmenge kann manuell durch Aufrufen aufgefüllt werden`CreateDatasetContent`oder automatisch nach einem`trigger`Sie geben an. Weitere Informationen finden Sie unterCreateDatasetund`CreateDatasetContent`.

Themen

- Beispiel 1 — Erstellen eines SQL-Datensatzes (Java)
- Beispiel 2 — Erstellen einer SQL-Datenmenge mit einem Delta-Fenster (Java)
- Beispiel 3 — Erstellen einer Container-Datenmenge mit einem eigenen Zeitplan-Trigger (Java)
- Beispiel 4 — Erstellen einer Container-Datenmenge mit einer SQL-Datenmenge als Trigger (Java)
- Beispiel 5 — Erstellen einer SQL-Datenmenge (CLI)
- Beispiel 6 — Erstellen einer SQL-Datenmenge mit einem Delta-Fenster (CLI)

Beispiel 1 — Erstellen eines SQL-Datensatzes (Java)

```
CreateDatasetRequest request = new CreateDatasetRequest();
request.setDatasetName(dataSetName);
DatasetAction action = new DatasetAction();
```

```
//Create Action
action.setActionName("SQLAction1");
action.setQueryAction(new SqlQueryDatasetAction().withSqlQuery("select * from
 DataStoreName"));

// Add Action to Actions List
List<DatasetAction> actions = new ArrayList<DatasetAction>();
actions.add(action);

//Create Trigger
DatasetTrigger trigger = new DatasetTrigger();
trigger.setSchedule(new Schedule().withExpression("cron(0 12 * * ? *)"));

//Add Trigger to Triggers List
List<DatasetTrigger> triggers = new ArrayList<DatasetTrigger>();
triggers.add(trigger);

// Add Triggers and Actions to CreateDatasetRequest object
request.setActions(actions);
request.setTriggers(triggers);

// Add RetentionPeriod to CreateDatasetRequest object
request.setRetentionPeriod(new RetentionPeriod().withNumberOfDays(10));
final CreateDatasetResult result = iot.createDataset(request);
```

Ausgabe bei Erfolg:

```
{DatasetName: <datatsetName>, DatasetArn: <datatsetARN>, RetentionPeriod: {unlimited:
 true} or {numberOfDays: 10, unlimited: false}}
```

Beispiel 2 — Erstellen einer SQL-Datenmenge mit einem Delta-Fenster (Java)

```
CreateDatasetRequest request = new CreateDatasetRequest();
request.setDatasetName(dataSetName);
DatasetAction action = new DatasetAction();

//Create Filter for DeltaTime
QueryFilter deltaTimeFilter = new QueryFilter();
deltaTimeFilter.withDeltaTime(
                new DeltaTime()
```

```
                .withOffsetSeconds(-1 * EstimatedDataDelayInSeconds)
                .withTimeExpression("from_unixtime(timestamp)"));

//Create Action
action.setActionName("SQLActionWithDeltaTime");
action.setQueryAction(new SqlQueryDatasetAction()
                .withSqlQuery("SELECT * from DataStoreName")
                .withFilters(deltaTimeFilter));

// Add Action to Actions List
List<DatasetAction> actions = new ArrayList<DatasetAction>();
actions.add(action);

//Create Trigger
DatasetTrigger trigger = new DatasetTrigger();
trigger.setSchedule(new Schedule().withExpression("cron(0 12 * * ? *)"));

//Add Trigger to Triggers List
List<DatasetTrigger> triggers = new ArrayList<DatasetTrigger>();
triggers.add(trigger);

// Add Triggers and Actions to CreateDatasetRequest object
request.setActions(actions);
request.setTriggers(triggers);

// Add RetentionPeriod to CreateDatasetRequest object
request.setRetentionPeriod(new RetentionPeriod().withNumberOfDays(10));
final CreateDatasetResult result = iot.createDataset(request);
```

Ausgabe bei Erfolg:

```
{DatasetName: <datatsetName>, DatasetArn: <datatsetARN>, RetentionPeriod: {unlimited:
 true} or {numberOfDays: 10, unlimited: false}}
```

Beispiel 3 — Erstellen einer Container-Datenmenge mit einem eigenen Zeitplan-Trigger (Java)

```
CreateDatasetRequest request = new CreateDatasetRequest();
request.setDatasetName(dataSetName);
DatasetAction action = new DatasetAction();

//Create Action
```

```
action.setActionName("ContainerActionDataset");
action.setContainerAction(new ContainerDatasetAction()
        .withImage(ImageURI)
        .withExecutionRoleArn(ExecutionRoleArn)
        .withResourceConfiguration(
                new ResourceConfiguration()
                .withComputeType(new ComputeType().withAcu(1))
                .withVolumeSizeInGB(1))
        .withVariables(new Variable()
        .withName("VariableName")
        .withStringValue("VariableValue"));

// Add Action to Actions List
List<DatasetAction> actions = new ArrayList<DatasetAction>();
actions.add(action);

//Create Trigger
DatasetTrigger trigger = new DatasetTrigger();
trigger.setSchedule(new Schedule().withExpression("cron(0 12 * * ? *)"));

//Add Trigger to Triggers List
List<DatasetTrigger> triggers = new ArrayList<DatasetTrigger>();
triggers.add(trigger);

// Add Triggers and Actions to CreateDatasetRequest object
request.setActions(actions);
request.setTriggers(triggers);

// Add RetentionPeriod to CreateDatasetRequest object
request.setRetentionPeriod(new RetentionPeriod().withNumberOfDays(10));
final CreateDatasetResult result = iot.createDataset(request);
```

Ausgabe bei Erfolg:

```
{DatasetName: <datatsetName>, DatasetArn: <datatsetARN>, RetentionPeriod: {unlimited:
 true} or {numberOfDays: 10, unlimited: false}}
```

Beispiel 4 — Erstellen einer Container-Datenmenge mit einer SQL-Datenmenge als Trigger (Java)

```
CreateDatasetRequest request = new CreateDatasetRequest();
request.setDatasetName(dataSetName);
```

```
DatasetAction action = new DatasetAction();

//Create Action
action.setActionName("ContainerActionDataset");
action.setContainerAction(new ContainerDatasetAction()
        .withImage(ImageURI)
        .withExecutionRoleArn(ExecutionRoleArn)
        .withResourceConfiguration(
                new ResourceConfiguration()
                .withComputeType(new ComputeType().withAcu(1))
                .withVolumeSizeInGB(1))
        .withVariables(new Variable()
        .withName("VariableName")
        .withStringValue("VariableValue"));

// Add Action to Actions List
List<DatasetAction> actions = new ArrayList<DatasetAction>();
actions.add(action);

//Create Trigger
DatasetTrigger trigger = new DatasetTrigger()
        .withDataset(new TriggeringDataset()
                .withName(TriggeringSQLDataSetName));

//Add Trigger to Triggers List
List<DatasetTrigger> triggers = new ArrayList<DatasetTrigger>();
triggers.add(trigger);

// Add Triggers and Actions to CreateDatasetRequest object
request.setActions(actions);
request.setTriggers(triggers);
final CreateDatasetResult result = iot.createDataset(request);
```

Ausgabe bei Erfolg:

```
{DatasetName: <datatsetName>, DatasetArn: <datatsetARN>}
```

Beispiel 5 — Erstellen einer SQL-Datenmenge (CLI)

```
aws iotanalytics --endpoint <EndPoint>  --region <Region> create-dataset --dataset-
name="<dataSetName>" --actions="[{\"actionName\":\"<ActionName>\", \"queryAction\":
{\"sqlQuery\":\"<SQLQuery>\"}}]" --retentionPeriod numberOfDays=10
```

Ausgabe bei Erfolg:

```
{
    "datasetName": "<datasetName>",
    "datasetArn": "<datatsetARN>",
    "retentionPeriod": {unlimited: true} or {numberOfDays: 10, unlimited: false}
}
```

Beispiel 6 — Erstellen einer SQL-Datenmenge mit einem Delta-Fenster (CLI)

Delta-Fenster sind eine Reihe von benutzerdefinierten, sich nicht überlappenden und kontinuierlichen Zeitintervallen. In Delta-Fenstern können Sie Dataset-Inhalte mit neuen Daten erstellen und Analysen durchführen, die seit der letzten Analyse im Datenspeicher eingetroffen sind. Sie erstellen ein Delta-Fenster, indem Sie`deltaTime`in der`filters`Teil einer`queryAction`eines Datensatzes (CreateDataset) enthalten. Normalerweise möchten Sie den Dataset-Inhalt automatisch erstellen, indem Sie auch einen Zeitintervall-Trigger einrichten (`triggers:schedule:expression`) enthalten. Grundsätzlich können Sie auf diese Weise Nachrichten filtern, die während eines bestimmten Zeitfensters eingetroffen sind, sodass die in Nachrichten aus früheren Zeitfenstern enthaltenen Daten nicht doppelt gezählt werden.

In diesem Beispiel erstellen wir einen neuen Datensatz, der automatisch alle 15 Minuten einen neuen Datensatzinhalt erstellt, wobei nur die Daten verwendet werden, die seit dem letzten Mal eingetroffen sind. Wir legen eine Verzögerung von 3 Minuten (180 Sekunden) `deltaTime` fest. So können Daten mit 3 Minuten Verzögerung im angegebenen Datenspeicher eingehen. Wenn also der Datensatz-Inhalt um 10:30 Uhr erstellt wird, werden die verwendeten Daten (im Datensatz-Inhalt enthalten) mit Zeitstempeln zwischen 10:12 Uhr und 10:27 Uhr (dh 10:30 Uhr - 15 Minuten - 3 Minuten bis 10:30 Uhr - 3 Minuten) verwendet.

```
aws iotanalytics --endpoint <EndPoint>  --region <Region> create-dataset --cli-input-
json file://delta-window.json
```

Wo ist die Akte`delta-window.json`enthält Folgendes.

```
{
  "datasetName": "delta_window_example",
  "actions": [
    {
      "actionName": "delta_window_action",
```

```
      "queryAction": {
        "sqlQuery": "SELECT temperature, humidity, timestamp FROM my_datastore",
        "filters": [
          {
            "deltaTime": {
              "offsetSeconds": -180,
              "timeExpression": "from_unixtime(timestamp)"
            }
          }
        ]
      }
    }
  ],
  "triggers": [
    {
      "schedule": {
        "expression": "cron(0/15 * * * ? *)"
      }
    }
  ]
}
```

Ausgabe bei Erfolg:

```
{
    "datasetName": "<datasetName>",
    "datasetArn": "<datatsetARN>",
}
```

Containerizing eines Notebook

Dieser Abschnitt enthält Informationen zur Erstellung eines Docker-Containers mithilfe eines Jupyter-Notebooks. Es stellt ein Sicherheitsrisiko dar, wenn Sie Notebooks von Drittanbietern wiederverwenden: Die enthaltenen Container können beliebigen Code mit Ihren Benutzerberechtigungen ausführen. Zusätzlich kann das vom Notizbuch generierte HTML in derAWS IoT AnalyticsKonsole, die einen potenziellen Angriffsvektor auf den Computer bereitstellt, der den HTML-Code anzeigt. Stellen Sie sicher, dass Sie dem Autor von Drittanbieter-Notebooks vertrauen, bevor Sie diese verwenden.

Eine Möglichkeit zum Ausführen von erweiterten Analysefunktionen besteht in der Verwendung eines Jupyter-Notebooks. Jupyter Notebook bietet leistungsstarke Data-Science-Tools, die maschinelles

Lernen und eine Reihe statistischer Analysen durchführen können. Weitere Informationen finden Sie unterNotebook-Vorlagen. (Beachten Sie, dass wir derzeit keine Containerisierung im Inneren unterstützen JupyterLab.) Sie können Ihr Jupyter-Notebook und Ihre Bibliotheken in einen Container packen, der regelmäßig mit einem neuen Datenstapel ausgeführt wird, sobald er von empfangen wirdAWS IoT Analyticswährend eines Delta-Zeitfensters, das Sie definieren. Sie können einen Analyseauftrag planen, der den Container und die neuen, segmentierten Daten verwendet, die innerhalb des angegebenen Zeitfensters erfasst wurden, und dann die Ausgabe des Auftrags für future geplante Analysen speichern.

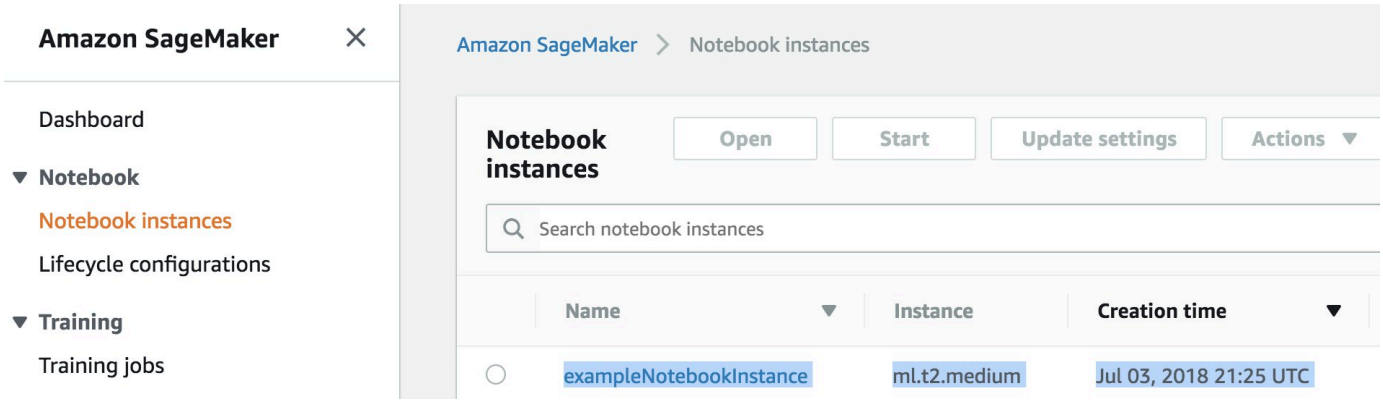
Wenn Sie eine erstellt haben SageMaker Instanz unter Verwendung desAWS IoT AnalyticsKonsole nach dem 23. August 2018, dann wurde die Installation der Containerisierungserweiterung automatisch für Sie durchgeführtund Sie können beginnen, ein containerisiertes Image zu erstellen. Befolgen Sie andernfalls die Anleitung in diesem Abschnitt, um die Notebook-Containerisierung auf Ihrem zu aktivieren. SageMaker Instanz. Im Folgenden modifizieren Sie Ihre SageMaker Ausführungsrolle, mit der Sie das Container-Image in Amazon EC2 hochladen und die Containerisierungserweiterung installieren können.

Aktivieren der Containerisierung von Notebook-Instanzen, die nicht überAWS IoT AnalyticsKonsole

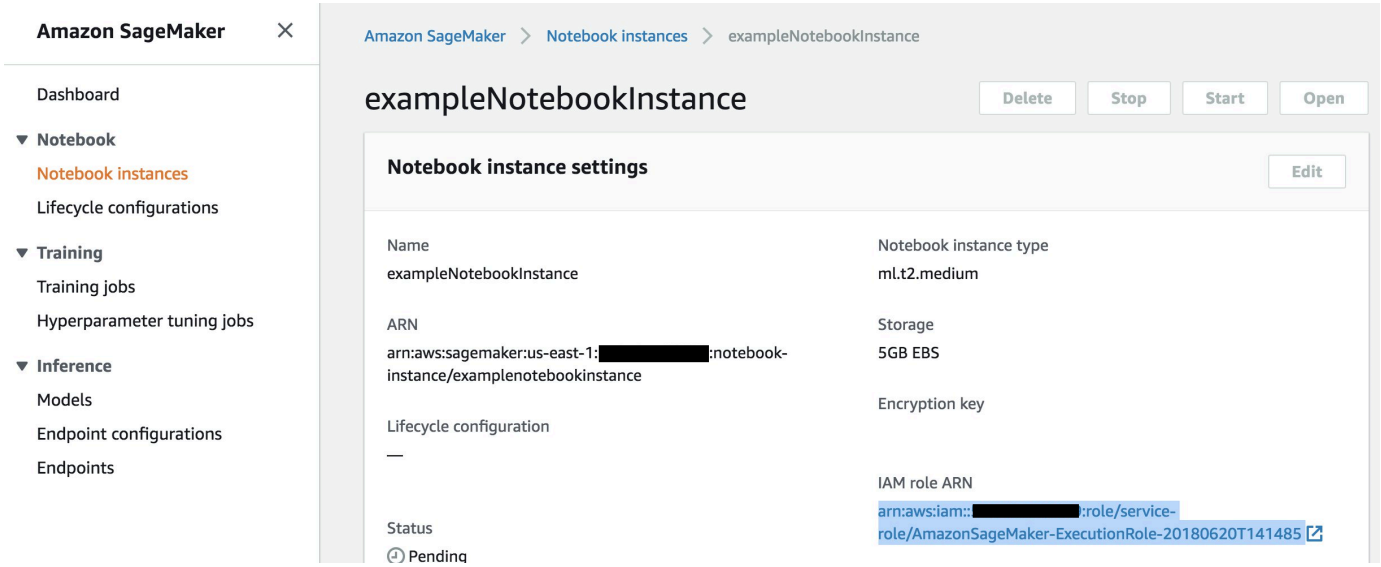
Wir empfehlen Ihnen, ein neues SageMaker -Instanz über dieAWS IoT AnalyticsKonsole, anstatt diese Schritte zu befolgen. Neue Instances unterstützen automatisch die Containerisierung.

Wenn du neu startest SageMaker Nach dem Aktivieren der Containerisierung, wie hier gezeigt, müssen Sie die IAM-Rollen und -Richtlinien nicht erneut hinzufügen, sondern müssen die Erweiterung erneut installieren, wie im letzten Schritt gezeigt.

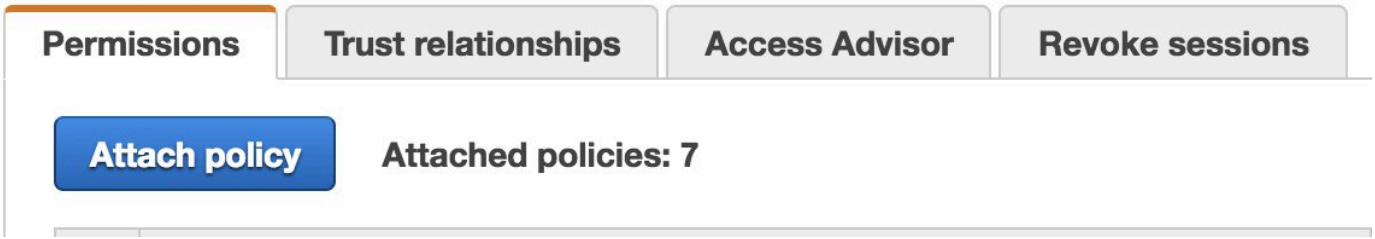
1. Um Ihrer Notebook-Instance Zugriff auf Amazon ECS zu gewähren, wählen Sie SageMaker Instanz auf der SageMaker Seite::



2. UnterIAM-Rolle ARN, wähle das SageMaker Ausführungsrolle.

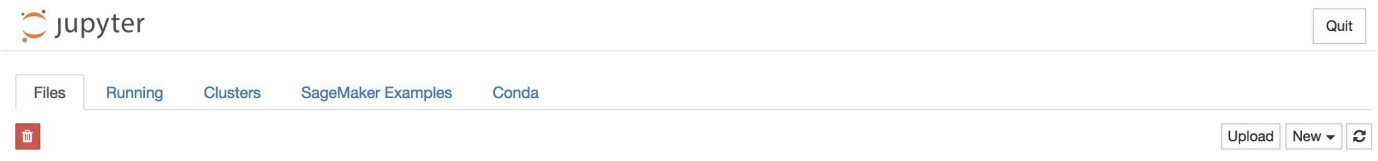


3. Wählen Sie Attach Policy (Richtlinie anfügen) aus. Definieren Sie anschließend die Richtlinie, die unterPermissions (Berechtigungen) angezeigt wird, und fügen Sie sie hinzu. Wenn das Symbol`AmazonSageMakerFullAccess`Richtlinie ist noch nicht angehängt, hängen Sie sie ebenfalls an.



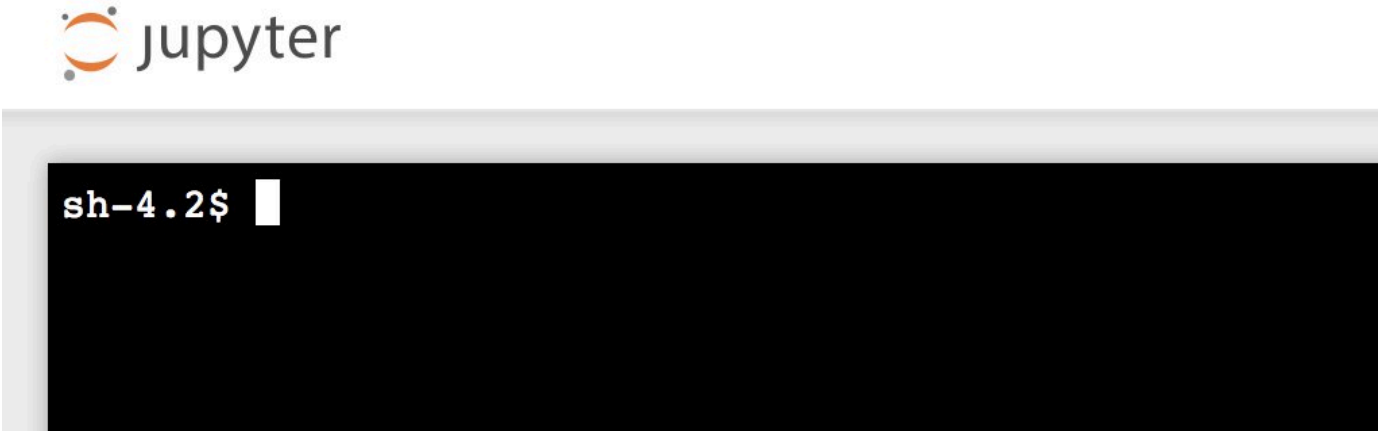
Sie müssen auch den Containerisierungscode von Amazon S3 herunterladen und auf Ihrer Notebook-Instance installieren. Der erste Schritt besteht darin, auf die SageMaker das Terminal der Instanz.

1. Wählen Sie in Jupyterneu.



2. Wählen Sie im Menü, das erscheint,Terminal.

3. Geben Sie im Terminal die folgenden Befehle ein, um den Code herunterzuladen, zu entpacken und zu installieren. Beachten Sie, dass diese Befehle alle Prozesse beenden, die von Ihren Notebooks darauf ausgeführt werden SageMaker Instanz.




```
cd /tmp

aws s3 cp s3://iotanalytics-notebook-containers/iota_notebook_containers.zip /tmp

unzip iota_notebook_containers.zip

cd iota_notebook_containers

chmod u+x install.sh

./install.sh
```

Warten Sie ein paar Minuten, bis die Erweiterung validiert und installiert wurde.

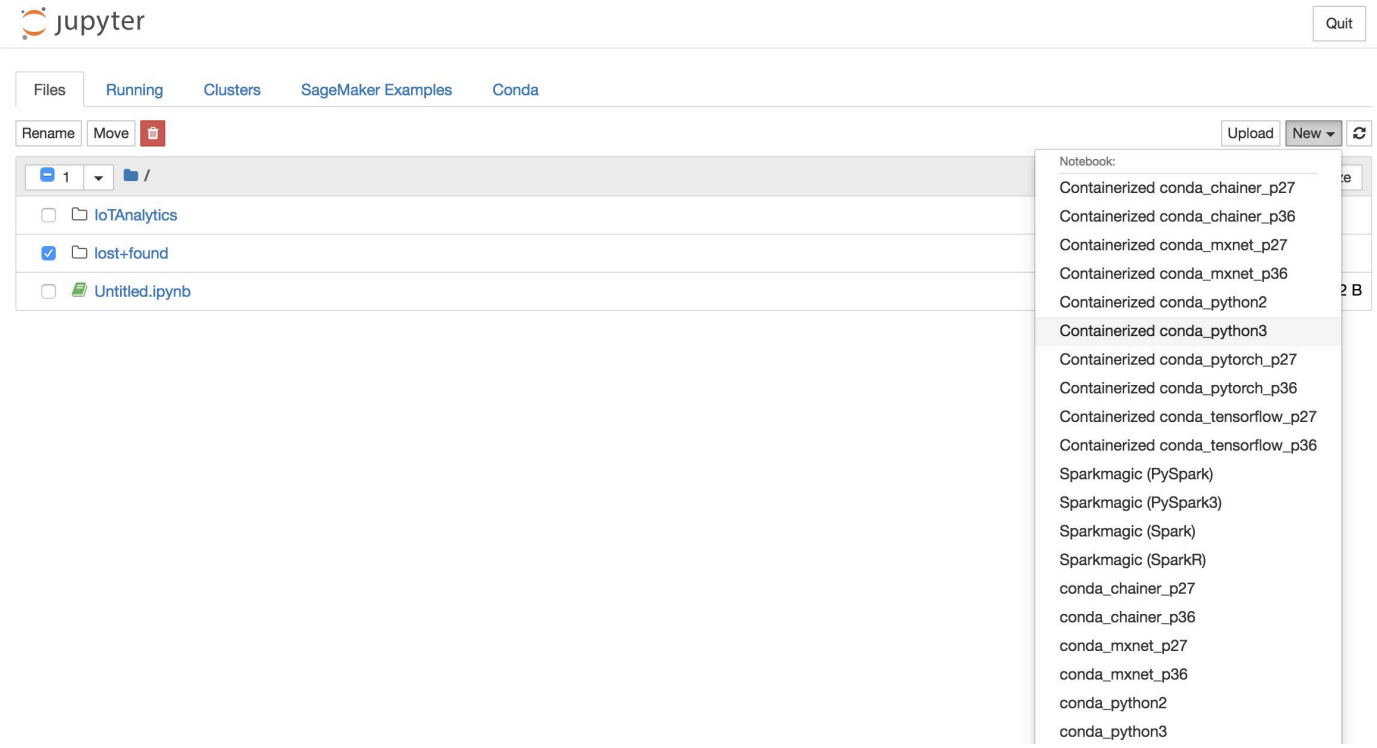
Aktualisieren Sie die Containerisierung Ihres Notebooks

Wenn du deine erstellt hast SageMaker Instance via derAWS IoT AnalyticsKonsole nach dem 23. August 2018, dann wurde die Containerisierungserweiterung automatisch installiert. Sie können die Erweiterung aktualisieren, indem Sie Ihre Instance neu starten SageMaker -Konsole. Wenn Sie die Erweiterung manuell installiert haben, können Sie sie aktualisieren, indem Sie die unter Containerisierung von nicht erstellten Notebook-Instanzen aktivieren aufgeführten Terminalbefehle erneut ausführenAWS IoT Analytics-Konsole.

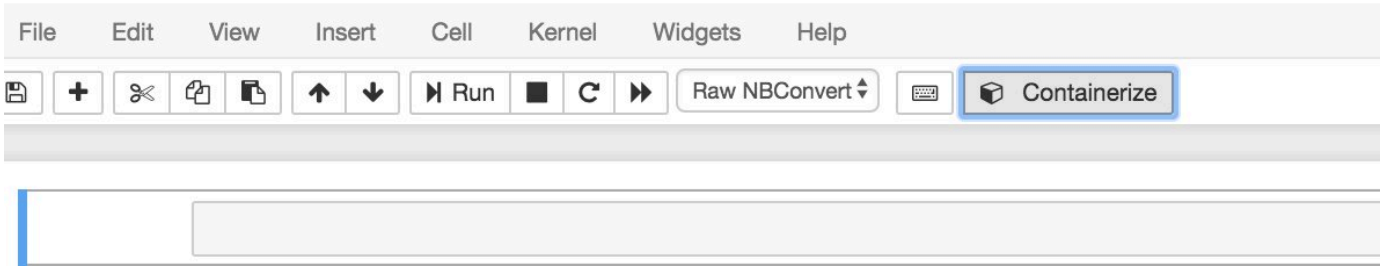
Erstellen eines Container-Image

In diesem Abschnitt zeigen wir die notwendigen Schritte zur Containerisierung eines Notebooks. Um zu beginnen, rufen Sie Ihr Jupyter-Notebook auf, um ein Notebook mit einem containerisierten Kernel zu erstellen.

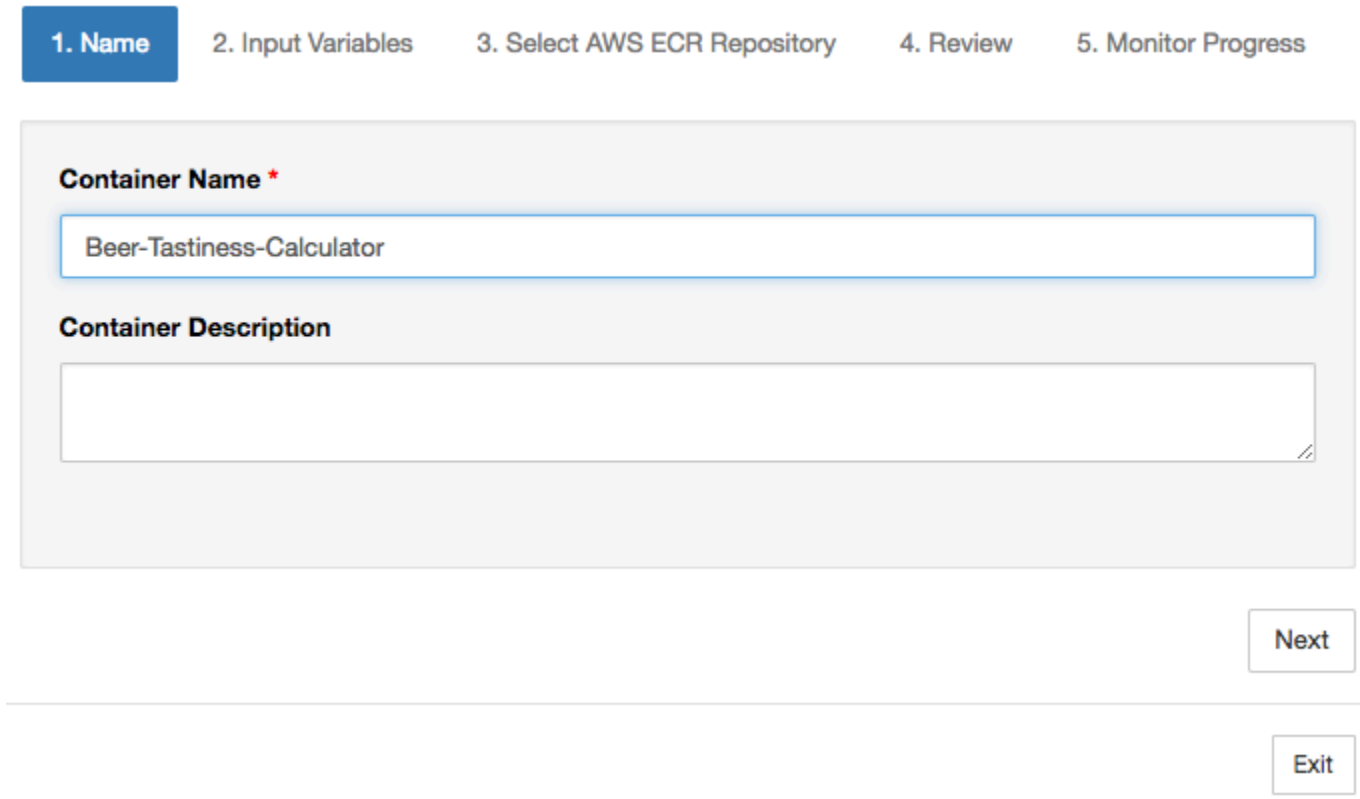
1. In Ihrem Jupyter-Notebook wählen Sie New (Neu) aus und anschließend aus der Dropdown-Liste den gewünschten Kernel-Typ aus. (Der Kerneltyp sollte mit „Containerized“ beginnen und mit dem Kernel enden, den Sie sonst ausgewählt hätten. Wenn Sie beispielsweise nur eine einfache Python 3.0-Umgebung wie „conda_python3" wollen, wählen Sie „Containerized conda_python3").



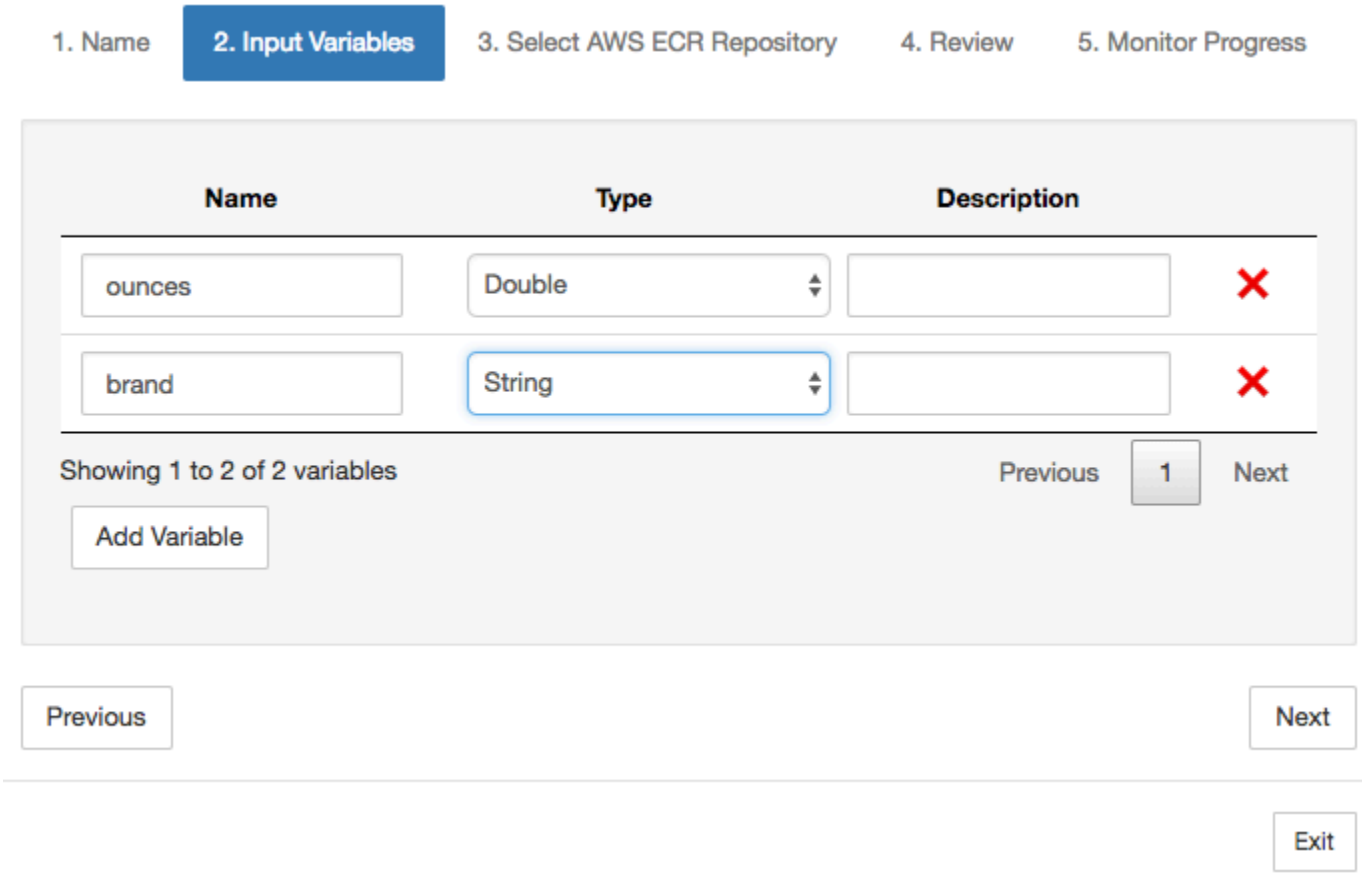
2. Nachdem Sie die Arbeit an Ihrem Notebook abgeschlossen haben und es containerisieren möchten, wählen SieContainerisierung.



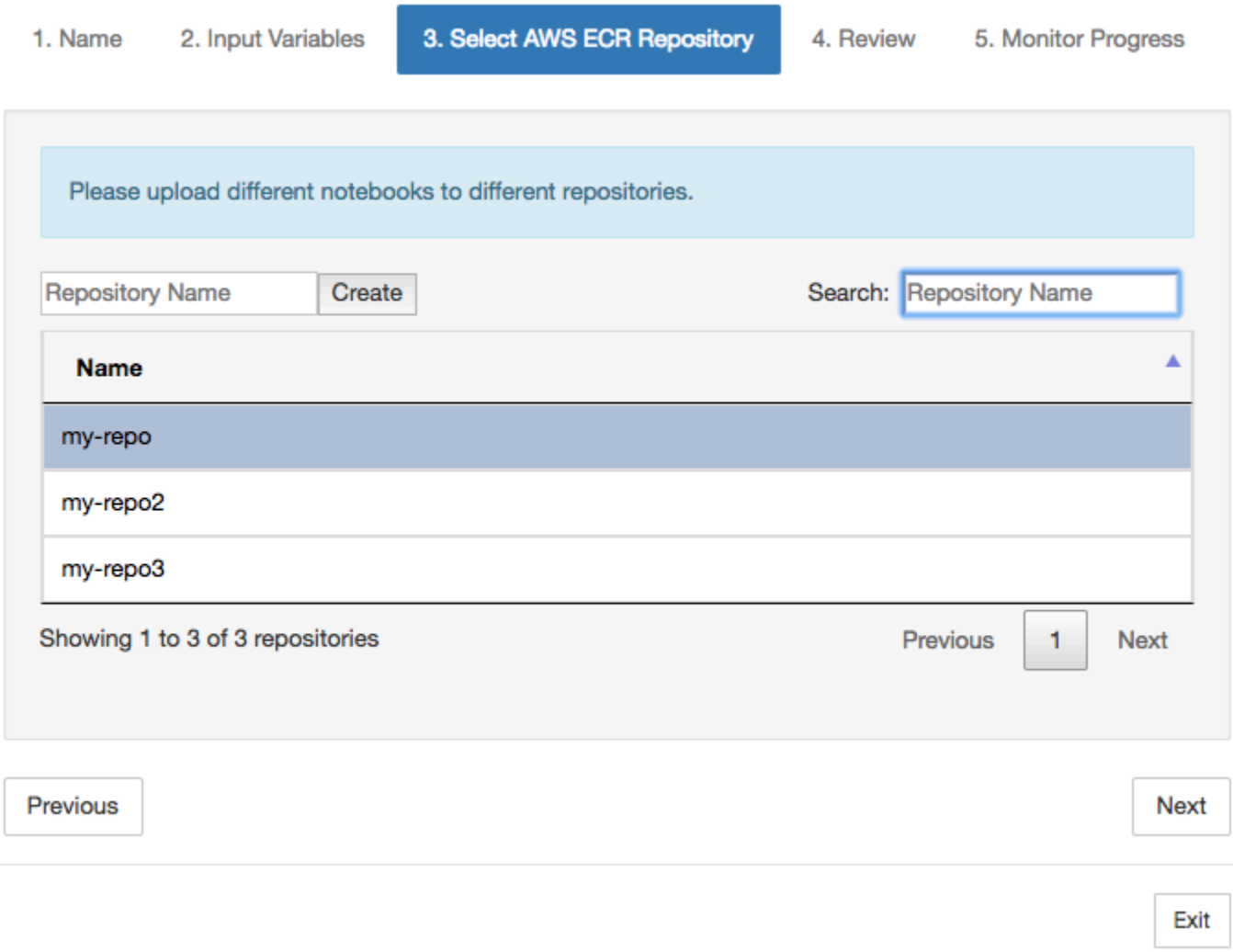
3. Geben Sie einen Namen für das containerisierte Notebook ein. Sie können auch eine optionale Beschreibung eingeben.



4. Geben Sie die Input Variables (Eingabevariablen) (Parameter) ein, mit denen Ihr Notebook aufgerufen werden soll. Sie können die Eingabevariablen auswählen, die automatisch von Ihrem Notebook erkannt wurden, oder benutzerdefinierte Variablen festlegen. (Beachten Sie, dass Eingabevariablen nur erkannt werden, wenn Sie Ihr Notebook zuvor ausgeführt haben.) Für jede Eingabevariable wählen Sie einen Typ aus. Sie können auch eine optionale Beschreibung der Eingabevariablen eingeben.

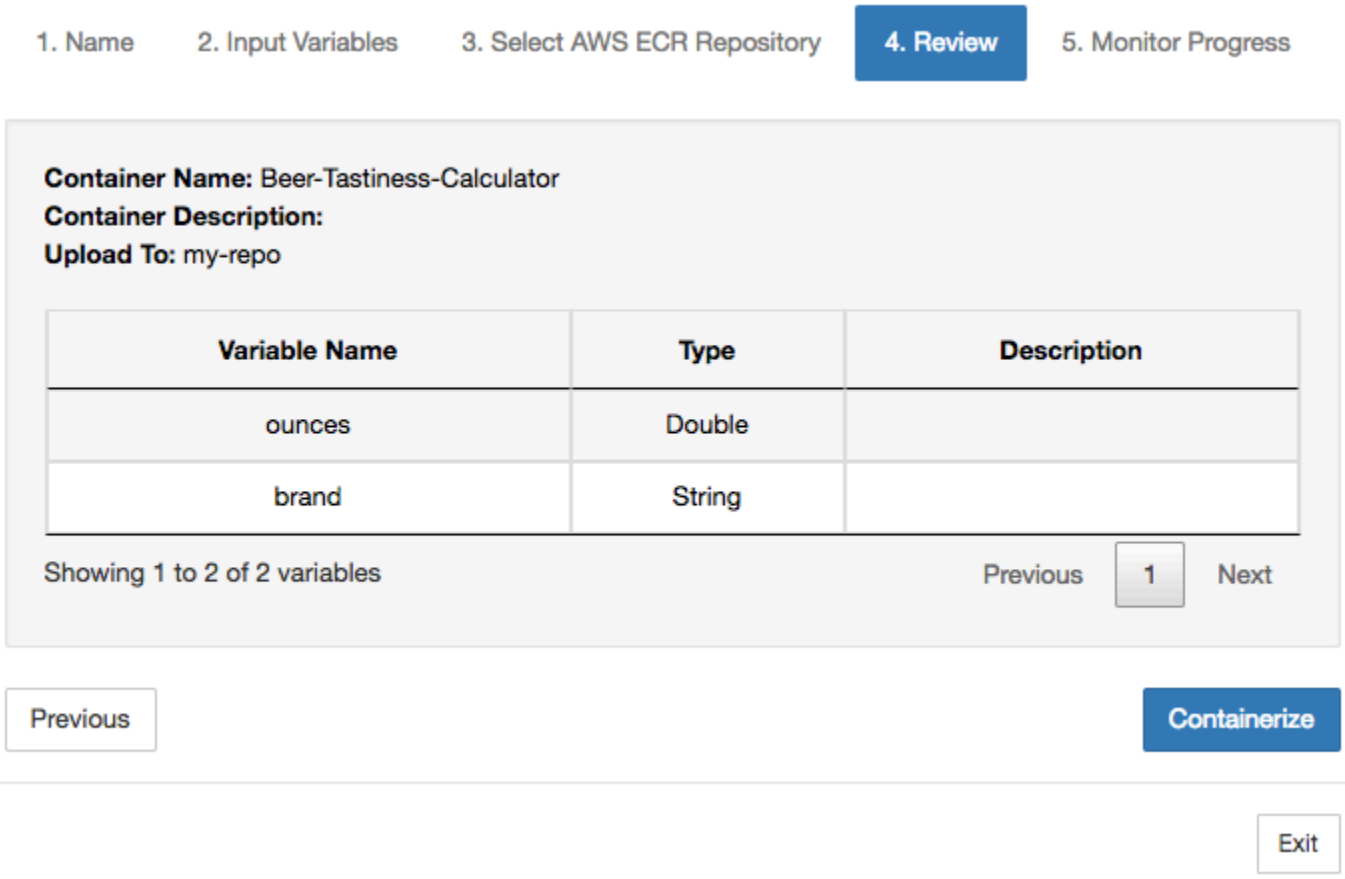


5. Wählen Sie das Amazon ECR-Repository, in das das aus dem Notizbuch erstellte Bild hochgeladen werden soll.

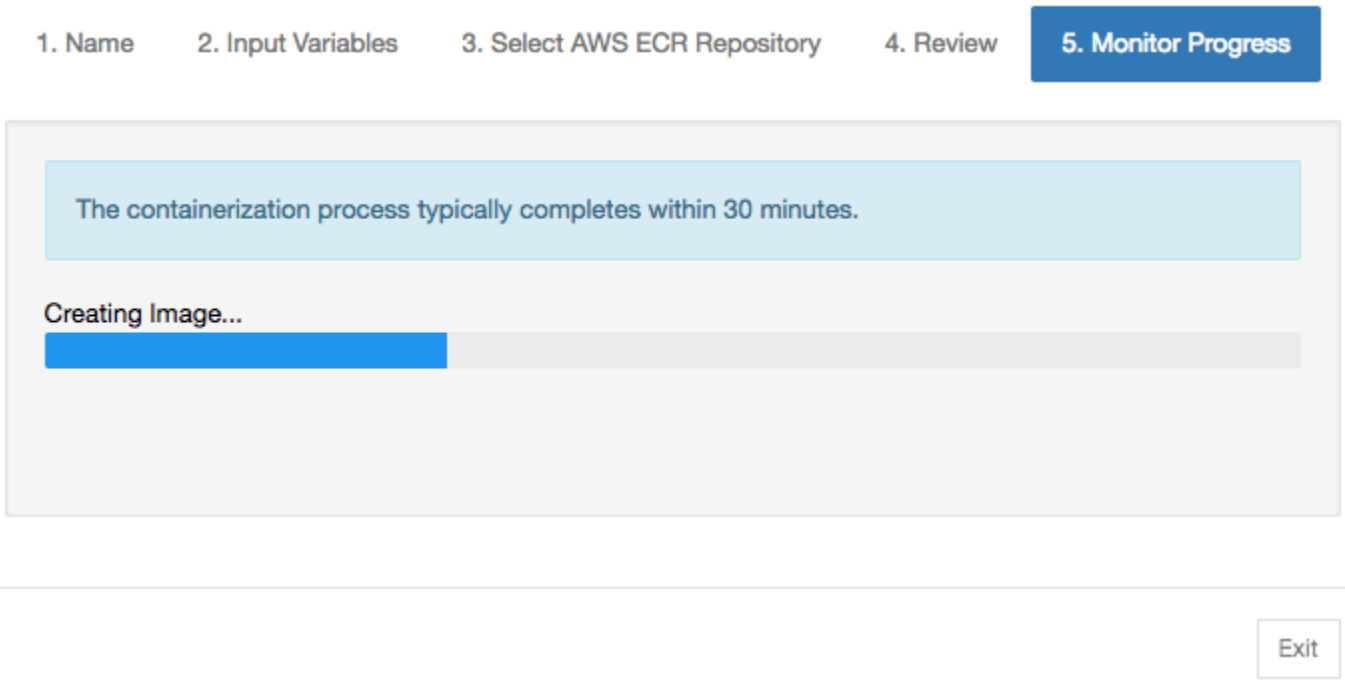


6. WählenContainerisierungum den Prozess zu starten.

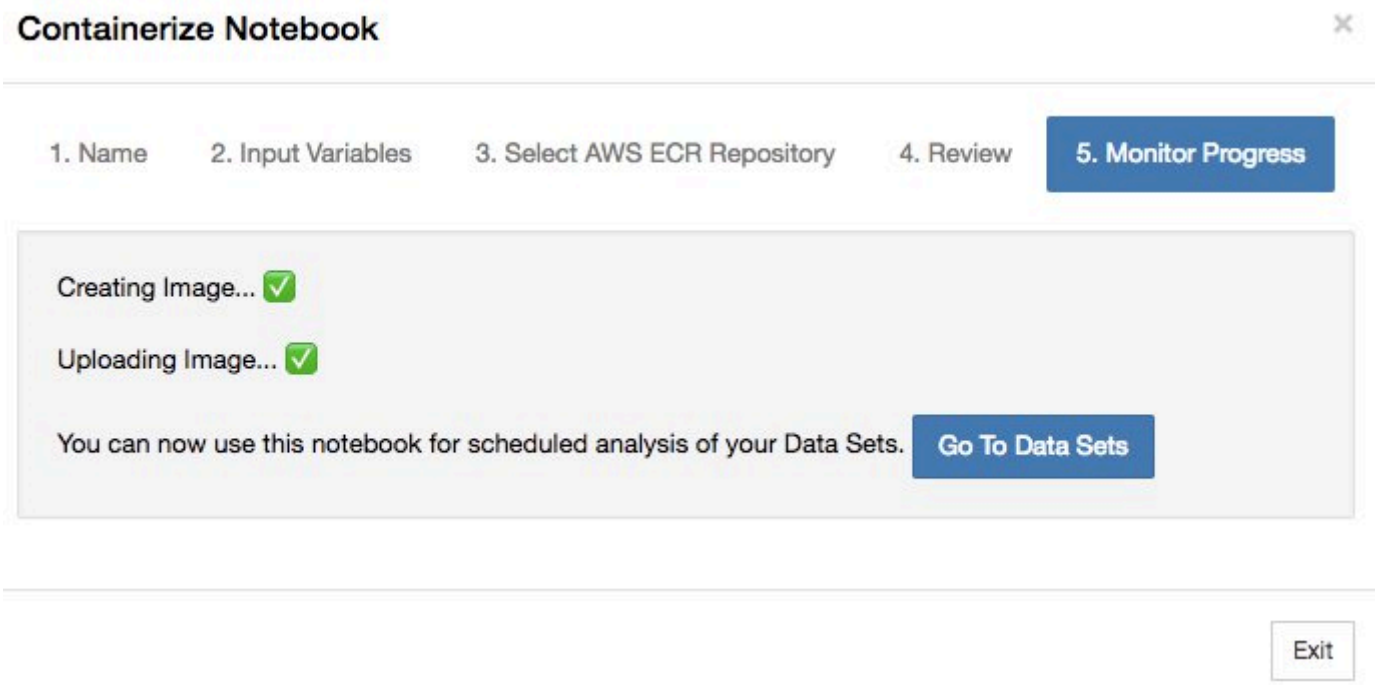
   Sie erhalten eine Übersicht, die Ihre Beiträge zusammenfasst. Beachten Sie, dass Sie den Vorgang nicht mehr stornieren können. Der Vorgang kann bis zu einer Stunde dauern.



7. Die nächste Seite zeigt den Fortschritt.



8. Wenn Sie Ihren Browser versehentlich schließen, können Sie den Status des Containerisierungsprozesses imNotebooksAbschnitt derAWS IoT Analytics-Konsole.
9. Nach Abschluss des Vorgangs wird das containerisierte Image auf Amazon ECR gespeichert und kann verwendet werden.



Verwenden eines benutzerdefinierten Containers für die Analyse

Dieser Abschnitt enthält Informationen zur Erstellung eines Docker-Containers mithilfe eines Jupyter-Notebooks. Es stellt ein Sicherheitsrisiko dar, wenn Sie Notebooks von Drittanbietern wiederverwenden: Die enthaltenen Container können beliebigen Code mit Ihren Benutzerberechtigungen ausführen. Zusätzlich kann das vom Notizbuch generierte HTML in derAWS IoT AnalyticsKonsole, die einen potenziellen Angriffsvektor auf den Computer bereitstellt, der den HTML-Code anzeigt. Stellen Sie sicher, dass Sie dem Autor von Drittanbieter-Notebooks vertrauen, bevor Sie diese verwenden.

Sie können Ihren eigenen benutzerdefinierten Container erstellen und mit demAWS IoT AnalyticsService. Dazu richten Sie ein Docker-Image ein und laden es in Amazon ECR hoch. Anschließend richten Sie einen Datensatz ein, um eine Container-Aktion auszuführen. In diesem Abschnitt finden Sie ein Beispiel für das Verfahren unter Verwendung von Octave.

In diesem Tutorial wird davon ausgegangen, dass Sie:

- Octave auf Ihrem lokalen Computer installiert haben
- Ein Docker-Konto, das auf Ihrem lokalen Computer eingerichtet ist
- Importieren in &S3;AWS-Konto bei Amazon ECR oderAWS IoT AnalyticsZugriff

Schritt 1: Richten eines Docker-Image

Es gibt drei zentrale Dateien, die Sie für dieses Tutorial benötigen. Die Namen und Inhalte finden Sie hier:

- `Dockerfile`— Die anfängliche Einrichtung für den Containerisierungsprozess von Docker.

```
FROM ubuntu:16.04

# Get required set of software
RUN apt-get update
RUN apt-get install -y software-properties-common
RUN apt-get install -y octave
RUN apt-get install -y python3-pip

# Get boto3 for S3 and other libraries
RUN pip3 install --upgrade pip
RUN pip3 install boto3
RUN pip3 install urllib3

# Move scripts over
ADD moment moment
ADD run-octave.py run-octave.py

# Start python script
ENTRYPOINT ["python3", "run-octave.py"]
```

- `run-octave.py`— Parst JSON vonAWS IoT Analytics, führt das Octave-Skript aus und lädt Artefakte auf Amazon S3 hoch.

```
import boto3
import json
import os
import sys
from urllib.parse import urlparse

# Parse the JSON from IoT Analytics
```

```
with open('/opt/ml/input/data/iotanalytics/params') as params_file:
    params = json.load(params_file)

variables = params['Variables']

order = variables['order']
input_s3_bucket = variables['inputDataS3BucketName']
input_s3_key = variables['inputDataS3Key']
output_s3_uri = variables['octaveResultS3URI']

local_input_filename = "input.txt"
local_output_filename = "output.mat"

# Pull input data from S3...
s3 = boto3.resource('s3')
s3.Bucket(input_s3_bucket).download_file(input_s3_key, local_input_filename)

# Run Octave Script
os.system("octave moment {} {} {}".format(local_input_filename,
 local_output_filename, order))

# # Upload the artifacts to S3
output_s3_url = urlparse(output_s3_uri)
output_s3_bucket = output_s3_url.netloc
output_s3_key = output_s3_url.path[1:]

s3.Object(output_s3_bucket, output_s3_key).put(Body=open(local_output_filename,
 'rb'), ACL='bucket-owner-full-control')
```

- `moment`— Ein einfaches Octave-Skript, das den Moment basierend auf einer Eingabe- oder Ausgabedatei und einer bestimmten Reihenfolge berechnet.

```
#!/usr/bin/octave -qf

arg_list = argv ();
input_filename = arg_list{1};
output_filename = arg_list{2};
order = str2num(arg_list{3});

[D,delimiterOut]=importdata(input_filename)
M = moment(D, order)

save(output_filename,'M')
```

1. Laden Sie die Inhalte der einzelnen Dateien herunter. Erstellen Sie ein neues Verzeichnis und platzieren Sie alle Dateien darin und danncdin dieses Verzeichnis.
2. Führen Sie den folgenden Befehl aus.

```
docker build -t octave-moment .
```

3. Sie sollten ein neues Image in Ihrem Docker-Repository sehen. Überprüfen Sie dies, indem Sie den folgenden Befehl ausführen.

```
docker image ls | grep octave-moment
```

Schritt 2: Laden Sie das Docker-Image in ein Amazon ECR-Repository hoch

1. Erstellen Sie ein Repository in Amazon ECR.

```
aws ecr create-repository --repository-name octave-moment
```

2. Holen Sie sich das Login in Ihre Docker-Umgebung.

```
aws ecr get-login
```

3. Kopieren Sie die Ausgabe und führen Sie diesen Befehl aus. Die Ausgabe sollte wie folgt aussehen.

```
docker login -u AWS -p password -e none https://your-aws-account-
id.dkr.ecr..amazonaws.com
```

4. Kennzeichnen Sie das von Ihnen erstellte Bild mit dem Amazon ECR-Repository-Tag.

```
docker tag your-image-id  your-aws-account-id.dkr.ecr.region.amazonaws.com/octave-
moment
```

5. Verschieben Sie das Image zu Amazon ECR.

```
docker push your-aws-account-id.dkr.ecr.region.amazonaws.com/octave-moment
```

Schritt 3: Laden Sie Ihre Beispieldaten in einen Amazon S3 S3-Bucket hoch

1. Laden Sie Folgendes in eine Datei herunter`input.txt`.

```
0.857549  -0.987565  -0.467288  -0.252233  -2.298007
 0.030077  -1.243324  -0.692745   0.563276   0.772901
-0.508862  -0.404303  -1.363477  -1.812281  -0.296744
-0.203897   0.746533   0.048276   0.075284   0.125395
 0.829358   1.246402  -1.310275  -2.737117   0.024629
 1.206120   0.895101   1.075549   1.897416   1.383577
```

2. Erstellen eines Amazon-S3-Buckets mit dem`octave-sample-data-`*`your-aws-account-id`*.
3. Hochladen der Datei`input.txt`im Amazon S3 Bucket, den Sie gerade erstellt haben. Sie sollten nun ein Bucket mit dem Name`octave-sample-data-`*`your-aws-account-id`*das enthält das`input.txt`file.

Schritt 4: Erstellen einer Containerausführungsrolle

1. Kopieren Sie Folgendes in eine Datei mit dem Name`role1.json`. Ersetzen*`your-aws-account-id`*mit deinemAWS-Konto-ID und*`aws-region`*mit demAWS-Region IhrerAWS-Ressourcen.

> **Note**
>
> Dieses Beispiel enthält einen globalen Bedingungskontextschlüssel zum Schutz vor dem Confused -Deputy-Problem. Weitere Informationen finden Sie unter the section called “Dienstübergreifende Confused-Deputy-Prävention”.

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

```
                "StringEquals": {
                  "aws:SourceAccount": "your-aws-account-id"
                },
                "ArnLike": {
                  "aws:SourceArn": "arn:aws:iotanalytics:aws-region:your-aws-account-
id:dataset/DOC-EXAMPLE-DATASET"
                }
              }
    ]
}
```

2. Erstellen Sie eine Rolle, die Zugriffsberechtigungen für erteilt SageMaker undAWS IoT Analytics, unter Verwendung der Dateirole1.jsondie Sie heruntergeladen haben.

```
aws iam create-role --role-name container-execution-role --assume-role-policy-
document file://role1.json
```

3. Laden Sie Folgendes in eine Datei mit dem Namenpolicy1.jsonund ersetzeyour-account-idmit deiner Konto-ID (siehe den zweiten ARN unterStatement:Resource) enthalten.

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Effect": "Allow",
     "Action": [
       "s3:GetBucketLocation",
       "s3:PutObject",
       "s3:GetObject",
       "s3:PutObjectAcl"
     ],
     "Resource": [
       "arn:aws:s3:::*-dataset-*/*",
       "arn:aws:s3:::octave-sample-data-your-account-id/*"
   },
   {
     "Effect": "Allow",
     "Action": [
       "iotanalytics:*"
     ],
     "Resource": "*"
   },
   {
```

```
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

4. Erstellen Sie eine IAM-Richtlinie mit der`policy.json`Datei, die Sie gerade heruntergeladen haben.

```
aws iam create-policy --policy-name ContainerExecutionPolicy --policy-document
 file://policy1.json
```

5. Fügen Sie der Rolle die -Richtlinie an.

```
aws iam attach-role-policy --role-name container-execution-role --policy-arn
 arn:aws:iam::your-account-id:policy/ContainerExecutionPolicy
```

Schritt 5: Erstellen eines Datensatzes mit einer Container-Aktion

1. Laden Sie Folgendes in eine Datei mit dem Namen`cli-input.json`und ersetze alle Instanzen von*your-account-id*und*region*mit den entsprechenden Werten.

```
{
    "datasetName": "octave_dataset",
    "actions": [
        {
            "actionName": "octave",
            "containerAction": {
                "image": "your-account-id.dkr.ecr.region.amazonaws.com/octave-
moment",
                "executionRoleArn": "arn:aws:iam::your-account-id:role/container-
execution-role",
                "resourceConfiguration": {
                    "computeType": "ACU_1",
                    "volumeSizeInGB": 1
                },
                "variables": [
                    {
                        "name": "octaveResultS3URI",
                        "outputFileUriValue": {
                            "fileName": "output.mat"
                        }
                    },
                    {
                        "name": "inputDataS3BucketName",
                        "stringValue": "octave-sample-data-your-account-id"
                    },
                    {
                        "name": "inputDataS3Key",
                        "stringValue": "input.txt"
                    },
                    {
                        "name": "order",
                        "stringValue": "3"
                    }
                ]
            }
        }
    ]
}
```

2. Erstellen eines Datensatzes mit der Dateicli-input.jsondu hast es gerade heruntergeladen und bearbeitet.

```
aws iotanalytics create-dataset –cli-input-json file://cli-input.json
```

Schritt 6: Generierung von Datensatz-Inhalten aufrufen

1. Führen Sie den folgenden Befehl aus.

```
aws iotanalytics create-dataset-content --dataset-name octave-dataset
```

Schritt 7: Abrufen des Datensat

1. Führen Sie den folgenden Befehl aus.

```
aws iotanalytics get-dataset-content --dataset-name octave-dataset --version-id \
$LATEST
```

2. Möglicherweise müssen Sie einige Minuten warten, bis der`DatasetContentState`ist`SUCCEEDED`.

Schritt 8: Drucken Sie die Ausgabe auf Octave

1. Verwenden Sie die Octave-Shell, um die Ausgabe aus dem Container zu drucken, indem Sie den folgenden Befehl ausführen.

```
bash> octave
octave> load output.mat
octave> disp(M)
-0.016393 -0.098061 0.380311 -0.564377 -1.318744
```

VisualisierenAWS IoT AnalyticsDaten

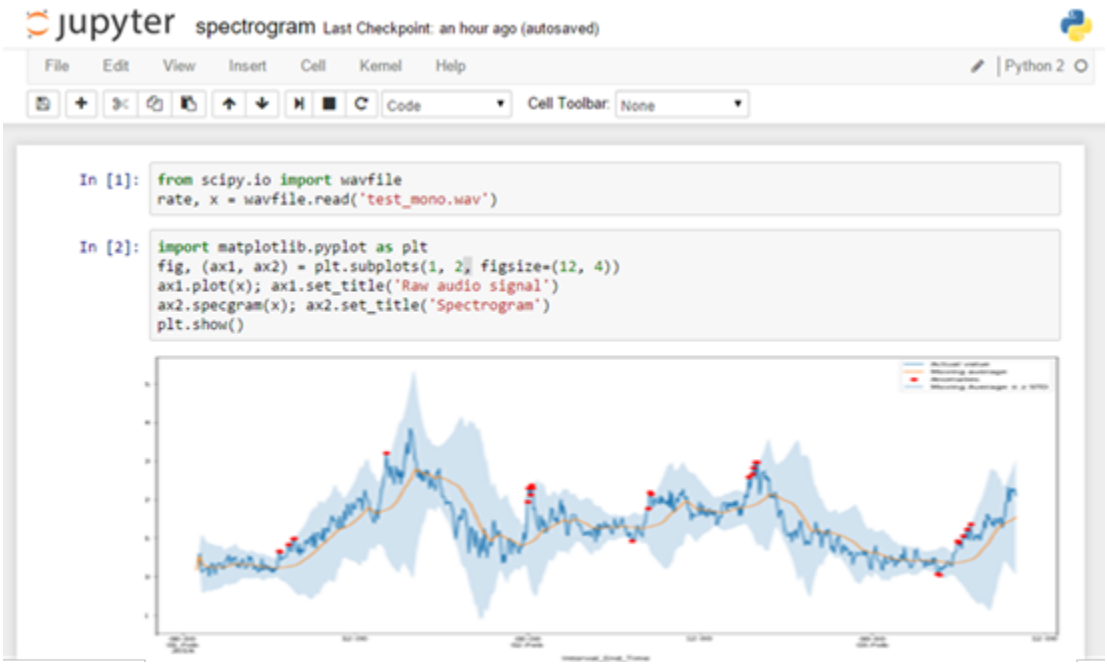
So visualisieren SieAWS IoT Analytics-Daten können Sie denAWS IoT Analytics-Konsole oder Amazon QuickSight.

Themen

- VisualisierenAWS IoT AnalyticsDaten mit der Konsole
- VisualisierenAWS IoT Analytics-Daten mit Amazon QuickSight

VisualisierenAWS IoT AnalyticsDaten mit der Konsole

AWS IoT Analyticskann die HTML-Ausgabe Ihres Container-Datasets einbetten (in der Dateioutput.html) auf der Inhaltsseite des Container-Datasets desAWS IoT AnalyticsKonsoleaus. Wenn Sie beispielsweise ein Container-Dataset definieren, das ein Jupyter-Notebook ausführt, und erstellen eine Visualisierung in Ihrem Jupyter-Notebook, sieht Ihr Dataset möglicherweise wie folgt aus.



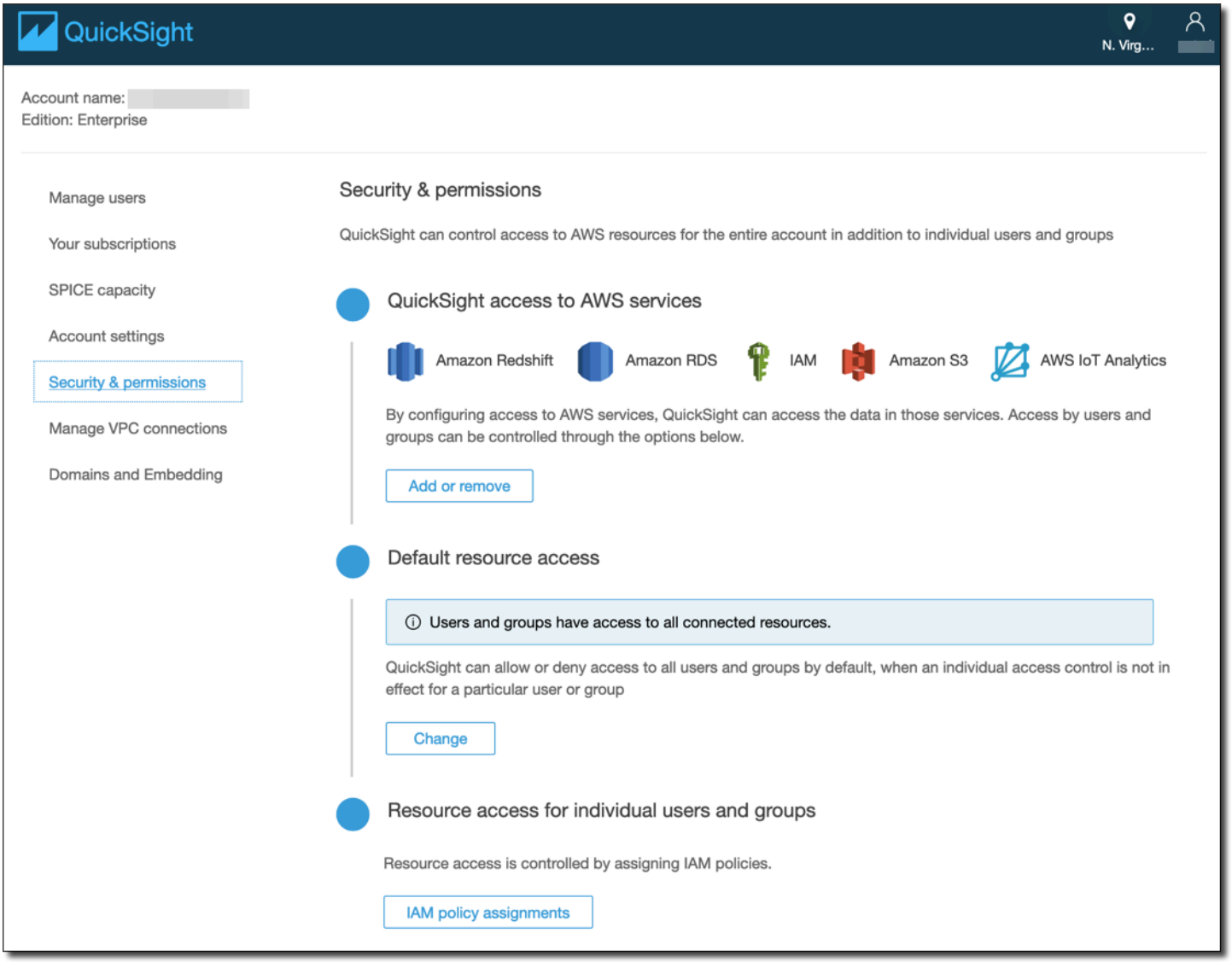
Nachdem der Container Dataset-Inhalt erstellt wurde, können Sie dann diese Visualisierung auf der Konsole anzeigenDatasetinhaltsseite.

Weitere Informationen zum Erstellen eines Container-Datasets, das ein Jupyter-Notebook ausführt, finden Sie unterAutomatisieren von Workflowsaus.

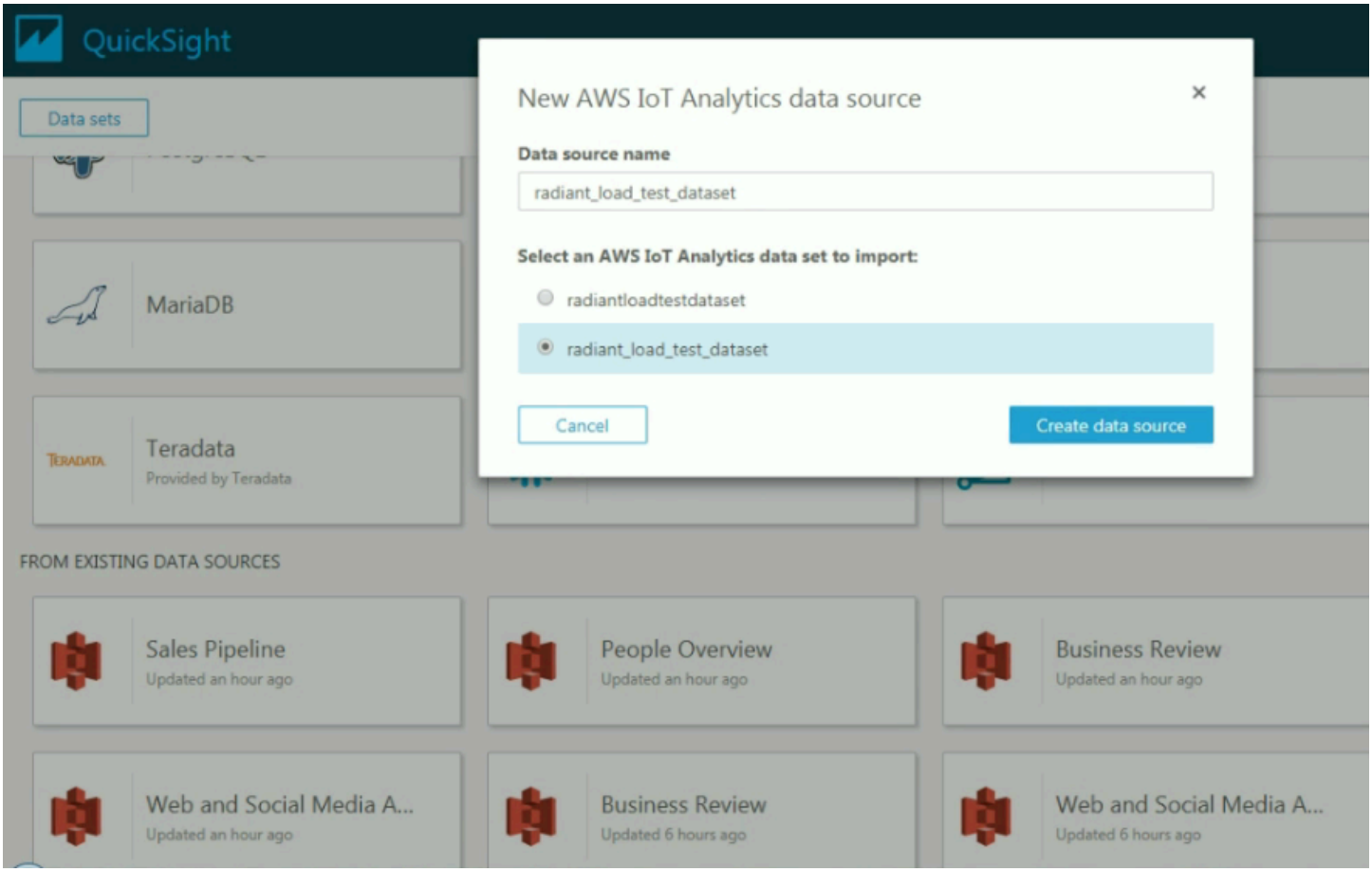
VisualisierenAWS IoT Analytics-Daten mit Amazon QuickSight

AWS IoT Analyticsbietet direkte Integration mitAmazon QuickSightaus. Amazon QuickSight ist ein schneller Geschäftsanalyse-Service, den Sie verwenden können, um Visualisierungen zu erstellen, Ad-hoc-Analysen auszuführen und schnell geschäftliche Erkenntnisse anhand Ihrer Daten zu gewinnen. Amazon QuickSight ermöglicht es Organisationen, auf hunderttausende Benutzer zu skalieren, und bietet dank eines robusten Moduls im Arbeitsspeicher (SPICE) eine schnelle und gezielte Abnahmebearbeitung. Sie können Ihre auswählenAWS IoT AnalyticsDatensätze im Amazon QuickSight konsolen und beginnen Sie mit der Erstellung von Dashboards und Visualisierungen. Amazon QuickSight ist in verfügbar.diese Regionenaus.

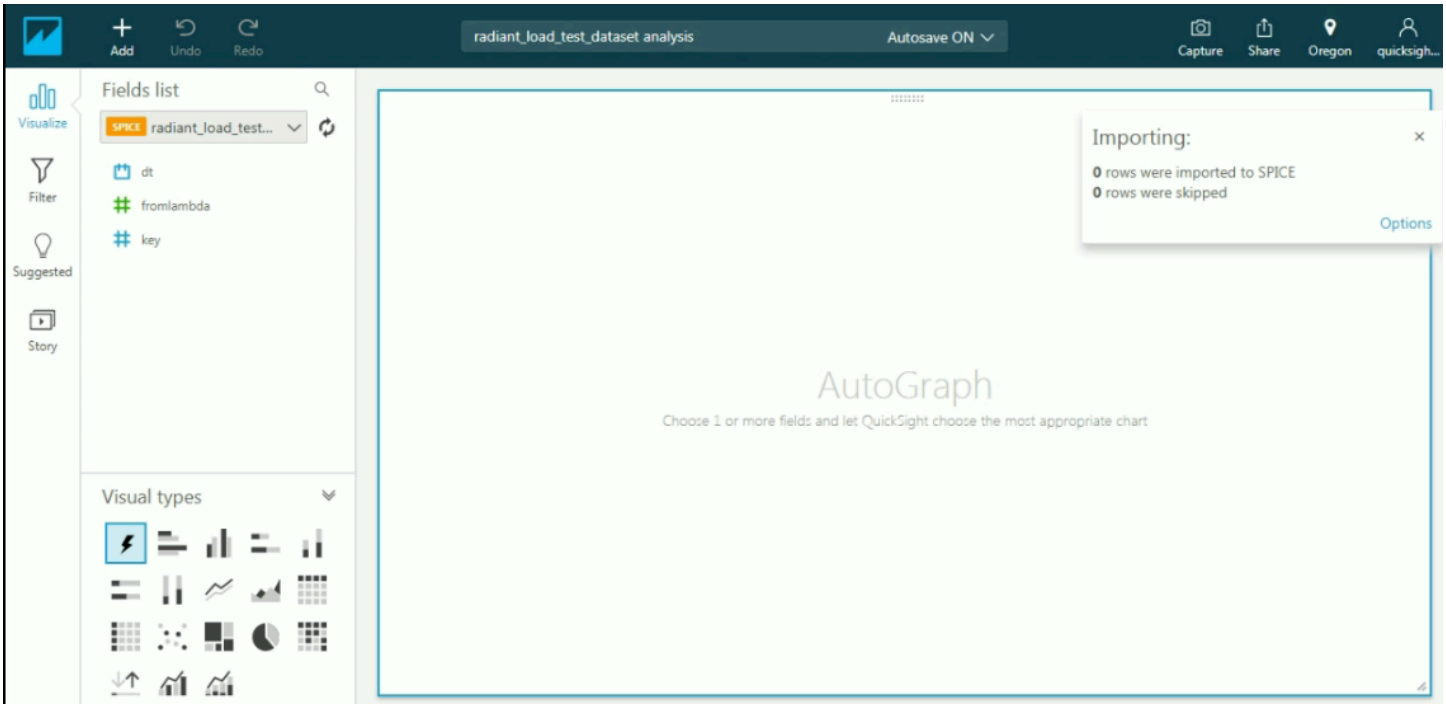
So beginnen Sie mit Ihrem Amazon QuickSight Visualisierungen, Sie müssen ein Amazon erstellen QuickSight Konto. Stellen Sie sicher, dass Sie Amazon geben QuickSight Zugriff auf IhreAWS IoT Analytics-Daten, wenn Sie Ihr -Konto einrichten. Wenn Sie bereits ein -Konto haben, geben Sie Amazon QuickSight Zugriff auf IhreAWS IoT AnalyticsDaten durch AuswahlAdmin,Verwalten von QuickSight,Sicherheit & Berechtigungenaus. UNDERQuickSight Zugriff aufAWSDienstleistungen, wählenHinzufügen oder Entfernenund aktivieren Sie dann das Kontrollkästchen nebenAWS IoT Analyticsund wähleAktualisierenaus.



Nachdem Ihr -Konto eingerichtet wurde, vom Administrator Amazon QuickSight Konsolenseite wählenNeue AnalysisundNeuer Datasetund dann wählen SieAWS IoT Analyticsals Quelle. Geben Sie einen Namen für Ihre Datenquelle ein, wählen Sie ein zu importierendes Dataset aus und wählen Sie dannDatenquelle anlegenaus.



Nachdem Sie Ihre Datenquelle erstellt haben, können Sie Visualisierungen in Amazon QuickSight erstellen.



Weitere Informationen über Amazon QuickSight Dashboards und Datensätze finden Sie imAmazon QuickSight Dokumentationaus.

Markieren Ihrer AWS IoT Analytics-Ressourcen

Zur einfacheren Verwaltung von Kanälen, Datasets, Datenspeichern und Pipelines können Sie den einzelnen Ressourcen bei Bedarf eigene Metadaten in Form von Tags zuweisen. Dieses Kapitel beschreibt Tags und zeigt, wie Sie sie erstellen.

Themen

Grundlagen zu Tags (Markierungen)

Mit Tags (Markierungen) können Sie Ihre AWS IoT Analytics-Ressourcen auf unterschiedliche Weise kategorisieren (z. B. nach Zweck, Eigentümer oder Umgebung). Dies ist hilfreich, wenn Sie viele Ressourcen desselben Typs haben. In diesem Fall können Sie basierend auf den zugewiesenen Tags schnell bestimmte Ressourcen identifizieren. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, die Sie beide selbst definieren können. Sie können zum Beispiel eine Reihe von Tags für Ihre Kanäle definieren, mit denen Sie den Typ des Geräts nachverfolgen können, das für die Nachrichtenquelle jedes einzelnen Kanals verantwortlich ist. Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Eine Anzahl einheitlicher Tag (Markierung)-Schlüssel vereinfacht das Verwalten der Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen.

Sie können Tags auch verwenden, um Ihre Kosten zu kategorisieren und zu verfolgen. Wenn Sie Tags auf Kanäle, Datensätze, Datenspeicher oder Pipelines anwenden,AWS generiert einen Kostenzuordnungsbericht als CSV-Datei mit Ihrer Nutzung und Kosten gemäß Ihren Tags. Sie können Tags anwenden, die geschäftliche Kategorien (wie Kostenstellen, Anwendungsnamen oder Eigentümer) darstellen, um die Kosten für mehrere Services zu organisieren. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch.

Der Tag-Editor in derAWS Billing and Cost Management Konsole ist benutzerfreundlich und zentral und einheitlich dazu geeignet, Tags zentral und einheitlich zu erstellen und zu verwalten.

Weitere Informationen finden Sie unter Arbeiten mit dem Tag Editor im Erste Schritte mit demAWS Management Console.

Sie können mit Tags arbeiten, indem SieAWS CLI und dieAWS IoT Analytics API verwenden. Sie können Tags mit Kanälen, Datasets, Datenspeichern und Pipelines verknüpfen, wenn Sie diese erstellen. Verwenden Sie das Feld Tagsin den folgenden Befehlen:

- CreateChannel
- CreateDataset
- CreateDatastore
- CreatePipeline

Sie können Tags für vorhandene -Ressourcen hinzufügen, ändern oder löschen, ändern oder löschen. Verwenden Sie 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 mit demselben Schlüssel wie ein vorhandenes Tag für diese -Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle der Ressource zugeordneten Tags ebenfalls gelöscht.

Verwenden von Tags mit IAM-Richtlinien

Sie können das `Condition`-Element (auch als `Condition`-Block bezeichnet) mit den folgenden Bedingungskontextschlüsseln und -werten in einer IAM-Richtlinie zum Steuern des Benutzerzugriffs (Berechtigungen) basierend auf den Tags einer Ressource verwenden:

- Dien`iotanalytics:ResourceTag/<tag-key>: <tag-value>` zum Zulassen oder Verweigern von Benutzeraktionen für Ressourcen mit bestimmten Tags.

- Verwenden Sie `aws:RequestTag/<tag-key>: <tag-value>`, um festzulegen, dass ein bestimmtes Tag verwendet (oder nicht verwendet) wird, wenn Sie eine API-Anfrage stellen, um eine Ressource zu erstellen oder zu ändern, die Tags zulässt.
- Verwenden Sie `aws:TagKeys: [<tag-key>, ...]`, um zu verlangen, dass ein bestimmter Satz von Tag-Schlüsseln verwendet wird (oder nicht), wenn eine API-Anforderung zum Erstellen einer Ressource durchgeführt wird, die Tags zulässt.

> **Note**
>
> Die Bedingungskontext-Schlüssel/-Werte in einer IAM-Richtlinie gelten nur fürAWS IoT Analytics Aktionen, bei denen ein Bezeichner für eine Ressource, die mit Tags versehen werden kann, ein erforderlicher Parameter ist. Beispielsweise DescribeLoggingOptionsist die Verwendung von auf der Grundlage von Schlüsseln/Werten im Bedingungskontext nicht erlaubt/verweigert, da in dieser Anfrage auf keine taggbare Ressource (Kanal, Datensatz, Datenspeicher oder Pipeline) verwiesen wird.

Weitere Informationen finden Sie unter Controlling access using tags (Zugriffssteuerung mit Tags) im IAM-Benutzerhandbuch. Der Referenzabschnitt zur IAM-JSON-Richtlinie dieses Handbuchs enthält detaillierte Syntax, Beschreibungen und Beispiele für die Elemente, Variablen und Bewertungslogik von JSON-Richtlinien in IAM.

Die folgende Beispielrichtlinie wendet zweigleisige Einschränkungen an. Ein Benutzer, der durch diese Richtlinie eingeschränkt ist:

1. Eine Ressource kann nicht mit dem Tag „env=prod“ versehen werden (siehe Zeile`"aws:RequestTag/env" : "prod"` im Beispiel).
2. Eine Ressource, die ein vorhandenes Tag „env=prod“ hat, kann nicht geändert oder darauf zugegriffen werden (siehe Zeile`"iotanalytics:ResourceTag/env" : "prod"` im Beispiel).

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

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/env" : "prod"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "iotanalytics:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iotanalytics:ResourceTag/env" : "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iotanalytics:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Sie können auch mehrere Tag-Werte für einen bestimmten Tag-Schlüssel angeben, indem Sie sie wie im folgenden Beispiel in eine Liste aufnehmen.

```
"StringEquals" : {
  "iotanalytics:ResourceTag/env" : ["dev", "test"]
}
```

> **Note**
>
> Wenn Sie Benutzern den Zugriff zu Ressourcen auf der Grundlage von Tags gewähren oder verweigern, müssen Sie daran denken, Benutzern explizit das Hinzufügen und Entfernen dieser Tags 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 modifizieren.

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 127 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 255 Unicode-Zeichen in UTF-8
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Verwenden Sie`aws: prefix` in Tag-Namen oder Werten nicht das, da es für dieAWS -Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Quelllimit angerechnet.
- Wenn Ihr Markierungsschema für mehrere -Services und -Ressourcen verwendet wird, denken Sie daran, dass andere Services möglicherweise Einschränkungen für zulässige Zeichen haben. Im allgemeinen zulässige Zeichen: Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = . _ : / @.

SQL-Ausdrücke inAWS IoT Analytics

Datasets werden unter Anwendung von SQL-Ausdrücken auf Daten in einen Datastore erzeugt.AWS IoT Analyticsnutzt dieselben SQL-Abfragen, Funktionen und Operatoren wie Amazon Athena.

AWS IoT Analyticsunterstützt eine Teilmenge der ANSI-Standard-SQL-Syntax.

```
SELECT [ ALL | DISTINCT ] select_expression [, ...]
[ FROM from_item [, ...] ]
[[ INNER | OUTER ] LEFT | RIGHT | FULL | CROSS JOIN join_item [ ON join_condition ]]
[ WHERE condition ]
[ GROUP BY [ ALL | DISTINCT ] grouping_element [, ...] ]
[ HAVING condition ]
[ UNION [ ALL | DISTINCT ] union_query ]
[ ORDER BY expression [ ASC | DESC ] [ NULLS FIRST | NULLS LAST] [, ...] ]
[ LIMIT [ count | ALL ] ]
```

Eine Beschreibung der Parameter finden Sie unterParameterimAmazon Athena Athena-Dokumentationaus.

AWS IoT Analyticsund Amazon Athena unterstützt Folgendes nicht:

- `WITH`-Klausel
- `CREATE TABLE AS SELECT`-Anweisungen.
- `INSERT INTO`-Anweisungen.
- Vorbereitete Anweisungen, die Sie nicht ausführen können`EXECUTE`mit`USING`aus.
- `CREATE TABLE LIKE`
- `DESCRIBE INPUT` und `DESCRIBE OUTPUT`
- `EXPLAIN`-Anweisungen.
- Benutzerdefinierte Funktionen (UDF oder UDAF)
- Gespeicherte Prozeduren
- Verbundene Konnektoren

Themen

- Unterstützte SQL-Funktionalität inAWS IoT Analytics

- Behebung häufiger Probleme mit SQL-Abfragen inAWS IoT Analytics

Unterstützte SQL-Funktionalität inAWS IoT Analytics

Datensätze werden mithilfe von SQL-Ausdrücken für Daten in einem Datenspeicher generiert. Die Abfragen, die Sie ausführen,AWS IoT Analytics basieren auf Presto 0.217.

Unterstützte Datentypen

AWS IoT Analyticsund Amazon Athena unterstützen diese Datentypen.

- primitive_type
  - `TINYINT`
  - `SMALLINT`
  - `INT`
  - `BIGINT`
  - `BOOLEAN`
  - `DOUBLE`
  - `FLOAT`
  - `STRING`
  - `TIMESTAMP`
  - `DECIMAL(precision, scale)`
  - `DATE`
  - `CHAR`(Zeichendaten fester Länge mit einer bestimmten Länge)
  - `VARCHAR`(Zeichendaten variabler Länge mit einer bestimmten Länge)
- array_type
  - `ARRAY<data_type>`
- map_type
  - `MAP<primitive_type, data_type>`
- struct_type
  - `STRUCT<col_name:data_type[COMMENT col_comment][,...]>`

> **Note**
>
> AWS IoT Analyticsund Amazon Athena unterstützt einige Datentypen nicht.

Unterstützte Funktionen

Die Funktionen von Amazon Athena undAWS IoT Analytics SQL basieren auf Presto 0.217. Informationen zu verwandten Funktionen, Operatoren und Ausdrücken finden Sie unter Funktionen und Operatoren und in den folgenden spezifischen Abschnitten der Presto-Dokumentation.

- Logische Operatoren
- Vergleichsfunktionen und Operatoren
- Bedingte Ausdrücke
- Konvertierungs-Funktionen
- Mathematische Funktionen und Operatoren
- Bitweise-Funktionen
- Dezimale Funktionen und Operatoren
- Zeichenfolgen-Funktionen und -Operatoren
- Binäre Funktionen
- Datums- und Zeitfunktionen und -Operatoren
- Funktionen für reguläre Ausdrücke
- JSON-Funktionen und -Operatoren
- URL-Funktionen
- Aggregationsfunktionen
- Fensterfunktionen
- Farb-Funktionen
- Array-Funktionen und -Operatoren
- Zuordnungs-Funktionen und -Operatoren
- Lambda-Ausdrücke und -Funktionen
- Teradata-Funktionen

> **Note**
>
> AWS IoT Analyticsund Amazon Athena unterstützt keine benutzerdefinierten Funktionen (UDFs oder UDAFs) oder gespeicherte Prozeduren.

Behebung häufiger Probleme mit SQL-Abfragen inAWS IoT Analytics

Verwenden Sie die folgenden Informationen für die Problembehandlung bei Ihren SQL-Abfragen inAWS IoT Analyticsaus.

- Um einem einzigen Anführungszeichen zu ent, gehen Sie mit einem weiteren einzigen Zitat voraus. Verwechseln Sie dies nicht mit einem doppelten Anführungszeichen.

  Example Beispiel

  ```
  SELECT 'O''Reilly'
  ```

- Um Unterstrichen zu entkommenverwenden Sie Backticks, um Datenspeicher-Spaltennamen zu umschließen, die mit einem Unterstrich beginnen.

  Example Beispiel

  ```
  SELECT `_myMessageAttribute` FROM myDataStore
  ```

- So entkommen Sie Namen mit Zahlenumschließen, umschließen Sie Datenspeichernamen, die Zahlen enthalten, in doppelte Anführungszeichen.

  Example Beispiel

  ```
  SELECT * FROM "myDataStore123"
  ```

- Um reservierte Schlüsselwörter zu entumschließen, reservierte Schlüsselwörter in doppelte Anführungszeichen umschließen. Weitere Informationen finden Sie unterListe reservierter SchlüsselwörterinSQL SELECT-Anweisungenaus.

Sicherheit in AWS IoT Analytics

Cloud-Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die entwickelt wurde, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Das -Modell der geteilten Verantwortung hat dies als Sicherheit der Cloud und Sicherheit in der Cloud beschrieben:

- Sicherheit der Cloud – AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Services in der AWS Cloud ausführt. stellt Ihnen AWS außerdem Services bereit, 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 Analytics, finden Sie unter -AWS Services im Rahmen des Compliance-Programms .
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. 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 geteilten Verantwortung bei der Verwendung von einsetzen können AWS IoT Analytics. Die folgenden Themen veranschaulichen, wie Sie konfigurieren, AWS IoT Analytics um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Ihnen bei der Überwachung und Sicherung Ihrer - AWS IoT Analytics Ressourcen helfen können.

AWS Identity and Access Management in AWS IoT Analytics

AWS Identity and Access Management (IAM) ist ein - AWS Service, mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von - AWS IoT Analytics Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein - AWS Service, den Sie ohne zusätzliche Kosten nutzen können.

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS IoT Analytics.

Service-Benutzer – Wenn Sie den AWS IoT Analytics Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS IoT Analytics Funktionen ausführen, 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 für AWS IoT Analytics Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS IoT Analytics haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für AWS IoT Analytics Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS IoT Analytics. Ihre Aufgabe besteht darin, zu bestimmen, auf welche AWS IoT Analytics Funktionen und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit verwenden kann AWS IoT Analytics, finden Sie unter Funktionsweise AWS IoT Analytics von mit IAM.

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

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsanmeldeinformationen bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

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

Je nachdem, um welchen Benutzertyp Sie es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung

bei AWSfinden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

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

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

AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

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

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

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

IAM-Rollen

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

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-ServicesSie jedoch eine Richtlinie direkt an

eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder -Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das der Instance zugeordnet ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-

Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

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

Verwalten des Zugriffs mit Richtlinien

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

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, 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. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

Identitätsbasierte Richtlinien

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

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie

stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, erfahren Sie unter Logik der Richtlinienbewertung im IAM-Benutzerhandbuch.

Funktionsweise AWS IoT Analytics von mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS IoT Analytics, sollten Sie verstehen, welche IAM-Funktionen Sie mit verwenden können AWS IoT Analytics. Einen Überblick über das Zusammenwirken von AWS IoT Analytics und anderen - AWS Services mit IAM finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Themen auf dieser Seite:

- AWS IoT Analytics Identitätsbasierte Richtlinien
- AWS IoT Analytics ressourcenbasierte Richtlinien
- Autorisierung auf der Basis von AWS IoT Analytics Tags
- AWS IoT Analytics IAM-Rollen

AWS IoT Analytics Identitätsbasierte Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie erlaubte oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zugelassen oder verweigert werden. AWS IoT Analytics unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Das Element `Action` einer identitätsbasierten IAM-Richtlinie beschreibt die spezifischen Aktionen, die von der Richtlinie zugelassen oder abgelehnt werden. Richtlinienaktionen haben in der Regel denselben Namen wie die zugehörige AWS API-Operation. Die Aktionen werden in einer Richtlinie verwendet, um Berechtigungen zum Ausführen der zugehörigen Operation zu erteilen.

Richtlinienaktion in AWS IoT Analytics verwendet das folgende Präfix vor der Aktion: `iotanalytics:` Um beispielsweise jemandem die Berechtigung zum Erstellen eines AWS IoT Analytics -Kanals mit der AWS IoT Analytics `CreateChannel` API-Operation zu erteilen, fügen Sie die `iotanalytics:BatchPuMessage` Aktion in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein - `Action` oder -`NotAction`Element enthalten. AWS IoT Analytics definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

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

```
"Action": [
    "iotanalytics:action1",
    "iotanalytics: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": "iotanalytics:Describe*"
```

Eine Liste der AWS IoT Analytics Aktionen finden Sie unter Von definierte Aktionen AWS IoT Analytics im IAM-Benutzerhandbuch.

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 unter Verwendung eines ARN oder eines Platzhalters (*) an, um anzugeben, dass die Anweisung für alle Ressourcen gilt.

Die AWS IoT Analytics Datensatzressource hat den folgenden ARN.

```
arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}
```

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

Um beispielsweise das `Foobar`-Dataset in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:iotanalytics:us-east-1:123456789012:dataset/Foobar"
```

Um alle Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:iotanalytics:us-east-1:123456789012:dataset/*"
```

Einige AWS IoT Analytics Aktionen, z. B. das Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

Einige AWS IoT Analytics API-Aktionen umfassen mehrere Ressourcen. Beispielsweise `CreatePipeline` verweist als Kanal und Datensatz, sodass ein Benutzer über Berechtigungen zur Verwendung des Kanals und des Datensatzes verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

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

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

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, wertet AWS die Bedingung mittels 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 unter IAM-Richtlinienelemente: Variablen und Tags (Markierungen) im IAM-Benutzerhandbuch.

AWS IoT Analytics stellt keine bereinigungsspezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel . im IAM-Benutzerhandbuch.

Beispiele

Beispiele für AWS IoT Analytics identitätsbasierte Richtlinien finden Sie unter AWS IoT Analytics Beispiele für identitätsbasierte Richtlinien.

AWS IoT Analytics ressourcenbasierte Richtlinien

AWS IoT Analytics unterstützt keine ressourcenbasierten Richtlinien. Ein Beispiel für eine detaillierte Seite mit ressourcenbasierten Richtlinien finden Sie unter Verwenden ressourcenbasierter Richtlinien für AWS Lambda im AWS Lambda -Entwicklerhandbuch.

Autorisierung auf der Basis von AWS IoT Analytics Tags

Sie können Tags an AWS IoT Analytics Ressourcen anfügen oder Tags in einer Anforderung an übergeben AWS IoT Analytics. Um den Zugriff basierend auf Tags zu steuern, geben Ihre Tag-Informationen im Bedingungselement einer Richtlinie mithilfe der `aws:TagKeys`Bedingungsschlüssel `iotanalytics:ResourceTag/{key-name}, aws:RequestTag/{key-name}` oder an. Weitere Informationen zum Markieren von AWS IoT Analytics Ressourcen finden Sie unter Markieren Ihrer AWS IoT Analytics Ressourcen.

Ein Beispiel für eine identitätsbasierte Richtlinie zum Beschränken des Zugriffs auf eine Ressource basierend auf den Tags auf dieser Ressource finden Sie unter Anzeigen von AWS IoT Analytics Kanälen basierend auf Tags.

AWS IoT Analytics IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

Verwenden temporärer Anmeldeinformationen mit AWS IoT Analytics

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

AWS IoT Analytics unterstützt die Verwendung temporärer Anmeldeinformationen nicht.

Service-verknüpfte Rollen

Servicegebundene Rollen ermöglichen es dem AWS Service, auf Ressourcen in anderen Services zuzugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

AWS IoT Analytics unterstützt keine serviceverknüpften 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 zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

AWS IoT Analytics unterstützt Servicerollen.

Dienstübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem 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,AWSbietet Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, mit Serviceprinzipalen, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung des`aws:SourceArn`und`aws:SourceAccount`Globale Bedingungskontextschlüssel in Ressourcenrichtlinien. Dies schränkt die Berechtigungen ein, dieAWS IoT Analyticsgibt der Ressource einen weiteren Dienst. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der effektivste Weg, um sich vor dem Confused Deputy-Problem zu schützen, ist`aws:SourceArn`globaler Bedingungskontextschlüssel mit dem vollständigen Amazon-Ressourcenname (ARN) der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. Zum Beispiel `arn:aws:`*`iotanalytics`*`::`*`123456789012`*`:*`.

Themen

- Prävention für Amazon S3Eimer
- Prävention mit Amazon CloudWatch Logs (Protokolle)
- Confused -Deputy-Prävention fürAWS IoT AnalyticsRessourcen

Prävention für Amazon S3Eimer

Wenn Sie vom Kunden verwalteten Amazon S3 S3-Speicher für IhreAWS IoT AnalyticsDatenspeicher, der Amazon S3 S3-Bucket, in dem Ihre Daten gespeichert werden, kann verwirrten Deputy Problemen ausgesetzt sein.

Nikki Wolf verwendet beispielsweise einen Amazon S3 S3-Bucket im Besitz eines Kunden namens*`DOC-BEISPIEL-BUCKET`*. Der Bucket speichert Informationen für eineAWS IoT AnalyticsDatenspeicher, der in der Region erstellt wurde*`us-east-1`*. Sie legt eine Richtlinie fest, die dasAWS IoT Analyticsabzufragender Dienstprinzip*`DOC-BEISPIEL-BUCKET`*in ihrem Namen. Nikkis Mitarbeiter, Li Juan, fragt*`DOC-BEISPIEL-BUCKET`*von ihrem eigenen Konto aus und erstellt einen Datensatz mit den Ergebnissen. Infolgedessen hat derAWS IoT AnalyticsDie Dienstleiterin fragte Nikkis Amazon S3 S3-Bucket in Lis Namen ab, obwohl Li die Anfrage von ihrem Konto aus ausgeführt hatte.

Um dies zu verhindern, kann Nikki die`aws:SourceAccount`-Bedingung für`aws:SourceArn`Bedingung in der Richtlinie für*DOC-BEISPIEL-BUCKET*.

Geben Sie den**`aws:SourceAccount`**Bedingung- Das folgende Beispiel einer Bucket-Richtlinie gibt an, dass nurAWS IoT AnalyticsRessourcen aus Nikkis Konto (*123456789012*) kann darauf zugreifen*DOC-BEISPIEL-BUCKET*.

```
{
    "Version": "2012-10-17",
    "Id": "MyPolicyID",
    "Statement": [
        {
            "Sid": "ConfusedDeputyPreventionExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

Geben Sie den**`aws:SourceArn`**Bedingung- Alternativ kann Nikki das`aws:SourceArn`Bedingung.

```
{
```

```
    "Version": "2012-10-17",
    "Id": "MyPolicyID",
    "Statement": [
        {
            "Sid": "ConfusedDeputyPreventionExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:iotanalytics:us-east-1:123456789012:dataset/DOC-
EXAMPLE-DATASET",
                        "arn:aws:iotanalytics:us-east-1:123456789012:datastore/DOC-
EXAMPLE-DATASTORE"
                    ]
                }
            }
        }
    ]
}
```

Prävention mit Amazon CloudWatch Logs (Protokolle)

Sie können das Confused Deputy-Problem während der Überwachung mit Amazon umgehen CloudWatch Logs. Die folgende Ressourcenrichtlinie zeigt, wie das verwirrte Deputy-Problem verhindert werden kann:

- Der Globale Bedingungskontextschlüsselaws:SourceArn
- Dieaws:SourceAccountmit deinemAWS-Konto-ID
- Die Kundenressource, die mit demsts:AssumeRoleanfragen inAWS IoT Analytics

Ersetzen*123456789012*mit deinemAWS-Konto-ID und*us-east-1*mit der Region IhresAWS IoT Analyticsaccount im folgenden Beispiel.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": "logs:PutLogEvents",
            "Resource": "*",
            "Condition":{
                "ArnLike":{
                    "aws:SourceArn":"arn:aws:iotanalytics:us-east-1:123456789012:*/*"
                },
                "StringEquals":{
                    "aws:SourceAccount":"123456789012"
                }
            }
    ]
}
```

Weitere Informationen zur Aktivierung und Konfiguration von Amazon CloudWatch Protokolle, siehethe section called “Protokollierung und Überwachung”.

Confused -Deputy-Prävention fürAWS IoT AnalyticsRessourcen

Wenn du gewährstAWS IoT AnalyticsBerechtigung, Aktionen auf IhremAWS IoT AnalyticsRessourcen können die Ressourcen verwirrten Stellvertreterfragen ausgesetzt sein. Um das verwirrte Deputy-Problem zu vermeiden, können Sie die erteilten Berechtigungen einschränkenAWS IoT Analyticsmit den folgenden Beispiel-Ressourcenrichtlinien.

Themen

- Prävention fürAWS IoT Analytics-Kanäle und -Datenspeicher

- Vermeidung des Problems des verwirrten StellvertretersAWS IoT AnalyticsRegeln zur Bereitstellung von Datensatz

Prävention fürAWS IoT Analytics-Kanäle und -Datenspeicher

Sie verwenden IAM-Rollen, um dieAWS-Ressourcen, dieAWS IoT Analyticskann in Ihrem Namen darauf zugreifen. Um zu verhindern, dass Ihre Rolle dem verwirrten Stellvertreterproblem ausgesetzt wird, können SieAWS-Konto in der`aws:SourceAccount`Element und der ARN desAWS IoT AnalyticsRessource in der`aws:SourceArn`Element der Vertrauensrichtlinie, die Sie einer Rolle zuordnen.

Im folgenden Beispiel ersetzen*123456789012*mit deinemAWS-Konto-ID und*arn: aws:iot-analytics:aws-region:123456789012: Kanal/DOC-Beispiel-Kanal*mit dem ARN einesAWS IoT AnalyticsKanal oder Datenspeicher.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "iotanalytics.amazonaws.com"
       },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iotanalytics:aws-region:123456789012:channel/DOC-
EXAMPLE-CHANNEL"
        }
      }
    }
  ]
}
```

Weitere Informationen zu den vom Kunden verwalteten S3-Speicheroptionen für Kanäle und Datenspeicher finden Sie

unterCustomerManagedChannelS3StorageundCustomerManagedDatastoreS3Storagein derAWS IoT AnalyticsAPI-Referenz.

Vermeidung des Problems des verwirrten StellvertretersAWS IoT AnalyticsRegeln zur Bereitstellung von Datensatz

Die IAM-RolleAWS IoT Analyticsgeht davon aus, dass Datensatzabfrageergebnisse an Amazon S3 oder anAWS IoT Eventskann verwirrten Stellvertreterproblemen ausgesetzt sein. Um das Confused -Deputy-Problem zu vermeiden,AWS-Konto in deraws:SourceAccountElement und der ARN desAWS IoT AnalyticsRessource in deraws:SourceArnElement der Vertrauensrichtlinie, die Sie Ihrer Rolle zuordnen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfusedDeputyPreventionExampleTrustPolicyDocument",
      "Effect": "Allow",
      "Principal": {
        "Service": "iotanalytics.amazonaws.com"
       },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iotanalytics:aws-region:123456789012:dataset/DOC-
EXAMPLE-DATASET"
        }
      }
    }
  ]
}
```

Weitere Informationen zum Konfigurieren von Regeln zur Bereitstellung von Dataset-Inhalten finden Sie untercontentDeliveryRulesin derAWS IoT AnalyticsAPI-Referenz.

AWS IoT Analytics Beispiele für identitätsbasierte Richtlinien

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS IoT Analytics -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben über die AWS Management Console

AWS CLI, die oder die AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen zum Erstellen einer identitätsbasierten IAM-Richtlinie anhand dieser Beispiel-JSON-Richtliniendokumente finden Sie unter Erstellen von Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.

Themen auf dieser Seite:

- Bewährte Methoden für Richtlinien
- Verwenden der AWS IoT Analytics Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugreifen auf eine AWS IoT Analytics Eingabe
- Anzeigen von AWS IoT Analytics Kanälen basierend auf Tags

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie können festlegen, ob jemand AWS IoT Analytics Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr AWS -Konto verursachen. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit von AWS verwalteten Richtlinien – Um AWS IoT Analytics schnell mit der Verwendung von zu beginnen, verwenden Sie von AWS verwaltete Richtlinien, um Ihren Mitarbeitern die von ihnen benötigten Berechtigungen zu erteilen. Diese Richtlinien sind bereits in Ihrem Konto verfügbar und werden von verwaltet und aktualisiert AWS. Weitere Informationen finden Sie unter Erste Schritte mit Berechtigungen mit von AWS verwalteten Richtlinien im IAM-Benutzerhandbuch.
- Gewähren der geringsten Berechtigung – Wenn Sie benutzerdefinierte Richtlinien erstellen, gewähren Sie 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 unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.

- Aktivieren von MFA für sensible Vorgänge – Fordern Sie Benutzer für zusätzliche Sicherheit auf, Multi-Faktor-Authentifizierung (MFA) zu verwenden, um auf sensible Ressourcen oder API-Operationen zuzugreifen. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.
- Verwenden von Richtlinienbedingungen für zusätzliche Sicherheit – Sofern dies praktikabel ist, definieren Sie die Bedingungen, unter denen Ihre identitätsbasierten Richtlinien den Zugriff auf eine Ressource zulassen. Sie können beispielsweise eine Bedingung schreiben, um einen Bereich zulässiger IP-Adressen anzugeben, von denen eine Anforderung stammen muss. Sie können auch Bedingungen schreiben, die Anforderungen nur innerhalb eines bestimmten Datums- oder Zeitbereichs zulassen oder die Verwendung von SSL oder MFA fordern. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Verwenden der AWS IoT Analytics Konsole

Um auf die AWS IoT Analytics Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS IoT Analytics Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die mindestens erforderlichen Berechtigungen. Die Konsole funktioniert nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten weiterhin die AWS IoT Analytics Konsole verwenden können, fügen Sie den Entitäten auch die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "iotanalytics:BatchPutMessage",
                 "iotanalytics:CancelPipelineReprocessing",
                 "iotanalytics:CreateChannel",
                 "iotanalytics:CreateDataset",
                 "iotanalytics:CreateDatasetContent",
                 "iotanalytics:CreateDatastore",
                 "iotanalytics:CreatePipeline",
```

```
                "iotanalytics:DeleteChannel",
                "iotanalytics:DeleteDataset",
                "iotanalytics:DeleteDatasetContent",
                "iotanalytics:DeleteDatastore",
                "iotanalytics:DeletePipeline",
                "iotanalytics:DescribeChannel",
                "iotanalytics:DescribeDataset",
                "iotanalytics:DescribeDatastore",
                "iotanalytics:DescribeLoggingOptions",
                "iotanalytics:DescribePipeline",
                "iotanalytics:GetDatasetContent",
                "iotanalytics:ListChannels",
                "iotanalytics:ListDatasetContents",
                "iotanalytics:ListDatasets",
                "iotanalytics:ListDatastores",
                "iotanalytics:ListPipelines",
                "iotanalytics:ListTagsForResource",
                "iotanalytics:PutLoggingOptions",
                "iotanalytics:RunPipelineActivity",
                "iotanalytics:SampleChannelData",
                "iotanalytics:StartPipelineReprocessing",
                "iotanalytics:TagResource",
                "iotanalytics:UntagResource",
                "iotanalytics:UpdateChannel",
                "iotanalytics:UpdateDataset",
                "iotanalytics:UpdateDatastore",
                "iotanalytics:UpdatePipeline"
            ],
            "Resource": "arn:${Partition}:iotanalytics:${Region}:${Account}:channel/
${channelName}",
            "Resource": "arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/
${datasetName}",
            "Resource": "arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/
${datastoreName}",
            "Resource": "arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/
${pipelineName}"
        }
    ]
 }
```

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

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 enthält Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder 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 AWS IoT Analytics Eingabe

In diesem Beispiel möchten Sie einem Benutzer in Ihrem AWS-Konto Zugriff auf einen Ihrer AWS IoT Analytics Kanäle gewähren, `exampleChannel`. Sie möchten der Verwendung auch erlauben, Kanäle hinzuzufügen, zu aktualisieren und zu löschen.

Die Richtlinie gewährt dem Benutzer die `iotanalytics:ListChannels, iotanalytics:DescribeChannel, iotanalytics:CreateChannel, iotanalytics:DeleteChannel, and iotanalytics:UpdateChannel` Berechtigungen. Eine Beispielanleitung für den Amazon S3-Service, der Benutzern Berechtigungen erteilt und diese mithilfe der Konsole testet, finden Sie unter Eine Beispielanleitung: Verwenden von Benutzerrichtlinien zum Steuern des Zugriffs auf Ihren Bucket.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListChannelsInConsole",
         "Effect":"Allow",
         "Action":[
            "iotanalytics:ListChannels"
         ],
         "Resource":"arn:aws:iotanalytics:::*"
      },
      {
         "Sid":"ViewSpecificChannelInfo",
         "Effect":"Allow",
         "Action":[
            "iotanalytics:DescribeChannel"
         ],
         "Resource":"arn:aws:iotanalytics:::exampleChannel"
      },
      {
         "Sid":"ManageChannels",
         "Effect":"Allow",
         "Action":[
            "iotanalytics:CreateChannel",
            "iotanalytics:DeleteChannel",
            "iotanalytics:DescribeChannel",
            "iotanalytics:ListChannels",
            "iotanalytics:UpdateChannel"
         ],
```

```
         "Resource":"arn:aws:iotanalytics:::exampleChannel/*"
      }
   ]
}
```

Anzeigen von AWS IoT Analytics Kanälen basierend auf Tags

Sie können Bedingungen in Ihrer identitätsbasierten Richtlinie verwenden, um den Zugriff auf AWS IoT Analytics Ressourcen basierend auf Tags zu steuern. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die die Anzeige einer `channel` gestattet. Berechtigungen werden jedoch nur erteilt, wenn das `channel` Tag den Wert des Benutzernamens dieses Benutzers `0wner` hat. Diese Richtlinie gewährt auch die Berechtigungen, die für die Ausführung dieser Aktion auf der Konsole erforderlich sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListChannelsInConsole",
            "Effect": "Allow",
            "Action": "iotanalytics:ListChannels",
            "Resource": "*"
        },
        {
            "Sid": "ViewChannelsIfOwner",
            "Effect": "Allow",
            "Action": "iotanalytics:ListChannels",
            "Resource": "arn:aws:iotanalytics:*:*:channel/*",
            "Condition": {
                "StringEquals": {"iotanalytics:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Sie können diese Richtlinie den -Benutzern in Ihrem Konto zuweisen. Wenn ein Benutzer mit dem Namen `richard-roe` versucht, eine anzuzeigen AWS IoT Analytics `channel`, `channel` muss mit markiert werden`0wner=richard-roe or owner=richard-roe`. Andernfalls wird der Zugriff abgelehnt. Der Tag-Schlüssel `0wner` der Bedingung stimmt sowohl mit `0wner` als auch mit `owner` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung

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

Fehlerbehebung für AWS IoT Analytics Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit auftreten können AWS IoT Analytics.

Themen

- Ich bin nicht autorisiert, eine Aktion in auszuführen AWS IoT Analytics
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert.
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine - AWS IoT Analytics Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in auszuführen AWS IoT Analytics

Wenn Ihnen AWS Management Console mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihren Benutzernamen und Ihr Passwort zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` Benutzer versucht, die Konsole zu verwenden, um Details zu einem anzuzeigen, `channel` aber keine `iotanalytics:ListChannels` Berechtigungen besitzt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotanalytics:``ListChannels`` on resource: ``my-example-channel``
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, damit er mit der `iotanalytics:ListChannel` Aktion auf die `my-example-channel` Ressource zugreifen kann.

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 Analytics übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte 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 Analytics 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 meines AWS-Konto Zugriff auf meine - AWS IoT Analytics Ressourcen gewähren

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 Services, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACL) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre -Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob diese Funktionen AWS IoT Analytics unterstützt, finden Sie unter Funktionsweise AWS IoT Analytics von mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre AWS-Konten -Ressourcen in Ihrem Besitz finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.

- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollieren und Überwachen in AWS IoT Analytics

AWS bietet verschiedene Tools für die Überwachung von AWS IoT Analytics. Sie können einige dieser Tools für die Überwachung konfigurieren. Einige der Tools erfordern manuelle Eingriffe. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Automatisierte Überwachungstools

Sie können die folgenden automatisierten Tools zur Überwachung von AWS IoT verwenden und möglicherweise auftretende Probleme melden:

- Amazon CloudWatch Logs: Überwachen, Speichern und Zugriff auf Ihre Protokolldateien vonAWS CloudTrail oder anderen Quellen. Weitere Informationen finden Sie unter Was istAWS CloudTrail Überwachungsprotokolldateien im CloudWatch Amazon-Benutzerhandbuch.
- AWS CloudTrail-Protokollüberwachung: Teilen Sie Protokolldateien zwischen Konten, überwachen Sie CloudTrail Protokolldateien in Echtzeit, indem Sie sie an die CloudWatch Logs senden, schreiben Sie Anwendungen zur Protokollverarbeitung in Java und vergewissern Sie sich, dass nach der Lieferung bis keine Änderungen an den Protokolldaten vorgenommen wurden CloudTrail. Weitere Informationen finden Sie im AWS CloudTrailBenutzerhandbuch unter Arbeiten mit CloudTrail Protokolldateien.

Manuelle Überwachungstools

Ein weiterer wichtiger Bestandteil der Überwachung von AWS IoT ist die manuelle Überwachung derjenigen Elemente, die die CloudWatch -Alarme nicht abdecken. DasAWS IoT CloudWatch, und andereAWS Service-Console-Dashboards bieten einen at-a-glance Überblick über den Zustand IhrerAWS Umgebung. Zudem empfehlen wir die Überprüfung der Protokolldateien auf AWS IoT Analytics.

- Die AWS IoT Analytics-Konsole zeigt Folgendes:
  - Kanäle
  - Pipelines

  - Datastores
  - Datensätze
  - Notebooks
  - Einstellungen
  - Lernen
- Die CloudWatch -Homepage zeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

  Zusätzlich können Sie CloudWatch für folgende Aufgaben nutzen:
  - Erstellen angepasster Dashboards zur Überwachung der gewünschten Services.
  - Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen
  - Durchsuchen und Suchen aller AWS-Ressourcenmetriken
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden

Überwachung mit Amazon CloudWatch Logs

AWS IoT Analyticsunterstützt die Protokollierung mit Amazon CloudWatch. Sie können die CloudWatch Amazon-Protokollierung fürAWS IoT Analytics mithilfe des `PutLoggingOptions`API-Vorgangs aktivieren und konfigurieren. In diesem Abschnitt wird beschrieben, wie Sie`PutLoggingOptions` mitAWS Identity and Access Management (IAM) die CloudWatch Amazon-Protokollierung für konfigurieren und aktivieren könnenAWS IoT Analytics.

Weitere Informationen zu CloudWatch -Protokollen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch. Weitere Informationen zuAWS IAM finden Sie im AWS Identity and Access Management-Benutzerhandbuch.

> **Note**
>
> Bevor Sie dieAWS IoT Analytics Protokollierung aktivieren, stellen Sie sicher, dass Sie die Zugriffsberechtigungen für CloudWatch Logs verstehen. Benutzer mit Zugriff auf CloudWatch Logs können Ihre Debugging-Informationen sehen. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Amazon CloudWatch Logs.

Erstellen Sie eine IAM-Rolle, um die Protokollierung zu aktivieren

So erstellen Sie eine IAM-Rolle, um die Protokollierung für Amazon zu aktivieren CloudWatch

1. Verwenden Sie die AWSIAM-Konsole oder den folgendenAWS IAM-CLI-Befehl, CreateRole, um eine neue IAM-Rolle mit einer Vertrauensbeziehungsrichtlinie (Vertrauensrichtlinie) zu erstellen. Die Vertrauensrichtlinie erteilt einer Entität wie Amazon die Berechtigung CloudWatch, die Rolle zu übernehmen.

```
aws iam create-role --role-name exampleRoleName --assume-role-policy-document
       exampleTrustPolicy.json
```

   Die`exampleTrustPolicy.json` Datei enthält den folgenden Inhalt.

> **Note**
>
> Dieses Beispiel enthält einen globalen Bedingungskontextschlüssel zum Schutz vor dem Confused-Deputy-Problem. Ersetzen Sie *123456789012* durch IhreAWS Konto-ID und *aws-region* durch dieAWS Region IhrerAWS Ressourcen. Weitere Informationen finden Sie unter the section called “Dienstübergreifende Confused-Deputy-Prävention”.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": "iotanalytics.amazonaws.com"
         },
         "Action": "sts:AssumeRole",
         "Condition": {
           "StringEquals": {
             "aws:SourceAccount": "123456789012"
           },
           "ArnLike": {
             "aws:SourceArn": "arn:aws:iotanalytics:aws-region:123456789012:*"
           }
         }
```

```
      }
   ]
}
```

Sie verwenden den ARN dieser Rolle später, wenn Sie denAWS IoT AnalyticsPutLoggingOptions Befehl aufrufen.

2. Verwenden SieAWS IAM PutRolePolicy, um der Rolle, die Sie in Schritt 1 erstellt haben, eine Berechtigungsrichtlinie (`arole policy`) zuzuordnen.

   ```
   aws iam put-role-policy --role-name exampleRoleName --policy-name
   examplePolicyName --policy-document exampleRolePolicy.json
   ```

   Die exampleRolePolicy JSON-Datei enthält den folgenden Inhalt.

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

3. Verwenden Sie den CloudWatch Amazon-Befehl, um Amazon dieAWS IoT Analytics Erlaubnis zu erteilen CloudWatch, Ereignisse zu protokollieren PutResourcePolicy.

   > **Note**
   >
   > Um das Sicherheitsproblem des verwirrten Stellvertreters zu vermeiden, empfehlen wir, dass Sie diesaws:SourceArn in Ihrer Ressourcenrichtlinie angeben. Dadurch wird der Zugriff eingeschränkt, sodass nur Anfragen zugelassen werden, die von einem bestimmten Konto stammen. Weitere Informationen über das Confused-Deputy-Problem finden Sie unterthe section called “Dienstübergreifende Confused-Deputy-Prävention”.

```
aws logs put-resource-policy --policy-in-json
exampleResourcePolicy.json
```

Die`exampleResourcePolicy.json` Datei enthält die folgende Ressourcenrichtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "iotanalytics.amazonaws.com"
            },
            "Action": "logs:PutLogEvents",
            "Resource": "*",
            "Condition":{
                "ArnLike":{
                    "aws:SourceArn":"arn:aws:iotanalytics:us-east-1:123456789012:*/
*"
                },
                "StringEquals":{
                    "aws:SourceAccount":"123456789012"
                }
            }
    ]
}
```

Konfigurieren und Aktivieren der Protokollierung

Verwenden Sie den`PutLoggingOptions` Befehl, um die CloudWatch Amazon-Protokollierung für zu konfigurieren und zu aktivierenAWS IoT Analytics. Der `roleArn` im Feld `loggingOptions` muss der ARN der Rolle sein, die Sie im vorherigen Abschnitt erstellt haben. Sie können auch den Befehl `DecribeLoggingOptions` verwenden, um die Einstellungen Ihrer Protokollierungsoptionen zu überprüfen.

PutLoggingOptions

Legt dieAWS IoT Analytics Protokollierungsoptionen fest oder aktualisiert sie. Wenn Sie den Wert eines`loggingOptions` Feldes aktualisieren, dauert es bis zu einer Minute, bis die Änderung

wirksam wird. Wenn Sie die Richtlinie ändern, die der Rolle zugeordnet ist, die Sie im`roleArn` Feld angegeben haben (z. B. um eine Richtlinie zu korrigieren, die nicht gültig ist), kann es außerdem bis zu fünf Minuten dauern, bis diese Änderung wirksam wird. Weitere Informationen finden Sie unter `PutLoggingOptions`.

DescribeLoggingOptions

Ruft die aktuellen Einstellungen derAWS IoT Analytics Protokollierungsoptionen ab. Weitere Informationen finden Sie unter `DescribeLoggingOptions`

Namespace, Metriken und Dimensionen

AWS IoT Analyticsfügt die folgenden Metriken in das CloudWatch Amazon-Repository ein:

Namespace
AWS/IoT-Analytik

Metrik	Beschreibung
ActionExecution	Die Anzahl der ausgeführten Aktionen.
ActionExecutionThrottled	Die Anzahl der Aktionen, die gedrosselt werden.
ActivityExecutionError	Die Anzahl der Fehler, die beim Ausführen der Pipeline-Aktivität erzeugt wurden.
IncomingMessages	Die Anzahl der Nachrichten, die im Kanal eingehen.
PipelineConcurrentExecutionCount	Die Anzahl der Pipeline-Aktivitäten, die gleichzeitig ausgeführt wurden.

Dimension	Beschreibung
ActionType	Der Typ der Aktion, die überwacht wird.

Dimension	Beschreibung
ChannelName	Der Name des Kanals, der überwacht wird.
DatasetName	Der Name des überwachten Datensatzes.
DatastoreName	Der Name des Datenspeichers, der überwacht wird.
PipelineActivityName	Der Name der Pipeline-Aktivität, die überwacht wird.
PipelineActivityType	Der Typ der Pipeline-Aktivität, die überwacht wird.
PipelineName	Der Name der Pipeline, die überwacht wird.

Überwachen Sie mit Amazon CloudWatch Events

AWS IoT Analyticsveröffentlicht automatisch ein Ereignis auf Amazon CloudWatch Events, wenn während einerAWS Lambda Aktivität ein Laufzeitfehler auftritt. Dieses Ereignis enthält eine detaillierte Fehlermeldung und die Schlüssel der Amazon Simple Storage Service (Amazon S3) -Objekte, die die unverarbeiteten Kanalnachrichten speichern. Sie können die Amazon S3 S3-Schlüssel verwenden, um die unverarbeiteten Kanalnachrichten erneut zu verarbeiten. Weitere Informationen finden Sie unterWiederaufarbeitung von Channel-Nachrichten StartPipelineReprocessingAPI in der AWS IoT AnalyticsAPI-Referenz und Was ist Amazon CloudWatch Events im Amazon CloudWatch Events-Benutzerhandbuch.

Sie können auch Ziele konfigurieren, die es Amazon CloudWatch Events ermöglichen, Benachrichtigungen zu senden oder weitere Maßnahmen zu ergreifen. Sie können die Benachrichtigung beispielsweise an eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange senden und dann die`StartReprocessingMessage` API aufrufen, um die in den Amazon S3 S3-Objekten gespeicherten Kanalnachrichten zu verarbeiten. Amazon CloudWatch Events unterstützt viele Arten von Zielen, wie zum Beispiel die folgenden:

- Amazon Kinesis Streams
- AWS Lambda-Funktionen
- Amazon Simple Notification Service (Amazon SNS)-Themen

- Amazon Simple Queue Service (Amazon SQS)-Warteschlangen

Eine Liste der unterstützten Ziele finden Sie unter Amazon EventBridge Targets im EventBridge Amazon-Benutzerhandbuch.

Ihre CloudWatch Eventressourcen und die zugehörigen Ziele müssen sich in derAWS Region befinden, in der Sie IhreAWS IoT Analytics Ressourcen erstellt haben. Weitere Informationen finden Sie unter Dienstendpunkte und Kontingente in der Allgemeine AWS-Referenz.

Die Benachrichtigung, die an Amazon CloudWatch Events für Laufzeitfehler in derAWS Lambda Aktivität gesendet wird, verwendet das folgende Format.

```
{
    "version": "version-id",
    "id": "event-id",
    "detail-type": "IoT Analytics Pipeline Failure Notification",
    "source": "aws.iotanalytics",
    "account": "aws-account",
    "time": "timestamp",
    "region": "aws-region",
    "resources": [
        "pipeline-arn"
    ],
    "detail": {
        "event-detail-version": "1.0",
        "pipeline-name": "pipeline-name",
        "error-code": "LAMBDA_FAILURE",
        "message": "error-message",
        "channel-messages": {
            "s3paths": [
                "s3-keys"
            ]
        },
        "activity-name": "lambda-activity-name",
        "lambda-function-arn": "lambda-function-arn"
    }
}
```

Beispiel für eine Benachrichtigung:

```
{
```

```
    "version": "0",
    "id": "204e672e-ef12-09af-4cfd-de3b53673ec6",
    "detail-type": "IoT Analytics Pipeline Failure Notification",
    "source": "aws.iotanalytics",
    "account": "123456789012",
    "time": "2020-10-15T23:47:02Z",
    "region": "ap-southeast-2",
    "resources": [
        "arn:aws:iotanalytics:ap-southeast-2:123456789012:pipeline/
test_pipeline_failure"
    ],
    "detail": {
        "event-detail-version": "1.0",
        "pipeline-name": "test_pipeline_failure",
        "error-code": "LAMBDA_FAILURE",
        "message": "Temp unavaliable",
        "channel-messages": {
        "s3paths": [
            "test_pipeline_failure/channel/cmr_channel/__dt=2020-10-15
 00:00:00/1602805530000_1602805560000_123456789012_cmr_channel_0_257.0.json.gz"
        ]
    },
    "activity-name": "LambdaActivity_33",
    "lambda-function-arn": "arn:aws:lambda:ap-
southeast-2:123456789012:function:lambda_activity"
    }
}
```

Verspätete Datenbenachrichtigungen über Amazon CloudWatch Events erhalten

Wenn Sie Datensatzinhalte mithilfe von Daten aus einem bestimmten Zeitraum erstellen, kommen einige Daten möglicherweise nicht rechtzeitig zur Verarbeitung an. Um eine Verzögerung zu vermeiden, können Sie einen`deltaTime` Offset für den angeben,`QueryFilter` wenn Sie einen Datensatz erstellen, indem Sie eine`queryAction` (eine SQL-Abfrage) anwenden. AWS IoT Analyticsverarbeitet immer noch die Daten, die innerhalb der Deltazeit ankommen, und der Inhalt Ihres Datensatzes weist eine Zeitverzögerung auf. Die Funktion für verspätete DatenbenachrichtigungenAWS IoT Analytics ermöglicht das Senden von Benachrichtigungen über Amazon CloudWatch Events, wenn Daten nach der Deltazeit eintreffen.

Sie können dieAWS IoT Analytics Konsole, die API, AWS Command Line Interface(AWS CLI) oder das AWSSDK verwenden, um Regeln für verspätete Daten für einen Datensatz festzulegen.

In derAWS IoT Analytics API stellt das`LateDataRuleConfiguration` Objekt die Late-Data-Regeleinstellungen eines Datensatzes dar. Dieses Objekt ist Teil des`Dataset` Objekts, das mit den`UpdateDataset` API-Vorgängen`CreateDataset` und verknüpft ist.

Parameter

Beim Erstellen einer Regel für verspätete Daten für einen Datensatz mitAWS IoT Analytics müssen Sie die folgenden Informationen angeben:

`ruleConfiguration` (**`LateDataRuleConfiguration`**)

Eine Struktur, die die Konfigurationsinformationen einer Regel für verspätete Daten enthält.

`deltaTimeSessionWindowConfiguration`

Eine Struktur, die die Konfigurationsinformationen eines Deltazeitsitzungsfensters enthält.

DeltaTime gibt einen Zeitinterval an. Sie können `DeltaTime` verwenden, um Dataset-Inhalte mit Daten zu erstellen, die seit der letzten Ausführung im Datenspeicher eingetroffen sind. Ein Beispiel für finden Sie unter Erstellen eines SQL-Datensatzes mit einem Delta-Fenster (CLI).`DeltaTime`

`timeoutInMinutes`

Ein Zeitintervall. Sie können verwenden,`timeoutInMinutes` damit Benachrichtigungen zu verspäteten Daten zusammenfassenAWS IoT Analytics können, die seit der letzten Ausführung erzeugt wurden. AWS IoT Analyticssendet jeweils einen Stapel an Benachrichtigungen an CloudWatch Events.

Typ: Ganzzahl

Gültiger Bereich: 1—1 000

`ruleName`

Name der Regel für verspätete Daten.

Typ: Zeichenfolge

> **Important**
>
> Um anzugeben`lateDataRules`, muss das Dataset den`DeltaTime` Filter anwenden.

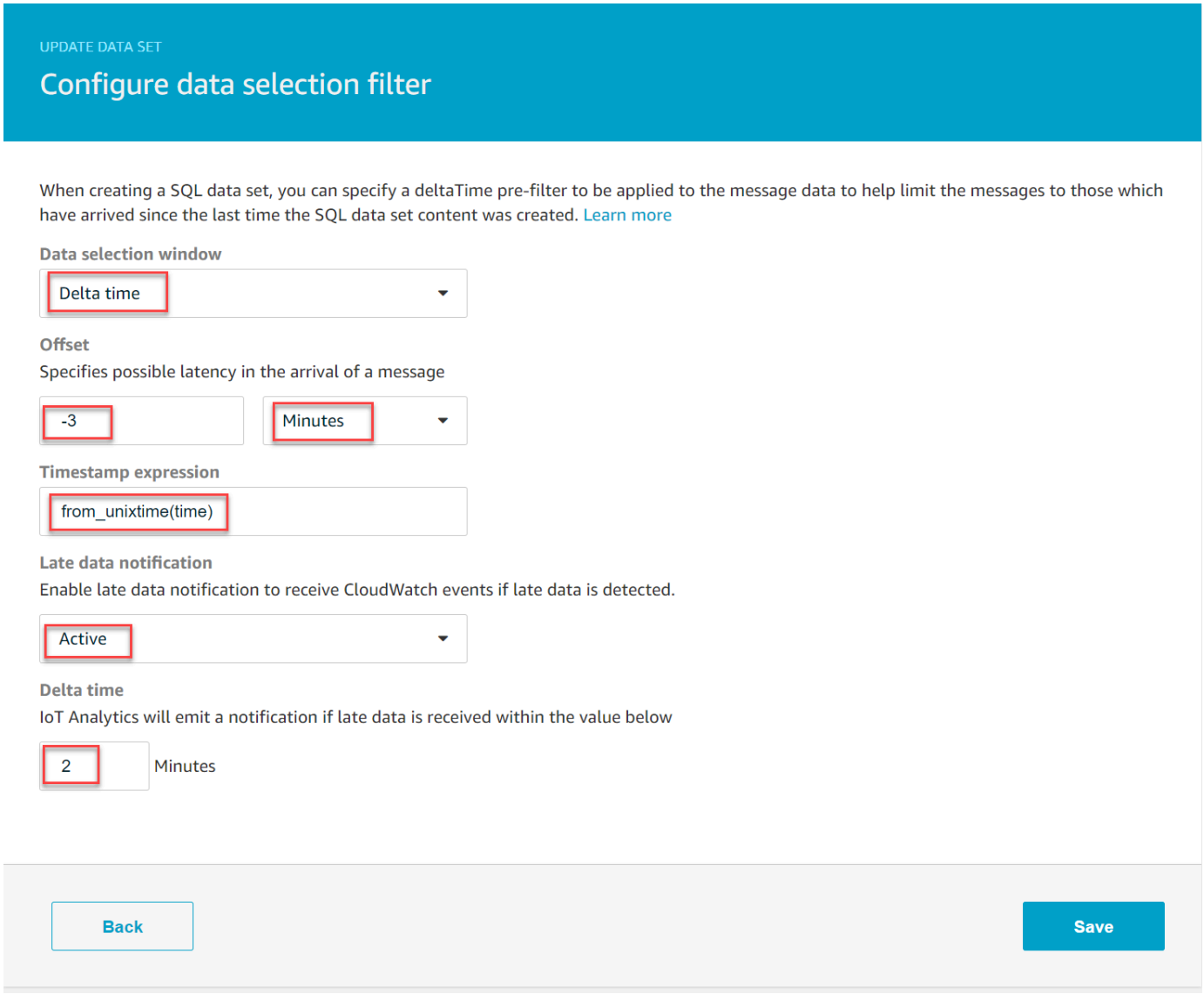
Regeln für verspätete Daten konfigurieren (Konsole)

Im folgenden Verfahren wird gezeigt, wie Sie die Regel für verspätete Daten eines Datensatzes in derAWS IoT Analytics Konsole konfigurieren.

So konfigurieren Sie Regeln für verspätete Daten

1. Melden Sie sich an der AWS IoT Analytics-Konsole an.
2. Wählen Sie im Navigationsbereich Datensätze aus.
3. Wählen Sie unter Datensätze den Zieldatensatz aus.
4. Wählen Sie im Navigationsbereich Details aus.
5. Wählen Sie im Bereich Delta-Fenster die Option Bearbeiten.
6. Führen Sie unter Configure data selection filter die folgenden Schritte aus:
   a. Wählen Sie für das Datenauswahlfenster die Option Deltazeit aus.
   b. Geben Sie für Offset einen Zeitraum ein, und wählen Sie dann eine Einheit aus.
   c. Geben Sie für Timestamp-Ausdruck einen Ausdruck ein. Dies kann der Name eines Zeitstempelfeldes oder ein SQL-Ausdruck sein, der die Uhrzeit ableiten kann, z. B. `from_unixtime (time)`.

      Weitere Informationen zum Schreiben eines Zeitstempelausdrucks finden Sie unter Funktionen und Operatoren für Datum und Uhrzeit in der Dokumentation zu Presto 0.172.
   d. Wählen Sie für Späte Datenbenachrichtigung die Option Aktiv aus.
   e. Geben Sie für Delta-Zeit eine Ganzzahl ein. Der gültige Bereich liegt zwischen 1 und 60
   f. Wählen Sie Speichern.



Regeln für späte Daten konfigurieren (CLI)

In derAWS IoT Analytics API stellt das`LateDataRuleConfiguration` Objekt die Late-Data-Regeleinstellungen eines Datensatzes dar. Dieses Objekt ist Teil des`Dataset` Objekts, das mit`CreateDataset` und verknüpft ist`UpdateDataset`. Sie können die API oder das AWSSDK verwenden AWS CLI, um Regeln für späte Daten für einen Datensatz festzulegen. Das folgende Beispiel verwendet die AWS CLI.

Um Ihren Datensatz mit den angegebenen Regeln für verspätete Daten zu erstellen, führen Sie den folgenden Befehl aus. Der Befehl setzt voraus, dass sich die`dataset.json` Datei im aktuellen Verzeichnis befindet.

> **Note**
>
> Sie können die UpdateDatasetAPI verwenden, um einen vorhandenen Datensatz zu aktualisieren.

```
aws iotanalytics create-dataset --cli-input-json file://dataset.json
```

Die`dataset.json` Datei sollte Folgendes enthalten:

- Ersetzen Sie *`demo_dataset`* durch den Namen des Zieldatensatzes.
- Ersetzen Sie *`demo_datastore`* durch den Namen des Zieldatenspeichers.
- Ersetzen Sie *`from_unixtime (time)`* durch den Namen eines Zeitstempelfeldes oder einen SQL-Ausdruck, der die Uhrzeit ableiten kann.

  Weitere Informationen zum Schreiben eines Zeitstempelausdrucks finden Sie unter Funktionen und Operatoren für Datum und Uhrzeit in der Dokumentation zu Presto 0.172.
- Ersetzen *`Sie das Timeout`* durch eine Ganzzahl zwischen 1—60.
- Ersetzen Sie *`demo_rule`* durch einen beliebigen Namen.

```
{
    "datasetName": "demo_dataset",
    "actions": [
        {
            "actionName": "myDatasetAction",
            "queryAction": {
                "filters": [
                    {
                        "deltaTime": {
                            "offsetSeconds": -180,
                            "timeExpression": "from_unixtime(time)"
                        }
                    }
                ],
                "sqlQuery": "SELECT * FROM demo_datastore"
            }
        }
    ],
```

```
    "retentionPeriod": {
        "unlimited": false,
        "numberOfDays": 90
    },
    "lateDataRules": [
        {
            "ruleConfiguration": {
                "deltaTimeSessionWindowConfiguration": {
                    "timeoutInMinutes": timeout
                }
            },
            "ruleName": "demo_rule"
        }
    ]
}
```

Abonnieren von Benachrichtigungen zu verspäteten Daten

In CloudWatch Events können Sie Regeln erstellen, die festlegen, wie verspätete Datenbenachrichtigungen verarbeitet werden, die von gesendet wurdenAWS IoT Analytics. Wenn CloudWatch Events die Benachrichtigungen erhält, werden die in Ihren Regeln definierten Zielaktionen aufgerufen.

Voraussetzungen für das Erstellen von Regeln für CloudWatch Ereignisse

Führen Sie vor dem Erstellen einer CloudWatch Ereignisregel fürAWS IoT Analytics die die folgenden Schritte aus:

- Machen Sie sich unter Ereignisse, Regeln und Ziele vertraut. CloudWatch
- Erstellen und konfigurieren Sie die Ziele, die durch Ihre CloudWatch Events-Regeln aufgerufen werden. Regeln können viele Arten von Zielen aufrufen, z. B. die folgenden:
  - Amazon Kinesis Streams
  - AWS Lambda-Funktionen
  - Amazon Simple Notification Service (Amazon SNS)-Themen
  - Amazon Simple Queue Service (Amazon SQS)-Warteschlangen

  Ihre CloudWatch Events-Regel und die zugehörigen Ziele müssen sich in derAWS Region befinden, in der Sie IhreAWS IoT Analytics Ressourcen erstellt haben. Weitere Informationen finden Sie unter Dienstendpunkte und Kontingente in der Allgemeine AWS-Referenz.

Weitere Informationen finden Sie unter Was sind CloudWatch Ereignisse? und Erste Schritte mit Amazon CloudWatch Events im Amazon CloudWatch Events-Benutzerhandbuch.

Ereignis mit verspäteter Datenbenachrichtigung

Das Ereignis für verspätete Datenbenachrichtigungen verwendet das folgende Format.

```
{
 "version": "0",
 "id": "7f51dfa7-ffef-97a5-c625-abddbac5eadd",
 "detail-type": "IoT Analytics Dataset Lifecycle Notification",
 "source": "aws.iotanalytics",
 "account": "123456789012",
 "time": "2020-05-14T02:38:46Z",
 "region": "us-east-2",
 "resources": ["arn:aws:iotanalytics:us-east-2:123456789012:dataset/demo_dataset"],
 "detail": {
  "event-detail-version": "1.0",
  "dataset-name": "demo_dataset",
  "late-data-rule-name": "demo_rule",
  "version-ids": ["78244852-8737-4650-aa4d-3071a01338fa"],
  "message": null
 }
}
```

Erstellen Sie eine CloudWatch Ereignisregel, um verspätete Datenbenachrichtigungen zu erhalten

Im folgenden Verfahren wird gezeigt, wie Sie eine Regel erstellen, die Benachrichtigungen zuAWS IoT Analytics verspäteten Daten an eine Amazon SQS SQS-Warteschlange sendet.

So erstellen Sie eine CloudWatch Ereignisregel

1. Melden Sie sich bei der CloudWatchAmazon-Konsole an.
2. Wählen Sie im Navigationsbereich unter Events (Ereignisse) die Option Rules (Regeln) aus.
3. Wählen Sie auf der Seite Regeln die Option Regel erstellen aus.
4. Wählen Sie unter Event Source die Option Event Pattern aus.
5. Führen Sie im Abschnitt Build event pattern to match events by service die folgenden Schritte aus:

   a. Wählen Sie als Dienstname IoT Analytics
   b. Wählen Sie als Ereignistyp die Option IoT Analytics Dataset Lifecycle Notification aus.

c. Wählen Sie Bestimmte Datensatznamen aus, und geben Sie dann den Namen des Zieldatensatzes ein.

6. Wählen Sie unter Ziele die Option Ziel hinzufügen*.
7. Wählen Sie SQS-Warteschlange, und gehen Sie dann wie folgt vor:

   • Wählen Sie für Queue* die Zielwarteschlange aus.

8. Wählen Sie Configure details.
9. Geben Sie auf der Seite Schritt 2: Regeldetails konfigurieren einen Namen und eine Beschreibung ein.
10. Wählen Sie Create rule (Regel erstellen).

Protokollierung von AWS IoT Analytics-API-Aufrufen mit AWS CloudTrail

AWS IoT Analyticsist in integriertAWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS -Service durchgeführten Aktionen bereitstelltAWS IoT Analytics. CloudTrail erfasst eine Teilmenge von API-Aufrufen fürAWS IoT Analytics als Ereignisse, einschließlich Aufrufen von derAWS IoT Analytics -Konsole und von Code-Aufrufen an dieAWS IoT Analytics -APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen in einem Amazon S3 S3-Bucket, einschließlich Ereignisse für aktivierenAWS IoT Analytics. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an gestellte AnfrageAWS IoT Analytics, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und weitere Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS IoT Analytics-Informationen in AWS CloudTrail

CloudTrail wird beim Erstellen IhresAWS -Kontos für Sie aktiviert. Wenn eine Aktivität in auftrittAWS IoT Analytics, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen Ereignissen desAWS -Service in Ereignisverlauf protokolliert. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS IoT Analytics, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von

-Protokolldateien in einem Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andereAWS -Services konfigurieren, um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

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

AWS IoT Analyticsunterstützt die Protokollierung der folgenden Aktionen als Ereignisse in CloudTrail -Protokolldateien:

- CancelPipelineReprocessing
- CreateChannel
- CreateDataset
- CreateDatasetContent
- CreateDatastore
- CreatePipeline
- DeleteChannel
- DeleteDataset
- DeleteDatasetContent
- DeleteDatastore
- DeletePipeline
- DescribeChannel
- DescribeDataset
- DescribeDatastore
- DescribeLoggingOptions
- DescribePipeline

- GetDatasetContent
- ListChannels
- ListDatasets
- ListDatastores
- ListPipelines
- PutLoggingOptions
- RunPipelineActivity
- SampleChannelData
- StartPipelineReprocessing
- UpdateChannel
- UpdateDataset
- UpdateDatastore
- UpdatePipeline

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 Anforderung mit Root- oder AWS Identity and Access Management-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS IoT Analytics-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail -Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`CreateChannel` Aktion demonstriert.


```
{
"eventVersion": "1.05",
"userIdentity": {
"type": "AssumedRole",
"principalId": "ABCDE12345FGHIJ67890B:AnalyticsChannelTestFunction",
"arn": "arn:aws:sts::123456789012:assumed-role/AnalyticsRole/
AnalyticsChannelTestFunction",
"accountId": "123456789012",
"accessKeyId": "ABCDE12345FGHIJ67890B",
"sessionContext": {
"attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-02-14T23:43:12Z"
},
"sessionIssuer": {
 "type": "Role",
 "principalId": "ABCDE12345FGHIJ67890B",
 "arn": "arn:aws:iam::123456789012:role/AnalyticsRole",
 "accountId": "123456789012",
 "userName": "AnalyticsRole"
}
}
},
"eventTime": "2018-02-14T23:55:14Z",
"eventSource": "iotanalytics.amazonaws.com",
"eventName": "CreateChannel",
"awsRegion": "us-east-1",
"sourceIPAddress": "198.162.1.0",
"userAgent": "aws-internal/3 exec-env/AWS_Lambda_java8",
"requestParameters": {
"channelName": "channel_channeltest"
},
"responseElements": {
"retentionPeriod": {
"unlimited": true
},
"channelName": "channel_channeltest",
"channelArn": "arn:aws:iotanalytics:us-east-1:123456789012:channel/channel_channeltest"
},
"requestID": "7f871429-11e2-11e8-9eee-0781b5c0ac59",
```

```
"eventID": "17885899-6977-41be-a6a0-74bb95a78294",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
```

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`CreateDataset` Aktion demonstriert.

```
{
"eventVersion": "1.05",
"userIdentity": {
"type": "AssumedRole",
"principalId": "ABCDE12345FGHIJ67890B:AnalyticsDatasetTestFunction",
"arn": "arn:aws:sts::123456789012:assumed-role/AnalyticsRole/
AnalyticsDatasetTestFunction",
"accountId": "123456789012",
"accessKeyId": "ABCDE12345FGHIJ67890B",
"sessionContext": {
"attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-02-14T23:41:36Z"
},
"sessionIssuer": {
 "type": "Role",
 "principalId": "ABCDE12345FGHIJ67890B",
 "arn": "arn:aws:iam::123456789012:role/AnalyticsRole",
 "accountId": "123456789012",
 "userName": "AnalyticsRole"
}
}
},
"eventTime": "2018-02-14T23:53:39Z",
"eventSource": "iotanalytics.amazonaws.com",
"eventName": "CreateDataset",
"awsRegion": "us-east-1",
"sourceIPAddress": "198.162.1.0",
"userAgent": "aws-internal/3 exec-env/AWS_Lambda_java8",
"requestParameters": {
"datasetName": "dataset_datasettest"
},
"responseElements": {
"datasetArn": "arn:aws:iotanalytics:us-east-1:123456789012:dataset/
dataset_datasettest",
```

```
"datasetName": "dataset_datasettest"
},
"requestID": "46ee8dd9-11e2-11e8-979a-6198b668c3f0",
"eventID": "5abe21f6-ee1a-48ef-afc5-c77211235303",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
```

Compliance-Validierung für AWS IoT Analytics

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

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten unter AWS Artifact .

Ihre Compliance-Verantwortung bei der Verwendung von 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 Unterstützung der Compliance bereit:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte für die Bereitstellung von Basisumgebungen in bereitgestellt AWS , die sich auf Sicherheit und Compliance konzentrieren.
- Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe AWS von HIPAA-berechtigte Anwendungen erstellen können.

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

- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort gelten.
- AWS Kunden-Compliance-Leitfäden – Verstehen Sie das Modell der geteilten Verantwortung anhand der Compliance. Die Leitfäden fassen die bewährten Methoden zur Sicherung zusammen AWS-Services und ordnen die Leitlinien den Sicherheitskontrollen in mehreren Frameworks zu

(einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Officer (PCI) und International Organization for Standardization (ISO)).

- Bewertung von Ressourcen mit Regeln im -AWS Config Entwicklerhandbuch – Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub – Dies AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen.

Ausfallsicherheit in AWS IoT Analytics

Die AWS globale -Infrastruktur ist um - AWS Regionen und Availability Zones herum aufgebaut. AWS -Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mit Availability Zones können Sie Anwendungen und Datenbanken entwerfen und betreiben, die automatisch ohne Unterbrechung zwischen Availability Zones ausfallen. 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 Analytics

Als verwalteter Service AWS IoT Analytics ist durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

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

AWS IoT Analytics-Kontingente

Der Allgemeine AWS-ReferenzLeitfaden enthält die StandardkontingenteAWS IoT Analytics für einAWS Konto. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eineAWS Region. Weitere Informationen finden Sie im Allgemeine AWS-ReferenzLeitfaden unter AWS IoT AnalyticsEndpunkte und Kontingente sowieAWS Servicekontingente.

Informationen zum Anfordern einer Erhöhung des Servicekontingents finden Sie in der Support Center-Konsole. Weitere Informationen finden Sie unter Beantragen einer Quota-Erhöhung im Service-Quotas-Benutzerhandbuch.

AWS IoT Analytics-Befehle

In diesem Thema erfahren Sie mehr über die API-Operationen fürAWS IoT Analytics, einschließlich Beispielanfragen, Antworten und Fehlern für die unterstützten Webdienstprotokolle.

AWS IoT Analytics-Aktionen

Sie könnenAWS IoT AnalyticsAPI-Befehle zum Sammeln, Verarbeiten, Speichern und Analysieren Ihrer IoT-Daten. Weitere Informationen finden Sie im .Aktionendie unterstützt werden.AWS IoT AnalyticsimAWS IoT Analytics-API-Referenzaus.

DieAWS IoT AnalyticsAbschnitteimAWS CLIBefehlsreferenzSchließen Sie die einAWS CLIBefehle, die Sie zur Verwaltung und Manipulation verwenden könnenAWS IoT Analyticsaus.

AWS IoT Analytics-Daten

Sie können dasAWS IoT AnalyticsDaten-API-Befehle zur Durchführung erweiterter Aktivitäten mitAWS IoT Analytics `channel`,`pipeline`,`datastore`, und`dataset`aus. Weitere Informationen finden Sie im .-Datentypendie unterstützt werden.AWS IoT AnalyticsDaten imAWS IoT Analytics-API-Referenzaus.

Fehlerbehebung für AWS IoT Analytics

Im folgenden Abschnitt finden Sie Informationen zur Behebung von Fehlern und zur Behebung von Problemen mitAWS IoT Analytics.

Themen

Woher weiß ich, dass meine Nachrichten ankommenAWS IoT Analytics?

Prüfen Sie, ob die Regel zum Injizieren von Daten in den Channel über die Regel-Engine richtig konfiguriert ist.

```
aws iot get-topic-rule --rule-name your-rule-name
```

Die Antwort sollte wie folgt aussehen.

```
{
    "ruleArn": "arn:aws:iot:us-west-2:your-account-id:rule/your-rule-name",
    "rule": {
        "awsIotSqlVersion": "2016-03-23",
        "sql": "SELECT * FROM 'iot/your-rule-name'",
        "ruleDisabled": false,
        "actions": [
            {
                "iotAnalytics": {
                    "channelArn":
 "arn:aws:iotanalytics:region:your_account_id:channel/your-channel-name"
                }
            }
        ],
        "ruleName": "your-rule-name"
    }
}
```

Stellen Sie sicher, dass die in der Regel verwendete Region und der Kanal-Name korrekt sind. Um sicherzustellen, dass Ihre Daten die Regel-Engine erreichen und die Regel korrekt ausgeführt wird, möchten Sie möglicherweise ein neues Ziel hinzufügen, um eingehende Nachrichten vorübergehend im Amazon S3 S3-Bucket zu speichern.

Warum verliert meine Pipeline Nachrichten? Wie lässt sich dies beheben?

- Eine Aktivität hat eine ungültige JSON-Eingabe erhalten:

  Alle Aktivitäten, außer Lambda-Aktivitäten, benötigen speziell eine gültige JSON-Zeichenfolge als Eingabe. Wenn der von einer Aktivität empfangene JSON ungültig ist, wird die Nachricht verworfen und gelangt nicht in den Datenspeicher. Stellen Sie sicher, dass Sie gültige JSON-Nachrichten in den Service einspeisen. Stellen Sie im Falle einer binären Eingabe sicher, dass die erste Aktivität in Ihrer Pipeline eine Lambda-Aktivität ist, die die Binärdaten in gültiges JSON konvertiert, bevor sie an die nächste Aktivität übergeben oder im Datenspeicher gespeichert werden. Weitere Informationen finden Sie unter Beispiel 2 für eine Lambda-Funktion.
- Eine Lambda-Funktion, die von einer Lambda-Aktivität aufgerufen wird, besitzt keine ausreichenden Berechtigungen:

Stellen Sie sicher, dass jede Lambda-Funktion in einer Lambda-Aktivität über die Berechtigung verfügt, vomAWS IoT Analytics Dienst aus aufgerufen zu werden. Sie können zur Erteilung der Erlaubnis folgendenAWS CLI Befehl verwenden.

```
aws lambda add-permission --function-name <name> --region <region> --statement-id
 <id> --principal iotanalytics.amazonaws.com --action lambda:InvokeFunction
```

- Ein Filter oder eine removeAttribute-Aktivität ist falsch definiert:

  Stellen Sie sicher, dass die Definitionen, falls vorhanden,`filter` oder die`removeAttribute` Aktivitäten korrekt sind. Wenn Sie eine Nachricht herausfiltern oder alle Attribute aus einer Nachricht entfernen, wird diese Nachricht nicht in den Datenspeicher aufgenommen.

Warum gibt es keine Daten in meinem Datenspeicher?

- Nach der Dateneinspeisung dauert es eine gewisse Zeit, bis die Daten zur Verfügung stehen:

  Es kann nach der Übernahme der Daten in einen Kanal einige Minuten dauern, bis diese Daten im Datenspeicher zur Verfügung stehen. Die Dauer variiert je nach Anzahl der Pipeline-Aktivitäten und der Definition von benutzerdefinierten Lambda-Aktivitäten in Ihrer Pipeline.
- Nachrichten werden in Ihrer Pipeline herausgefiltert:

  Stellen Sie sicher, dass Sie keine Nachrichten in der Pipeline löschen. (Siehe vorherige Frage und Antwort.)
- Ihre Datensatzabfrage ist falsch:

  Stellen Sie sicher, dass die Abfrage, die den Datensatz aus dem Datenspeicher generiert, korrekt ist. Löschen Sie alle unnötigen Filter aus der Abfrage, um sicherzustellen, dass Ihre Daten Ihren Datenspeicher erreichen.

Warum wird mein Datensatz nur angezeigt`__dt`?

- Diese Spalte wird vom Dienst automatisch hinzugefügt und enthält die ungefähre Zeit der Datenübernahme. Sie kann verwendet werden, um Ihre Abfragen zu optimieren. Wenn Ihr Datensatz nichts anderes enthält, lesen Sie die vorherige Frage und Antwort.

Wie kodiere ich ein Ereignis, das durch die Vervollständigung des Datensatzes gesteuert wird?

- Sie müssen die Abfrage auf der Grundlage des`describe-dataset` Befehls einrichten, um zu überprüfen, ob der Status des Datensatzes mit einem bestimmten Zeitstempel ERFOLGREICH ist.

Wie konfiguriere ich meine Notebook-Instanz für die Verwendung richtigAWS IoT Analytics?

Führen Sie diese Schritte aus, um sicherzustellen, dass die IAM-Rolle, mit der Sie die Notebook-Instance erstellen, über die erforderlichen Berechtigungen verfügt:

1. Gehen Sie zur SageMaker Konsole und erstellen Sie eine Notebook-Instanz.
2. Tragen Sie die Details ein und wählen Sie create a new Role (eine neue Rolle erstellen). Notieren Sie sich den ARN der Rolle.
3. Erstellen Sie die Notebook-Instance. Dadurch entsteht auch eine Rolle, die verwendet SageMaker werden kann.
4. Gehen Sie zur IAM-Konsole und ändern Sie die neu erstellte SageMaker Rolle. Wenn Sie diese Rolle öffnen, sollte sie über eine verwaltete Richtlinie verfügen.
5. Klicken Sie auf Inline-Richtlinie hinzufügen, wählen Sie IoTAnalytics als Dienst und wählen Sie unter Leseberechtigung die Option aus GetDatasetContent.
6. Überprüfen Sie die Richtlinie, fügen Sie einen Richtliniennamen hinzu und erstellen Sie sie dann. Die neu erstellte Rolle hat jetzt die Richtlinienberechtigung, aus der ein Datensatz gelesenAWS IoT Analytics werden kann.
7. Gehen Sie zurAWS IoT Analytics Konsole und erstellen Sie Notizbücher in der Notebook-Instanz.
8. Warten Sie, bis sich die Notebook-Instance im Zustand „In Service” (in Betrieb) befindet.
9. Wählen Sie create notebooks (Notebooks erstellen) und wählen Sie die von Ihnen erstellte Notebook-Instance aus. Dadurch wird ein Jupyter-Notizbuch mit der ausgewählten Vorlage erstellt, das auf Ihre Datensätze zugreifen kann.

Warum kann ich in einer Instanz keine Notizbücher erstellen?

- Stellen Sie sicher, dass Sie eine Notebook-Instance mit der richtigen IAM-Richtlinie erstellen. (Befolgen Sie die Schritten aus der vorherigen Frage.)
- Stellen Sie sicher, dass sich die Notebook-Instance im Zustand „In Service” (in Betrieb) befindet. Wenn Sie eine Instanz erstellen, beginnt sie im Status „Pending“. In der Regel dauert es etwa fünf Minuten, bis sie in den Zustand „In Service” (In Betrieb) wechselt. Wenn die Notebook-Instance nach etwa fünf Minuten in den Status „Fehlgeschlagen“ wechselt, überprüfen Sie die Berechtigungen erneut.

Warum sehe ich meine Datensätze nicht in Amazon QuickSight?

Amazon benötigt QuickSight möglicherweise eine Genehmigung, um den Inhalt IhresAWS IoT Analytics Datensatzes lesen zu können. Gehen Sie folgendermaßen vor, um die Erlaubnis zu erteilen.

1. Wählen Sie Ihren Kontonamen in der oberen rechten Ecke von Amazon QuickSight und wählen Sie Verwalten QuickSight.
2. Wählen Sie im linken Navigationsbereich Sicherheit und Berechtigungen aus. Vergewissern Sie sich unterQuickSight Zugriff aufAWS Dienste, dass Zugriff gewährt wurdeAWS IoT Analytics.
   a. Wenn SieAWS IoT Analytics keinen Zugriff haben, wählen Sie Hinzufügen oder Entfernen.
   b. Wählen Sie das Kästchen neben AWS IoT Analyticsund wählen Sie dann Aktualisieren aus. Dadurch erhält Amazon die QuickSight Erlaubnis, den Inhalt Ihres Datensatzes zu lesen.
3. Versuchen Sie erneut, Ihre Daten zu visualisieren.

Stellen Sie sicher, dass Sie für beideAWS IoT Analytics und Amazon dieselbeAWS Region auswählen QuickSight. Andernfalls könnten Probleme beim Zugriff auf dieAWS Ressourcen auftreten. Eine Liste der unterstützten Regionen finden Sie unter AWS IoT AnalyticsEndpunkte und Kontingente und QuickSight Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Warum sehe ich die Schaltfläche „Containerize“ auf meinem vorhandenen Jupyter-Notebook nicht?

- Dies wird durch ein fehlendesAWS IoT Analytics Containerization Plugin verursacht. Wenn Sie Ihre SageMaker Notebook-Instance vor dem 23. August 2018 erstellt haben, müssen Sie das Plugin manuell installieren, indem Sie den Anweisungen unter Ein Notizbuch in Containern folgen.
- Wenn Sie die Schaltfläche „Containerize“ nicht sehen, nachdem Sie die SageMaker Notebook-Instanz von derAWS IoT Analytics Konsole aus erstellt oder manuell installiert haben, wenden Sie sich an denAWS IoT Analytics technischen Support.

Warum schlägt die Installation meines Containerisierungs-Plugins fehl?

- Normalerweise schlägt die Plugin-Installation aufgrund fehlender Berechtigungen in der SageMaker Notebook-Instanz fehl. Prüfen Sie unter Berichtigungen, welche Berechtigungen für die Notebook-Instance erforderlich sind, und fügen Sie die erforderlichen Berechtigungen zur Notebook-Instance-Rolle hinzu. Wenn das Problem weiterhin besteht, erstellen Sie von derAWS IoT Analytics Konsole aus eine neue Notebook-Instanz.
- Sie können die folgende Meldung im Protokoll getrost ignorieren, wenn sie während der Installation des Plugins erscheint: „Um diese Erweiterung im Browser jedes Mal zu initialisieren, wenn das Notebook (oder eine andere App) geladen wird.“

Warum gibt mein Containerisierungs-Plugin einen Fehler aus?

- Die Containerisierung kann aus mehreren Gründen fehlschlagen und Fehlermeldungen erzeugen. Stellen Sie sicher, dass Sie über den richtigen Kernel verfügen, bevor Sie Ihr Notebook containerisieren. Containerisierte Kernel beginnen mit dem Präfix "Containerized".
- Da das Plugin ein Docker-Image in einem ECR-Repository erstellt und speichert, stellen Sie sicher, dass Ihre Notebook-Instance-Rolle über ausreichende Berechtigungen zum Lesen, Aufführen und Erstellen von ECR-Repositorys verfügt. Prüfen Sie unter Berichtigungen, welche Berechtigungen für die Notebook-Instance erforderlich sind, und fügen Sie die erforderlichen Berechtigungen zur Notebook-Instance-Rolle hinzu.

- Stellen Sie außerdem sicher, dass der Name des Repositorys die ECR-Anforderungen erfüllt. ECR-Repository-Namen müssen mit einem Buchstaben beginnen und dürfen nur Kleinbuchstaben, Ziffern, Bindestriche, Unterstriche und Schrägstriche enthalten.
- Wenn der Containerisierungsprozess mit dem folgenden Fehler fehlschlägt: „Diese Instanz hat nicht genügend freien Speicherplatz, um die Containerisierung auszuführen“, versuchen Sie, das Problem mit einer größeren Instanz zu lösen.
- Wenn Sie Verbindungsfehler oder einen Image-Erstellungsfehler sehen, versuchen Sie es erneut. Wenn das Problem weiterhin besteht, starten Sie die Instance neu und installieren Sie die neueste Plugin-Version.

Warum sehe ich meine Variablen während der Containerisierung nicht?

- DasAWS IoT Analytics Containerisierungs-Plugin erkennt automatisch alle Variablen in Ihrem Notebook, nachdem es das Notebook mit dem Kernel „Containerized“ ausgeführt hat. Verwenden Sie einen der containerisierten Kernel, um das Notebook auszuführen, und führen Sie dann die Containerisierung durch.

Welche Variablen kann ich meinem Container als Eingabe hinzufügen?

- Sie können alle Variablen, deren Wert Sie während der Laufzeit ändern möchten, als Eingabe zu Ihrem Container hinzufügen. Auf diese Weise können Sie denselben Container mit unterschiedlichen Parametern ausführen, die zum Zeitpunkt der Datensatzerstellung angegeben werden müssen. Das Jupyter-PluginAWS IoT Analytics zur Containerisierung vereinfacht diesen Prozess, indem es die Variablen im Notebook automatisch erkennt und sie im Rahmen des Containerisierungsprozesses verfügbar macht.

Wie stelle ich meine Container-Ausgabe als Eingabe für die nachfolgende Analyse ein?

- Eine spezieller S3-Speicherort, an dem die ausgeführten Artefakte gespeichert werden können, wird für jede Ausführung Ihres Container-Datasets erstellt Um auf diesen Ausgabespeicherort

zuzugreifen, erstellen Sie eine Variable mit dem Typ `outputFileUriValue` in Ihrem Container-Dataset. Der Wert dieser Variable sollte ein S3-Pfad sein, der für die Speicherung Ihrer zusätzlichen Ausgabedateien verwendet wird. Um in nachfolgenden Läufen auf diese gespeicherten Artefakte zuzugreifen, können Sie die`getDatasetContent` API verwenden und die entsprechende Ausgabedatei auswählen, die für den nachfolgenden Lauf erforderlich ist.

Warum schlägt mein Container-Dataset fehl?

- Stellen Sie sicher, dass Sie das richtige`executionRole` an das Container-Dataset übergeben. Die Vertrauenspolitik der`executionRole` muss`iotanalytics.amazonaws.com` sowohl als auch beinhalten`sagemaker.amazonaws.com`.
- Wenn Sie den Grund für den Fehler sehen`AlgorithmError`, versuchen Sie, Ihren Container-Code manuell zu debuggen. Diese Fehlermeldung wird angezeigt, wenn ein Fehler im Container-Code vorliegt oder die Ausführungsrolle nicht über die Berechtigung zum Ausführen des Containers verfügt. Wenn Sie mithilfe desAWS IoT Analytics Jupyter-Plug-ins containerisiert haben, erstellen Sie eine neue SageMaker Notebook-Instanz mit derselben Rolle wie die ExecutionRole des ContainerDataset und versuchen Sie, das Notebook manuell auszuführen. Wenn der Container außerhalb des Jupyter-Plugins erstellt wurde, versuchen Sie, den Code manuell auszuführen und die Berechtigung auf die executionRole (Ausführungsrolle) einzuschränken.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen an derAWS IoT AnalyticsBenutzerhandbuchnach dem 3. November 2020. Für weitere Informationen über Aktualisierungen dieser Dokumentation können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Start der Region	AWS IoT Analytics ist jetzt in der Region Asien-Pazifik (Mumbai) erhältlich.	18. August 2021
Abfragen mit`JOIN`	Mit diesem Update können Sie`JOIN`um einen abzufrage nAWS IoT Analyticsdatensatz.	27. Juli 2021
Integration in AWS IoT SiteWise	Sie können jetzt verwenden AWS IoT AnalyticsqueryAWS IoT SiteWisedata.	27. Juli 2021
Benutzerdefinierte Partitionen	AWS IoT Analyticsunterstüt zt jetzt generell die Partition ierung Ihrer Daten nach Nachrichtenattributen oder Attributen, die durch Pipeline-Aktivitäten hinzugefügt	14. Juni 2021
Wiederherstellen von Kanalnachrichten	Mit diesem Update können Sie die Kanaldaten in den angegebenen Amazon S3 S3-Objekten erneut verarbeiten.	15. Dezember 2020
Parquet-Schema	AWS IoT AnalyticsDatenspei cher unterstützen jetzt das Parquet-Dateiformat.	15. Dezember 2020
Überwachen mit CloudWatch Events	AWS IoT Analyticsveröffent licht automatisch ein Ereignis	15. Dezember 2020

	bei Amazon CloudWatc h Ereignisse, bei denen ein Laufzeitfehler während einesAWS Lambdaaktivität.	
Benachrichtigung bei später Daten	Sie können diese Funktion verwenden, um Benachric htigungen über Amazon zu erhalten CloudWatch Ereigniss e, wenn verspätete Daten eintreffen	9. November 2020
Start der Region	startenAWS IoT Analyticsin China (Peking).	4. November 2020

Frühere Updates

In der folgenden Tabelle werden wichtige Änderungen an der Datei beschriebenAWS IoT AnalyticsBenutzerhandbuchvor dem 4. November 2020.

Änderung	Beschreibung	Datum
Start der Region	startenAWS IoT Analytics in der Region Asien-Pazifik (Sydney).	16. Juli 2020
Aktualisierung	Die Dokumentation wurde neu organisiert.	7. Mai 2020

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.