User Guide

AWS IoT SiteWise

AWS IoT SiteWise: User Guide

Table of Contents

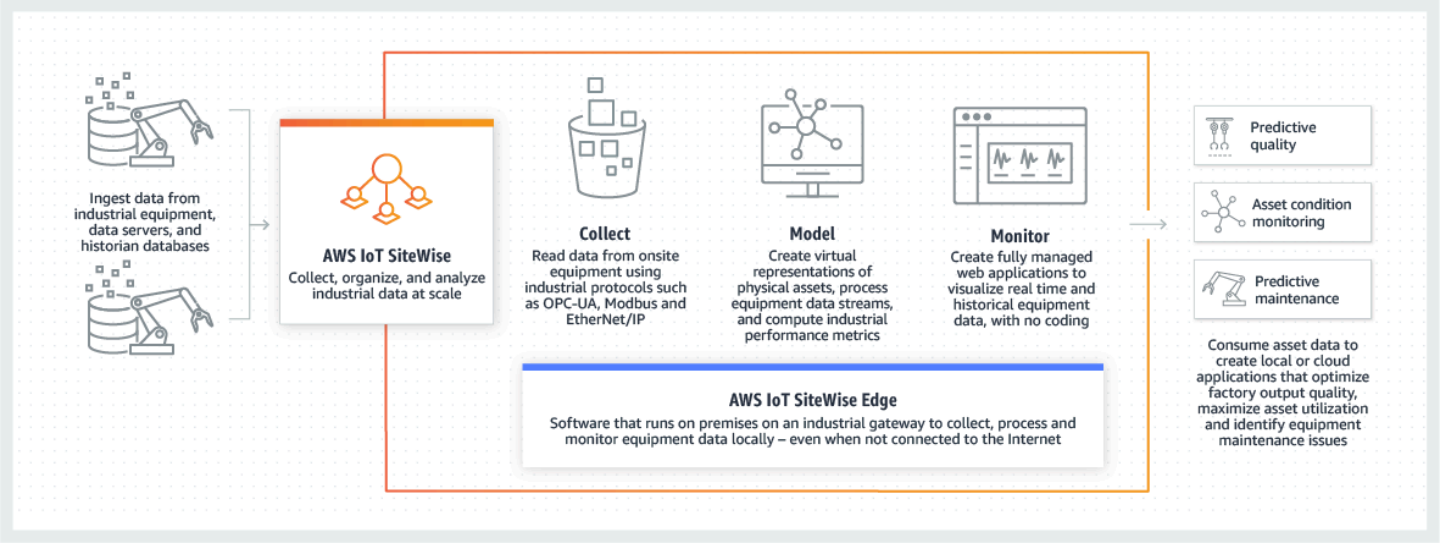
Was ist AWS IoT SiteWise?

AWS IoT SiteWise ist ein verwalteter Service, der es einfach macht, Daten von Industrieanlagen in großem Maßstab zu sammeln, zu speichern, zu organisieren und zu überwachen, damit Sie bessere, datengestützte Entscheidungen treffen können. Sie können ihn verwenden, AWS IoT SiteWise um Betriebsabläufe in allen Anlagen zu überwachen, schnell allgemeine industrielle Leistungskennzahlen zu berechnen und Anwendungen zu entwickeln, die Daten zu Industrieanlagen analysieren, um kostspielige Geräteprobleme zu vermeiden und Produktionslücken zu schließen.

AWS IoT SiteWise Monitor ermöglicht es Ihren operativen Benutzern, schnell Webanwendungen zu erstellen, mit denen Sie Ihre Industriedaten in Echtzeit anzeigen und analysieren können. Sie erhalten Einblicke in Ihre industriellen Operationen, indem Sie Metriken wie z. B. die mittlere störungsfreie Zeit und die Gesamtanlageneffektivität (Overall Equipment Effectiveness, OEE) konfigurieren und überwachen.

AWS IoT SiteWise Edge ist eine Komponente AWS IoT SiteWise , die die Erfassung, Speicherung und Verarbeitung von Daten auf lokalen Geräten ermöglicht. Dies ist nützlich, wenn Sie nur eingeschränkten Zugang zum Internet haben oder Ihre Daten privat halten müssen.

Das folgende Diagramm zeigt die grundlegende Architektur von AWS IoT SiteWise:



Themen

- Wie AWS IoT SiteWise funktioniert
- AWS IoT SiteWise Konzepte
- Anwendungsfälle für AWS IoT SiteWise

Wie AWS IoT SiteWise funktioniert

AWS IoT SiteWise bietet ein Framework zur Ressourcenmodellierung, mit dem Sie Darstellungen Ihrer industriellen Geräte, Prozesse und Anlagen erstellen können. Die Darstellungen Ihrer Geräte und Prozesse werden in als Anlagenmodelle bezeichnet AWS IoT SiteWise. Mit Anlagenmodellen definieren Sie, welche Rohdaten verwendet werden sollen, und wie diese zu nützlichen Kennzahlen verarbeitet werden. Erstellen und visualisieren Sie Anlagen und Modelle für Ihren industriellen Betrieb in der AWS IoT SiteWise Konsole. Sie können Anlagenmodelle auch so konfigurieren, dass sie Daten am Netzwerkrand oder in der AWS Cloud sammeln und verarbeiten.

Themen

Investieren Sie Industriedaten

Beginnen Sie mit der Nutzung, AWS IoT SiteWise indem Sie Industriedaten aufnehmen. Die Erfassung Ihrer Daten erfolgt auf eine von mehreren Arten:

- Direkte Erfassung von Servern vor Ort: Verwenden Sie Protokolle wie OPC-UA, um Daten direkt von Geräten vor Ort zu lesen. Stellen Sie die SiteWise Edge-Gateway-Software, kompatibel mit AWS IoT Greengrass V2, auf einer Vielzahl von Plattformen wie gängigen industriellen Gateways oder virtuellen Servern bereit. Sie können bis zu 100 OPC-UA-Server mit einem einzigen Gateway verbinden. AWS IoT SiteWise Weitere Informationen finden Sie unter SiteWise Anforderungen an das Edge-Gateway.

  Beachten Sie, dass Protokolle wie Modbus TCP und EtherNet/IP (EIP) durch unsere Partnerschaft mit im Rahmen von unterstützt werden. Domatica AWS IoT Greengrass V2
- Edge-Datenverarbeitung mit Paketen: Erweitern Sie Ihr SiteWise Edge-Gateway, indem Sie Pakete hinzufügen, um umfassende Edge-Funktionen zu ermöglichen. Mit SiteWise Edge, verfügbar auf AWS IoT Greengrass V2, wird die Datenverarbeitung direkt vor Ort ausgeführt, bevor sie

mithilfe eines AWS IoT Greengrass Streams sicher in die AWS Cloud übertragen wird. Weitere Informationen finden Sie unter Verwenden von Paketen.

- Adaptive Erfassung über Amazon S3 mit Massenoperationen: Wenn Sie mit einer großen Anzahl von Assets oder Asset-Modellen arbeiten, verwenden Sie Massenoperationen, um Ressourcen massenweise aus Amazon S3 S3-Buckets zu importieren und zu exportieren. Weitere Informationen finden Sie unter Massenoperationen mit Assets und Modellen.
- MQTT-Nachrichten mit AWS IoT Kernregeln: Verwenden Sie für Geräte, die mit AWS IoT Core verbunden sind und MQTT-Nachrichten senden, die AWS IoT Core-Regel-Engine, um diese Nachrichten weiterzuleiten. AWS IoT SiteWise Wenn Sie mit Core verbundene Geräte haben, die MQTT-Nachrichten senden, verwenden Sie die AWS IoT AWS IoT Core-Regel-Engine, um diese Nachrichten weiterzuleiten. AWS IoT SiteWise Weitere Informationen finden Sie unter Daten mithilfe AWS IoT Core von Regeln aufnehmen.
- Durch Ereignisse ausgelöste Datenaufnahme: Verwenden Sie AWS IoT Events Aktionen, um die SiteWise IoT-Aktion so zu konfigurieren, AWS IoT Events dass Daten gesendet werden, wenn Ereignisse eintreten. AWS IoT SiteWise Weitere Informationen finden Sie unter Daten werden aufgenommen von AWS IoT Events.
- AWS IoT SiteWise API: Ihre Anwendungen am Edge oder in der Cloud können Daten direkt an senden. AWS IoT SiteWise Weitere Informationen finden Sie unter Daten mithilfe der AWS IoT SiteWise API aufnehmen.

Modellieren Sie Ressourcen, um die gesammelten Daten zu kontextualisieren

Nach der Datenaufnahme können Sie anhand der Daten virtuelle Repräsentationen Ihrer Anlagen, Prozesse und Einrichtungen erstellen, indem Sie Modelle Ihrer physischen Abläufe erstellen. Ein Asset, das ein Gerät oder einen Prozess darstellt, überträgt Datenströme in die AWS Cloud. Vermögenswerte können auch logische Gerätegruppierungen bedeuten. Hierarchien werden durch die Zuordnung von Ressourcen gebildet, um komplexe Abläufe widerzuspiegeln. Diese Hierarchien ermöglichen es Anlagen, auf Daten aus zugehörigen untergeordneten Anlagen zuzugreifen. Vermögenswerte werden anhand von Anlagenmodellen erstellt. Asset-Modelle sind deklarative Strukturen, die Asset-Formate standardisieren. Verwenden Sie Komponenten von Assets für die Organisation und Wartbarkeit Ihrer Modelle wieder. Weitere Informationen finden Sie unter Modellieren von industriellen Komponenten.

Mit können Sie Ihre Ressourcen so konfigurieren AWS IoT SiteWise, dass die eingehenden Daten in kontextbezogene Metriken und Transformationen umgewandelt werden.

- Transformiert die Arbeit beim Empfang von Gerätedaten.
- Metriken werden in von Ihnen definierten Intervallen berechnet.

Metriken und Transformationen gelten sowohl für einzelne Anlagen als auch für mehrere Anlagen.AWS IoT SiteWise berechnet automatisch häufig verwendete statistische Aggregate wie Durchschnitt, Summe und Anzahl über verschiedene Zeiträume, die für Ihre Gerätedaten, Kennzahlen und Transformationen relevant sind.

Anlagen können synchronisiert werden mit. AWS IoT TwinMaker Weitere Informationen finden Sie unter Integration von AWS IoT SiteWise und AWS IoT TwinMaker.

Analysieren Sie mithilfe von Abfragen, Alarmen und Prognosen

Analysieren Sie das gesammelte Datum, AWS IoT SiteWise indem Sie Abfragen ausführen und Alarme einrichten. Sie können Amazon Lookout auch verwenden, um Anomalien innerhalb von Kennzahlen automatisch zu erkennen und deren Ursachen zu identifizieren.

- Richten Sie spezifische Alarme ein, um Ihr Team zu benachrichtigen, wenn Geräte oder Prozesse von der optimalen Leistung abweichen, und sorgen Sie so für eine schnelle Identifizierung und Lösung von Problemen. Weitere Informationen finden Sie unter Daten mit Alarmen überwachen.
- Verwenden Sie die AWS IoT SiteWise API-Operationen, um die aktuellen Werte, historischen Werte und Aggregate Ihrer Anlageneigenschaften über bestimmte Zeitintervalle abzufragen. Weitere Informationen finden Sie unter Daten abfragen von AWS IoT SiteWise.
- Verwenden Sie die Anomalieerkennung mit Amazon Lookout for Equipment, um Änderungen an Geräten oder Betriebsbedingungen zu identifizieren und zu visualisieren. Mit der Erkennung von Anomalien können Sie vorbeugende Wartungsmaßnahmen für Ihren Betrieb festlegen. Diese Integration ermöglicht es Kunden, Daten zwischen Amazon Lookout for Equipment AWS IoT SiteWise und Amazon Lookout for Equipment zu synchronisieren. Weitere Informationen finden Sie unter Erkennung von Geräteanomalien mit Amazon Lookout for Equipment.

Visualisieren Sie den Betrieb

Richten Sie SiteWise Monitor ein, um Webanwendungen für Ihre operativen Mitarbeiter zu erstellen. Die Webanwendungen helfen den Mitarbeitern, Ihre Abläufe zu visualisieren. Verwalten Sie verschiedene Zugriffsebenen für Ihre Mitarbeiter mithilfe von IAM Identity Center oder IAM. Konfigurieren Sie individuelle Logins und Berechtigungen für jeden Mitarbeiter, um bestimmte Teilbereiche eines gesamten Industriebetriebs einzusehen. AWS IoT SiteWise stellt diesen

Mitarbeitern einen Anwendungsleitfaden zur Verfügung, in dem sie lernen, wie sie Monitor verwenden können SiteWise .

Weitere Informationen zur Visualisierung Ihrer Betriebsabläufe finden Sie unterDaten überwachen mit AWS IoT SiteWise Monitor.

Daten speichern

Sie können Zeitreihenspeicher in Ihren industriellen Data Lake integrieren. AWS IoT SiteWise verfügt über drei Speicherebenen für industrielle Daten:

- Eine Hot-Storage-Tier, die für Echtzeitanwendungen optimiert ist.
- Eine warme Speicherebene, die für analytische Workloads optimiert ist.
- Ein vom Kunden verwaltetes Kühlspeicher-Tier, das Amazon S3 für Betriebsdatenanwendungen mit hoher Latenztoleranz verwendet.

AWS IoT SiteWise hilft Ihnen bei der Verwaltung der Speicherkosten, indem aktuelle Daten in der Hot-Storage-Tier aufbewahrt werden. Anschließend definieren Sie Richtlinien zur Datenspeicherung, um historische Daten in Speicher mit warmer oder kalter Speicherebene zu verschieben. Weitere Informationen finden Sie unter Verwaltung des Datenspeichers.

Sie können auch Asset-Metadaten importieren und exportieren. Weitere Informationen finden Sie unter Asset-Metadaten.

Integration in andere -Services

AWS IoT SiteWise lässt sich in mehrere AWS Dienste integrieren, um eine AWS IoT Komplettlösung in der AWS Cloud zu entwickeln. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten.

AWS IoT SiteWise Konzepte

Im Folgenden sind die Kernkonzepte von aufgeführt AWS IoT SiteWise:

Aggregate

> Aggregate sind grundlegende Metriken oder Messungen, die AWS IoT SiteWise automatisch für alle Zeitreihendaten berechnet werden. Weitere Informationen finden Sie unter Abfragen von Komponenteneigenschaften-Aggregaten.

Komponente

Wenn Sie Daten AWS IoT SiteWise aus Ihren Industrieanlagen eingeben oder aufnehmen, werden Ihre Geräte, Anlagen und Prozesse jeweils als Anlagen angezeigt. Jedem Asset sind Daten zugeordnet. Beispielsweise kann ein Gerät eine Seriennummer, einen Standort, eine Marke und ein Modell sowie ein Installationsdatum haben. Es kann auch Zeitreihenwerte für Verfügbarkeit, Leistung, Qualität, Temperatur, Druck und mehr enthalten. Gruppieren Sie Ressourcen in Hierarchien, sodass sie auf Daten zugreifen können, die in ihren untergeordneten Anlagen gespeichert sind. Weitere Informationen finden Sie unter Modellieren von industriellen Komponenten.

Komponentenhierarchie

Richten Sie Anlagenhierarchien ein, um logische Darstellungen Ihrer industriellen Abläufe zu erstellen. Definieren Sie dazu eine Hierarchie in einem Anlagenmodell und ordnen Sie anhand dieses Modells erstellte Anlagen der angegebenen Hierarchie zu. Bei Kennzahlen in übergeordneten Anlagen können Daten aus den Eigenschaften untergeordneter Anlagen kombiniert werden. Auf diese Weise können Sie Kennzahlen berechnen, die Einblicke in Ihren gesamten Betrieb oder einen bestimmten Teil davon bieten. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.

Komponentenmodell

Jede Anlage wird anhand eines Anlagenmodells erstellt. Vermögensmodelle sind Strukturen, die das Format Ihrer Vermögenswerte definieren und standardisieren. Sie sorgen für konsistente Informationen über mehrere Anlagen desselben Typs hinweg, sodass Sie Daten in Anlagen verwalten können, die Gruppen von Geräten repräsentieren. In jedem Komponentenmodell können Sie Attribute, Zeitreiheneingaben (Messungen), Zeitreihentransformationen (Transformationen), Zeitreihenaggregationen (Metriken) und Kompontenhierarchien definieren. Weitere Informationen finden Sie unter Modellieren von industriellen Komponenten.

Entscheiden Sie, wo die Eigenschaften Ihres Asset-Modells verarbeitet werden, indem Sie Ihr Asset-Modell für den Edge-Bereich konfigurieren. Verwenden Sie diese Funktion, um Asset-Daten auf Ihren lokalen Geräten zu verwalten und zu überwachen.

Komponenteneigenschaft

Bei Anlageneigenschaften handelt es sich um die Strukturen innerhalb jeder Anlage, die industrielle Daten enthalten. Jede Immobilie hat einen Datentyp und kann auch eine Einheit haben. Eine Eigenschaft kann ein Attribut, eine Messung, eine Transformation oder eine Metrik sein. Weitere Informationen finden Sie unter Definieren von Dateneigenschaften.

Konfigurieren Sie die Asset-Eigenschaften für die Berechnung am Edge. Weitere Informationen zur Verarbeitung von Daten am Netzwerkrand finden Sie unterthe section called “Aktivierung der Edge-Datenverarbeitung”.

Attribut

Bei Attributen handelt es sich um Eigenschaften eines Assets, die in der Regel konstant bleiben, z. B. der Gerätehersteller oder der Gerätestandort. Attribute können voreingestellte Werte haben. Jedes aus einem Asset-Modell erstellte Asset enthält die Standardwerte der in diesem Modell definierten Attribute. Weitere Informationen finden Sie unter Definition statischer Daten (Attribute).

Dashboard

Jedes Projekt enthält eine Reihe von Dashboards. Dashboards stellen eine Reihe von Visualisierungen für die Werte einer Gruppe von Komponenten bereit. Projekteigentümer erstellen die Dashboards und die darin enthaltenen Visualisierungen. Wenn ein Projekteigentümer bereit ist, die Gruppe von Dashboards freizugeben, kann der Eigentümer Betrachter zu dem Projekt einladen, wodurch diese Zugriff auf alle Dashboards in dem Projekt erhalten. Wenn Sie eine andere Gruppe von Betrachtern für verschiedene Dashboards wünschen, müssen Sie die Dashboards auf Projekte aufteilen. Wenn sich Zuschauer Dashboards ansehen, können sie den Zeitraum so anpassen, dass sie sich bestimmte Daten ansehen.

Datenstrom

Geben Sie Industriedaten ein oder nehmen Sie sie auf, AWS IoT SiteWise noch bevor Sie Anlagenmodelle und Anlagen erstellen. AWS IoT SiteWise generiert automatisch Datenströme, um Rohdatenströme von Ihren Geräten zu sammeln.

Alias für Datenströme

Datenstream-Aliase helfen Ihnen dabei, einen Datenstrom einfach zu identifizieren. Der Alias `server1-windfarm/3/turbine/7/temperature` gibt beispielsweise Temperaturwerte an, die von Turbine #7 im Windpark #3 stammen. Der Begriff `server1` ist der Name der Datenquelle, anhand dessen der OPC-UA-Server identifiziert werden kann. Er `server1-` ist ein Präfix, das allen von diesem OPC-UA-Server gemeldeten Datenströmen zugewiesen wird.

Zuordnung von Datenströmen

Nachdem Sie Asset-Modelle und Assets erstellt haben, verknüpfen Sie Datenstreams mit den in Ihren Assets definierten Asset-Eigenschaften, um Ihre Daten zu strukturieren. AWS IoT SiteWise kann dann Asset-Modelle und Assets verwenden, um eingehende Daten aus Ihren Datenströmen zu verarbeiten. Sie können Datenströme auch von Asset-Eigenschaften trennen. Weitere Informationen finden Sie unter Verwaltung von Datenströmen.

Formel

Jede Transformations - und Metrikeigenschaft enthält eine Formel, die beschreibt, wie die Eigenschaft Daten transformiert oder aggregiert. Diese Formeln beinhalten Eigenschaftseingaben, Operatoren und Funktionen, die von angeboten werden. AWS IoT SiteWise Weitere Informationen finden Sie unter Verwenden von Formelausdrücken.

Messung

Messungen sind Eigenschaften einer Anlage, die die rohen Sensorzeitreihendatenströme von einem Gerät oder einer Ausrüstung darstellen. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).

Metrik

Metriken sind Eigenschaften eines Assets, die aggregierte Zeitreihendaten darstellen. Jede Metrik wird von einem mathematischen Ausdruck (Formel) begleitet, der beschreibt, wie Datenpunkte aggregiert werden, und ein Zeitintervall für die Berechnung dieser Aggregation. Metriken generieren einen einzelnen Datenpunkt für jedes angegebene Zeitintervall. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

Pakete

SiteWise Edge-Gateways verwenden Pakete, um zu bestimmen, wie Daten gesammelt, verarbeitet und weitergeleitet werden. AWS IoT SiteWise Unterstützt derzeit das Datenerfassungspaket und das Datenverarbeitungspaket. Weitere Informationen zu den verfügbaren Paketen für Ihr SiteWise Edge-Gateway finden Sie unterthe section called “Verwenden von Paketen”.

Datenerfassungspaket

Verwenden Sie das Datenerfassungspaket, damit Ihr SiteWise Edge-Gateway Ihre Industriedaten sammeln und an das AWS Ziel Ihrer Wahl weiterleiten kann. Dieses Paket wird automatisch zu Ihrem SiteWise Edge-Gateway hinzugefügt und kann nicht entfernt werden.

Datenverarbeitungspaket

Verwenden Sie das Datenverarbeitungspaket, um Ihre Daten am Netzwerkrand zu verarbeiten und sie für die Verwendung in lokalen Anwendungen 30 Tage lang aufzubewahren.

Portal

Ein AWS IoT SiteWise Monitor Portal ist eine Webanwendung, mit der Sie Ihre AWS IoT SiteWise Daten visualisieren und gemeinsam nutzen können. Ein Portal verfügt über einen oder mehrere Administratoren und enthält keine oder mehrere Projekte.

Portaladministrator

Jedes SiteWise Monitor-Portal hat einen oder mehrere Portaladministratoren. Portaladministratoren verwenden das Portal, um Projekte zu erstellen, die Sammlungen von Komponenten und Dashboards enthalten. Der Portaladministrator weist dann jedem Projekt Komponenten und Eigentümer zu. Durch die Steuerung des Zugriffs auf das Projekt legen Portaladministratoren fest, welche Komponenten von Projekteigentümern und -betrachtern angezeigt werden können.

Projekt

Jedes SiteWise Monitor-Portal enthält eine Reihe von Projekten. Jedem Projekt ist eine Teilmenge Ihrer AWS IoT SiteWise -Komponenten zugeordnet. Projekteigentümer erstellen ein oder mehrere Dashboards, um eine konsistente Möglichkeit zum Anzeigen der mit diesen Komponenten verknüpften Daten bereitzustellen. Projekteigentümer können Betrachter zu dem Projekt einladen, damit diese die Komponenten und Dashboards in dem Projekt anzeigen können. Das Projekt ist die grundlegende Einheit für die gemeinsame Nutzung innerhalb von SiteWise Monitor. Projekteigentümer können Benutzer einladen, denen der AWS Administrator Zugriff auf das Portal gewährt hat. Ein Benutzer muss Zugriff auf ein Portal haben, bevor ein Projekt in diesem Portal für diesen Benutzer freigegeben werden kann.

Projekteigentümer

Jedes SiteWise Monitor-Projekt hat Besitzer. Projekteigentümer erstellen Visualisierungen in Form von Dashboards, um Betriebsdaten konsistent darzustellen. Wenn Dashboards zur Freigabe bereit sind, kann der Projekteigentümer Betrachter zu dem Projekt einladen. Projekteigentümer können dem Projekt auch andere Eigentümer zuweisen. Projekteigentümer können Schwellenwerte und Benachrichtigungseinstellungen für Alarme konfigurieren.

Projektbetrachter

Jedes SiteWise Monitor-Projekt hat Zuschauer. Projektbetrachter können eine Verbindung mit dem Portal herstellen, um die Dashboards anzuzeigen, die Projekteigentümer erstellt haben. In jedem Dashboard können Projektbetrachter den Zeitraum anpassen, um die Betriebsdaten besser zu verstehen. Projektbetrachter können nur Dashboards in den Projekten anzeigen, auf

die sie Zugriff haben. Projektbeobachter können Alarme bestätigen und die Schlummerfunktion aktivieren.

Eigenschaftsalias

Sie haben die Möglichkeit, Aliase für Asset-Eigenschaften zu erstellen, wie z. B. einen OPC-UA-Server-Datenstream-Pfad (z. B. /company/windfarm/3/turbine/7/temperature), um die Identifizierung einer Anlageneigenschaft beim Erfassen oder Abrufen von Anlagendaten zu vereinfachen. Wenn Sie ein SiteWise Edge-Gateway verwenden, um Daten von Servern aufzunehmen, müssen Ihre Eigenschafts-Aliase mit den Pfaden Ihrer Rohdatenströme übereinstimmen. Weitere Informationen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Eigenschaftsbenachrichtigung

Wenn Sie Eigenschaftsbenachrichtigungen für eine Vermögenseigenschaft aktivieren, AWS IoT SiteWise veröffentlicht AWS IoT Core jedes Mal, wenn diese Eigenschaft einen neuen Wert erhält, eine MQTT-Nachricht. Die Nutzdaten der Nachricht enthalten Details zur Aktualisierung dieses Eigenschaftswerts. Verwenden Sie Benachrichtigungen über Immobilienwerte, um Lösungen zu entwickeln, die Ihre Industriedaten AWS IoT SiteWise mit anderen AWS Diensten verbinden. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten.

SiteWise Edge-Gateway

Ein SiteWise Edge-Gateway befindet sich auf dem Gelände des Kunden, um Daten zu sammeln, zu verarbeiten und weiterzuleiten. Ein SiteWise Edge-Gateway stellt über das OPC-UA-Protokoll eine Verbindung zu Ihren industriellen Datenquellen her, um Daten zu sammeln, zu verarbeiten und an die AWS Cloud zu senden. SiteWise Edge-Gateways können auch eine Verbindung zu Partnerdatenquellen herstellen. SiteWise Edge-Gateways verwenden Pakete für die Datenerfassung, Edge-Verarbeitung und mehr. Weitere Informationen zu verfügbaren Paketen finden Sie unterthe section called “Verwenden von Paketen”.

Sie haben die Flexibilität, ein SiteWise Edge-Gateway auf jedem Gerät oder jeder Plattform zu erstellen, die ausgeführt werden kann AWS IoT Greengrass. Weitere Informationen finden Sie unter Verwenden von SiteWise Edge-Gateways.

Transformation

Transformationen sind Eigenschaften eines Assets, die transformierte Zeitreihendaten darstellen. Jede Transformation wird von einem mathematischen Ausdruck (Formel) begleitet, der festlegt, wie Datenpunkte von einer Form in eine andere konvertiert werden. Die transformierten

Datenpunkte stehen in einer one-to-one Beziehung zu den Eingabedatenpunkten. Weitere Informationen finden Sie unter Daten transformieren (transformiert).

Visualisierung

In jedem Dashboard entscheiden die Projekteigentümer, wie die Eigenschaften und Alarme der mit dem Projekt verknüpften Objekte angezeigt werden sollen. Die Verfügbarkeit kann als Liniendiagramm dargestellt werden, während andere Werte als Balkendiagramme oder Leistungskennzahlen (KPIs) angezeigt werden können. Alarme lassen sich am besten als Statusraster und Statuszeitleisten anzeigen. Projekteigentümer passen jede Visualisierung an, um die Daten für diese Komponente optimal darzustellen.

Anwendungsfälle für AWS IoT SiteWise

AWS IoT SiteWise wird in einer Vielzahl von Branchen für viele industrielle Datenerfassungs- und Analyseanwendungen eingesetzt.

Sammeln Sie konsistent Daten aus all Ihren Quellen, um Probleme schnell zu lösen. AWS IoT SiteWise bietet Fernüberwachung, um die Daten direkt vor Ort oder aus mehreren Quellen in vielen Einrichtungen zu sammeln. AWS IoT SiteWise bietet die notwendige Flexibilität für industrielle IoT-Datenlösungen.

Fertigung

AWS IoT SiteWise kann den Prozess der Erfassung und Nutzung von Daten aus Ihren Geräten vereinfachen, um Ineffizienzen zu lokalisieren und zu minimieren und so den industriellen Betrieb zu verbessern. AWS IoT SiteWise hilft Ihnen bei der Erfassung von Daten aus Fertigungslinien und Anlagen. Mit AWS IoT SiteWise können Sie die Daten in die AWS Cloud übertragen und Leistungskennzahlen für Ihre spezifischen Geräte und Prozesse erstellen. Sie können die erstellten Kennzahlen verwenden, um die Gesamteffektivität Ihrer Abläufe zu verstehen und Innovations- und Verbesserungsmöglichkeiten zu identifizieren. Sie können sich auch Ihren Herstellungsprozess ansehen und Geräte- und Prozessmängel, Produktionslücken oder Produktfehler identifizieren.

Nahrungsmittel und Getränke

Anlagen in der Nahrungsmittel- und Getränkeindustrie verarbeiten eine große Bandbreite von Lebensmitteln. So mahlen sie zum Beispiel Getreide zu Mehl, schneiden und verpacken Fleisch und erstellen, kochen und gefrieren für die Erwärmung in Mikrowellen geeignete Mahlzeiten. Lebensmittelverarbeitungsanlagen erstrecken sich häufig über mehrere Standorte, wobei sich die

Anlagen- und Gerätebediener an einem zentralen Standort befinden, um Prozesse und Ausrüstung zu überwachen. Kühlaggregate bewerten beispielsweise die Handhabung und das Verfallsdatum der Zutaten. Sie überwachen das Abfallaufkommen in allen Anlagen, um die betriebliche Effizienz sicherzustellen. Mit AWS IoT SiteWise können Sie Sensordatenströme von mehreren Standorten nach Produktionslinie und Anlage gruppieren, sodass Ihre Verfahrenstechniker die Anlagen besser verstehen und Verbesserungen vornehmen können.

Energie und Versorgung

Mit AWS IoT SiteWise können Sie Geräteprobleme einfacher und effizienter lösen. Sie können die Leistung Ihrer Anlagen aus der Ferne und in Echtzeit überwachen. Greifen Sie von überall auf historische Gerätedaten zu, um potenzielle Probleme zu lokalisieren, präzise Ressourcen bereitzustellen und Probleme schneller zu verhindern und zu beheben.

Erste Schritte mit AWS IoT SiteWise

Mit AWS IoT SiteWise können Sie Ihre Daten sammeln, organisieren, analysieren und visualisieren.

AWS IoT SiteWise bietet eine Demo, mit der Sie den Service erkunden können, ohne eine echte Datenquelle konfigurieren zu müssen. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo verwenden.

Sie können die folgenden Tutorials absolvieren, um sich mit bestimmten Funktionen von vertraut zu machen AWS IoT SiteWise:

- Daten von AWS IoT Dingen aufnehmen
- Visualisierung und gemeinsame Nutzung von Windparkdaten in Monitor SiteWise
- Veröffentlichung von Eigenschaftswertaktualisierungen in Amazon DynamoDB

In den folgenden Themen erfahren Sie mehr über AWS IoT SiteWise:

- Daten aufnehmen zu AWS IoT SiteWise
- Modellieren von industriellen Komponenten
- Aktivierung der Edge-Datenverarbeitung
- Daten überwachen mit AWS IoT SiteWise Monitor
- Daten abfragen von AWS IoT SiteWise
- Interaktion mit anderen AWS Diensten

Themen

Voraussetzungen

Sie müssen eine haben AWS-Konto , mit der Sie beginnen können AWS IoT SiteWise. Falls Sie noch keines haben, beachten Sie die Informationen unter Einrichtung eines AWS-Konto.

Verwenden Sie eine Region, in AWS IoT SiteWise der verfügbar ist. Weitere Informationen finden Sie unter AWS IoT SiteWise Endpunkte und -Kontingente. Sie können die Regionsauswahl in verwenden AWS Management Console , um zu einer dieser Regionen zu wechseln.

Einrichtung eines AWS-Konto

Themen

- Melde dich an für eine AWS-Konto
- Erstellen Sie einen Benutzer mit Administratorzugriff

Melde dich an für eine AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/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 eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

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

Erstellen Sie einen Benutzer mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

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

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

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

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

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

Melden Sie sich als Benutzer mit Administratorzugriff an

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

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

Weisen Sie weiteren Benutzern Zugriff zu

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

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

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

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Die AWS IoT SiteWise Demo verwenden

Mit der AWS IoT SiteWise Demo können Sie ganz einfach die Umgebung erkunden AWS IoT SiteWise . AWS IoT SiteWise stellt die Demo als AWS CloudFormation Vorlage bereit, die Sie einsetzen können, um Asset-Modelle, Assets und ein SiteWise Monitor-Portal zu erstellen und Beispieldaten für bis zu einer Woche zu generieren.

> **Important**
>
> Sobald Sie die Demo erstellt haben, werden Ihnen die Ressourcen in Rechnung gestellt, die durch diese Demo erstellt und verbraucht werden.

Themen

Die AWS IoT SiteWise Demo erstellen

Sie können die AWS IoT SiteWise Demo von der AWS IoT SiteWise Konsole aus erstellen.

> **Note**
>
> Die Demo erstellt Lambda-Funktionen, eine CloudWatch Event-Regel und die für die Demo erforderlichen AWS Identity and Access Management (IAM-) Rollen. Möglicherweise sehen Sie diese Ressourcen in Ihrem. AWS-Konto Wir empfehlen Ihnen, diese Ressourcen

beizubehalten, bis Sie mit der Demo fertig sind. Wenn Sie die Ressourcen löschen, funktioniert die Demo möglicherweise nicht mehr richtig.

Um die Demo in der AWS IoT SiteWise Konsole zu erstellen

1. Navigieren Sie zur AWS IoT SiteWise Konsole und suchen Sie die SiteWise Demo in der oberen rechten Ecke der Seite.
2. (Optional) Ändern Sie unter SiteWise Demo das Feld Tage, bis die Demo-Assets aufbewahrt werden sollen, um anzugeben, wie viele Tage die Demo aufbewahrt werden soll, bevor sie gelöscht wird.
3. (Optional) Gehen Sie wie folgt vor, um ein SiteWise Monitor-Portal zur Überwachung von Beispieldaten zu erstellen.

   > **Note**
   >
   > Die SiteWise Monitor-Ressourcen, die in dieser Demo erstellt und verbraucht werden, werden Ihnen in Rechnung gestellt. Weitere Informationen finden Sie in der AWS IoT SiteWise Preisübersicht unter SiteWise Monitor.

   a. Wählen Sie Ressourcen überwachen.
   b. Wählen Sie „Erlaubnis“.
   c. Wählen Sie eine bestehende IAM-Rolle aus, die Ihren föderierten IAM-Benutzern Zugriff auf das Portal gewährt.

      > **Important**
      >
      > Ihre IAM-Rolle muss über die folgenden Berechtigungen verfügen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:Describe*",
                "iotsitewise:List*",
```

```
                "iotsitewise:Get*",
                "cloudformation:DescribeStacks",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "sso:DescribeRegisteredRegions",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zur Arbeit mit SiteWise Monitor finden Sie unter Was ist AWS IoT SiteWise Monitor? im AWS IoT SiteWise Monitor Anwendungshandbuch.

4. Wählen Sie Create demo (Demo erstellen) aus.

   Das Erstellen der Demo dauert ca. 3 Minuten. Wenn die Demo nicht erstellt werden kann, verfügt Ihr Konto möglicherweise nicht über ausreichende Berechtigungen. Wechseln Sie zu einem Konto mit Administratorberechtigungen oder führen Sie die folgenden Schritte aus, um die Demo zu löschen, und versuchen Sie es erneut:

   a. Wählen Sie Demo löschen aus.

      Das Löschen der Demo dauert etwa 15 Minuten.

   b. Wenn die Demo nicht gelöscht wird, öffnen Sie die AWS CloudFormation Konsole, wählen Sie den Stack mit dem Namen IoT SiteWiseDemoAssets und wählen Sie in der oberen rechten Ecke Löschen aus.

   c. Wenn die Demo erneut nicht gelöscht werden kann, folgen Sie den Schritten in der AWS CloudFormation Konsole, um die Ressourcen zu überspringen, die nicht gelöscht werden konnten, und versuchen Sie es erneut.

5. Nachdem die Demo erfolgreich erstellt wurde, können Sie die Demo-Assets und -Daten in der AWS IoT SiteWise Konsole erkunden.

Die AWS IoT SiteWise Demo löschen

Die AWS IoT SiteWise Demo löscht sich nach einer Woche oder nach der Anzahl der Tage, die Sie ausgewählt haben, wenn Sie den Demo-Stack von der AWS CloudFormation Konsole aus erstellt haben. Sie können die Demo vorher löschen, wenn Sie mit den Demoressourcen fertig sind. Sie können die Demo auch löschen, wenn die Demo nicht erstellt werden kann. Gehen Sie wie folgt vor, um die Demo manuell zu löschen.

Um die Demo zu löschen AWS IoT SiteWise

1. Navigieren Sie zur AWS CloudFormation -Konsole.
2. Wählen Sie IoTSiteWiseDemoAssets aus der Liste der Stacks aus.
3. Wählen Sie Löschen aus.

   Wenn Sie den Stack löschen, werden alle für die Demo erstellten Ressourcen gelöscht.
4. Wählen Sie im Bestätigungsdialogfeld Stack löschen aus.

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

AWS IoT SiteWise Anleitungen

Willkommen auf der AWS IoT SiteWise Tutorial-Seite. Diese wachsende Sammlung von Tutorials vermittelt Ihnen das Wissen und die Fähigkeiten, die Sie benötigen, um sich mit den Feinheiten von vertraut zu machen. AWS IoT SiteWise Diese Tutorials bieten eine Vielzahl grundlegender Themen, die auf Ihre Bedürfnisse zugeschnitten sind. Während Sie sich mit den Tutorials befassen, erhalten Sie wertvolle Einblicke in verschiedene Aspekte von. AWS IoT SiteWise

Jedes Tutorial verwendet ein bestimmtes Ausrüstungsbeispiel. Diese Tutorials sind für Testumgebungen vorgesehen und verwenden fiktive Firmennamen, Modelle, Vermögenswerte, Eigenschaften usw. In den Tutorials finden Sie allgemeine Anleitungen. Die Tutorials sind nicht für den direkten Einsatz in einer Produktionsumgebung vorgesehen, es sei denn, sie werden sorgfältig geprüft und an die individuellen Anforderungen Ihres Unternehmens angepasst.

Themen

Berechnung der Gesamtanlageneffektivität in AWS IoT SiteWise

Dieses Tutorial enthält ein Beispiel dafür, wie die Gesamtanlageneffektivität (OEE) für einen Herstellungsprozess berechnet wird. Folglich können Ihre OEE-Berechnungen oder -Formeln von den hier dargestellten abweichen. Im Allgemeinen ist OEE definiert als `Availability * Quality * Performance`. Weitere Informationen über die Berechnung der OEE finden Sie unter Overall equipment effectiveness auf Wikipedia.

Voraussetzungen

Um dieses Tutorial abzuschließen, müssen Sie die Datenerfassung für ein Gerät mit den folgenden drei Daten-Streams konfigurieren:

- `Equipment_State`— Ein numerischer Code, der den Zustand der Maschine darstellt, z. B. Leerlauf, Störung, geplanter Stopp oder Normalbetrieb.

- `Good_Count`— Ein Datenstrom, bei dem jeder Datenpunkt die Anzahl der erfolgreichen Operationen seit dem letzten Datenpunkt enthält.
- `Bad_Count`— Ein Datenstrom, bei dem jeder Datenpunkt die Anzahl der erfolglosen Operationen seit dem letzten Datenpunkt enthält.

Informationen zum Konfigurieren der Datenerfassung finden Sie im Abschnitt Daten aufnehmen zu AWS IoT SiteWise. Wenn keine industriellen Operationen verfügbar sind, können Sie ein Skript schreiben, das Beispieldaten über die AWS IoT SiteWise -API generiert und hochlädt.

Berechnen der OEE

In diesem Tutorial erstellen Sie ein Komponentenmodell, das die OEE aus drei Dateneingabe-Streams berechnet: `Equipment_State`, `Good_Count`, und `Bad_Count`. Stellen Sie sich in diesem Beispiel eine allgemeine Verpackungsmaschine vor, beispielsweise eine Maschine, die zum Verpacken von Zucker, Kartoffelchips oder Farbe verwendet wird. Erstellen Sie in der AWS IoT SiteWise Konsole ein AWS IoT SiteWise Asset-Modell mit den folgenden Messungen, Transformationen und Metriken. Anschließend können Sie ein Asset erstellen, das die Verpackungsmaschine darstellt, und beobachten, wie die Gesamtanlageneffektivität AWS IoT SiteWise berechnet wird.

Definieren Sie die folgenden Messungen, um die Rohdaten-Streams von der Verpackungsmaschine darzustellen.

Messungen

- `Equipment_State`— Ein Datenstrom (oder eine Messung), der den aktuellen Zustand der Verpackungsmaschine in numerischen Codes wiedergibt:
  - `1024`— Die Maschine befindet sich im Leerlauf.
  - `1020`— Ein Fehler, z. B. ein Fehler oder eine Verzögerung.
  - `1000`— Ein geplanter Stopp.
  - `1111`— Ein normaler Betrieb.
- `Good_Count`— Ein Datenstrom, bei dem jeder Datenpunkt die Anzahl der erfolgreichen Operationen seit dem letzten Datenpunkt enthält.
- `Bad_Count`— Ein Datenstrom, bei dem jeder Datenpunkt die Anzahl der erfolglosen Operationen seit dem letzten Datenpunkt enthält.

Legen Sie mithilfe des `Equipment_State`-Messdaten-Streams und der darin enthaltenen Codes die folgenden Transformationen (oder abgeleiteten Messungen) fest. Transformationen haben eine one-to-one Beziehung zu Rohmessungen.

Transformationen

- `Idle = eq(Equipment_State, 1024)`— Ein transformierter Datenstrom, der den Ruhezustand der Maschine enthält.
- `Fault = eq(Equipment_State, 1020)`— Ein transformierter Datenstrom, der den Fehlerstatus der Maschine enthält.
- `Stop = eq(Equipment_State, 1000)`— Ein transformierter Datenstrom, der den geplanten Stoppstatus der Maschine enthält.
- `Running = eq(Equipment_State, 1111)`— Ein transformierter Datenstrom, der den normalen Betriebszustand der Maschine enthält.

Definieren Sie anhand der Rohmessungen und der transformierten Messungen die folgenden Metriken, die Maschinendaten über bestimmte Zeitintervalle aggregieren. Wählen Sie für jede Metrik dasselbe Zeitintervall aus, wenn Sie die Metriken in diesem Abschnitt definieren.

Metriken

- `Successes = sum(Good_Count)`— Die Anzahl der erfolgreich befüllten Pakete im angegebenen Zeitintervall.
- `Failures = sum(Bad_Count)`— Die Anzahl der Pakete, die im angegebenen Zeitintervall nicht erfolgreich gefüllt wurden.
- `Idle_Time = statetime(Idle)`— Die gesamte Leerlaufzeit der Maschine (in Sekunden) pro festgelegtem Zeitintervall.
- `Fault_Time = statetime(Fault)`— Die Gesamtfehlerzeit der Maschine (in Sekunden) pro festgelegtem Zeitintervall.
- `Stop_Time = statetime(Stop)`— Die gesamte geplante Stoppzeit der Maschine (in Sekunden) pro festgelegtem Zeitintervall.
- `Run_Time = statetime(Running)`— Die Gesamtbetriebszeit (in Sekunden) der Maschine ohne Probleme pro festgelegtem Zeitintervall.
- `Down_Time = Idle_Time + Fault_Time + Stop_Time`— Die gesamte Ausfallzeit der Maschine (in Sekunden) über das angegebene Zeitintervall, berechnet als Summe der Maschinenzustände außer`Run_Time`.

- `Availability = Run_Time / (Run_Time + Down_Time)`— Die Betriebszeit der Maschine oder der Prozentsatz der geplanten Zeit, während der die Maschine während des angegebenen Zeitintervalls betriebsbereit ist.
- `Quality = Successes / (Successes + Failures)`— Der Prozentsatz der erfolgreich abgefüllten Pakete der Maschine in den angegebenen Zeitintervallen.
- `Performance = ((Successes + Failures) / Run_Time) / Ideal_Run_Rate`— Die Leistung der Maschine im angegebenen Zeitintervall als Prozentsatz der für Ihren Prozess idealen Durchlaufgeschwindigkeit (in Sekunden).

  Ihre `Ideal_Run_Rate` beläuft sich beispielsweise auf 60 Pakete pro Minute (1 Paket pro Sekunde). Wenn Ihr Wert pro Minute oder pro Stunde angegeben `Ideal_Run_Rate` wird, müssen Sie ihn durch den entsprechenden Umrechnungsfaktor für Einheiten dividieren, da er in Sekunden angegeben `Run_Time` ist.
- `OEE = Availability * Quality * Performance`— Die Gesamtanlageneffektivität der Maschine über das angegebene Zeitintervall. Diese Formel berechnet OEE als Bruchteil von 1.

Daten von AWS IoT Dingen aufnehmen

In diesem Tutorial erfahren Sie, wie Sie mithilfe AWS IoT SiteWise von AWS IoT Geräteschatten Daten aus einer Flotte von Geräten aufnehmen. Geräteschatten sind JSON-Objekte, die aktuelle Statusinformationen für ein AWS IoT Gerät speichern. Weitere Informationen finden Sie unter Device Shadow Service im AWS IoT Entwicklerhandbuch.

Nachdem Sie dieses Tutorial abgeschlossen haben, können Sie einen Vorgang einrichten, der auf AWS IoT Dingen AWS IoT SiteWise basiert. Indem Sie AWS IoT Dinge verwenden, können Sie Ihren Betrieb in andere nützliche Funktionen von integrieren AWS IoT. Sie können beispielsweise AWS IoT Funktionen für die folgenden Aufgaben konfigurieren:

- Konfigurieren Sie zusätzliche Regeln, um Daten zu AWS IoT EventsAmazon DynamoDB und anderen zu streamen. AWS-Services Weitere Informationen finden Sie unter Regeln im AWS IoT Entwicklerhandbuch.
- Indexieren, durchsuchen und aggregieren Sie Ihre Gerätedaten mit dem AWS IoT Fleet Indexing Service. Weitere Informationen finden Sie unter Fleet Indexing Service im AWS IoT Entwicklerhandbuch.
- Prüfen und sichern Sie Ihre Geräte mit AWS IoT Device Defender. Weitere Informationen finden Sie unter AWS IoT Device Defender im AWS IoT -Entwicklerhandbuch.

In diesem Tutorial erfahren Sie, wie Sie Daten aus den Geräteschatten AWS IoT von Dingen in Assets aufnehmen. AWS IoT SiteWise Dazu erstellen Sie ein oder mehrere AWS IoT Dinge und führen ein Skript aus, das den Geräteshadow jedes Dings mit Daten zur CPU- und Speichernutzung aktualisiert. In diesem Tutorial verwenden Sie CPU- und Speichernutzungsdaten, um realistische Sensordaten zu imitieren. Anschließend erstellen Sie eine Regel mit einer AWS IoT SiteWise Aktion, die diese Daten bei AWS IoT SiteWise jeder Aktualisierung des Geräteshadows an ein Asset sendet. Weitere Informationen finden Sie unter Daten mithilfe AWS IoT Core von Regeln aufnehmen.

Themen

Voraussetzungen

Zum Durcharbeiten dieses Tutorials ist Folgendes erforderlich:

- Ein AWS-Konto. Falls Sie noch keines haben, beachten Sie die Informationen unter Einrichtung eines AWS-Konto.
- Ein Entwicklungscomputer, auf demWindows, macOSLinux, oder ausgeführt wird, Unix um auf den zuzugreifen AWS Management Console. Weitere Informationen finden Sie unter Erste Schritte mit AWS Management Console.
- Ein AWS Identity and Access Management (IAM-) Benutzer mit Administratorrechten.
- Python3 ist auf Ihrem Entwicklungscomputer oder auf dem Gerät installiert, das Sie als Objekt registrieren möchten AWS IoT .

Schritt 1: Eine AWS IoT Richtlinie erstellen

Erstellen Sie in diesem Verfahren eine AWS IoT Richtlinie, die es Ihren AWS IoT Dingen ermöglicht, auf die in diesem Tutorial verwendeten Ressourcen zuzugreifen.

Um eine AWS IoT Richtlinie zu erstellen

1. Melden Sie sich an der AWS Management Console an.
2. Sehen Sie sich die AWS Regionen an, in denen AWS IoT SiteWise es unterstützt wird. Wechseln Sie ggf. zu einer dieser unterstützten Regionen.
3. Navigieren Sie zur AWS IoT -Konsole. Wenn eine Schaltfläche „Gerät Connect“ angezeigt wird, wählen Sie sie aus.
4. Wählen Sie im linken Navigationsbereich Sicherheit und dann Richtlinien aus.
5. Wählen Sie Erstellen.
6. Geben Sie einen Namen für die AWS IoT Richtlinie ein (z. B.**`SiteWiseTutorialDevicePolicy`**).
7. Wählen Sie unter Richtliniendokument die Option JSON aus, um die folgende Richtlinie im JSON-Format einzugeben. Ersetzen Sie *`region`* und *`account-id`* durch Ihre Region und Ihre Konto-ID, z. B. **`us-east-1`** und **`123456789012`**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "arn:aws:iot:region:account-id:client/SiteWiseTutorialDevice*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Publish",
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get"
      ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/accepted",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/accepted",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get/accepted",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/rejected",
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": [
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/get/accepted",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/update/rejected",
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/delete/rejected"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow"
      ],
      "Resource": "arn:aws:iot:region:account-id:thing/SiteWiseTutorialDevice*"
    }
  ]
```

```
}
```

Diese Richtlinie ermöglicht es Ihren AWS IoT Geräten, mithilfe von MQTT-Nachrichten Verbindungen herzustellen und mit Geräteschatten zu kommunizieren. Weitere Informationen zu MQTT-Nachrichten finden Sie unter Was ist MQTT? . Um mit Geräteschatten zu interagieren, veröffentlichen und empfangen Ihre AWS IoT Dinge MQTT-Nachrichten zu Themen, die mit `$aws/things/thing-name/shadow/` beginnen. Diese Richtlinie enthält eine Ding-Richtlinienvariable, die als`${iot:Connection.Thing.ThingName}`. Diese Variable ersetzt in jedem Thema den Namen der verbundenen Sache. Die `iot:Connect` Anweisung beschränkt, welche Geräte Verbindungen herstellen können, und stellt so sicher, dass die Richtlinienvariable thing nur Namen ersetzen kann, die mit `SiteWiseTutorialDevice` beginnen.

Weitere Informationen finden Sie unter Ding-Richtlinienvariablen im AWS IoT Entwicklerhandbuch.

> **Note**
>
> Diese Richtlinie gilt für Objekte, deren Namen mit `SiteWiseTutorialDevice` beginnen. Um einen anderen Namen für Ihre Objekte zu verwenden, müssen Sie die Richtlinie entsprechend aktualisieren.

8. Wählen Sie Create (Erstellen) aus.

Schritt 2: Eine AWS IoT Sache erstellen und konfigurieren

In diesem Verfahren erstellen und konfigurieren Sie eine AWS IoT Sache. Sie können Ihren Entwicklungscomputer als ein AWS IoT Ding bezeichnen. Denken Sie im weiteren Verlauf daran, dass die Prinzipien, die Sie hier lernen, auch auf konkrete Projekte angewendet werden können. Sie haben die Flexibilität, AWS IoT Dinge auf jedem Gerät zu erstellen und einzurichten, auf dem ein AWS IoT SDK ausgeführt werden kann, einschließlich AWS IoT Greengrass FreeRTOS. Weitere Informationen finden Sie unter AWS IoT SDKs im Entwicklerhandbuch.AWS IoT

Um etwas zu erstellen und zu AWS IoT konfigurieren

1. Öffnen Sie eine Befehlszeile, und führen Sie den folgenden Befehl aus, um ein Verzeichnis für dieses Lernprogramm zu erstellen.

```
mkdir iot-sitewise-rule-tutorial
```

```
cd iot-sitewise-rule-tutorial
```

2. Führen Sie den folgenden Befehl aus, um ein Verzeichnis für die Zertifikate Ihres Objekts zu erstellen.

   ```
   mkdir device1
   ```

   Wenn Sie zusätzliche Objekte erstellen, erhöhen Sie die Nummer im Verzeichnisnamen entsprechend, um zu verfolgen, welche Zertifikate zu welchem Objekt gehören.

3. Navigieren Sie zur AWS IoT -Konsole.
4. Wählen Sie im linken Navigationsbereich im Abschnitt Verwalten die Option Alle Geräte aus. Wählen Sie dann Things (Objekte) aus.
5. Wenn das Dialogfeld You don't have any things yet (Sie haben noch keine Objekte) angezeigt wird, wählen Sie Create a thing (Objekt erstellen) aus. Wählen Sie andernfalls Dinge erstellen aus.
6. Wählen Sie auf der Seite „Dinge erstellen“ die Option „Ein einzelnes Ding erstellen“ und dann „Weiter“ aus.
7. Geben Sie auf der Seite „Dingeigenschaften angeben“ einen Namen für Ihr AWS IoT Ding ein (z. B.**`SiteWiseTutorialDevice1`**) und wählen Sie dann Weiter aus. Wenn Sie zusätzliche Objekte erstellen, erhöhen Sie die Nummer im Namen des Objekts entsprechend.

   > **Important**
   >
   > Der Name des Dings muss mit dem Namen übereinstimmen, der in der Richtlinie verwendet wurde, die Sie in Schritt 1: Erstellen einer AWS IoT Richtlinie erstellt haben. Andernfalls kann Ihr Gerät keine Verbindung zu herstellen AWS IoT.

8. Wählen Sie auf der Seite Gerätezertifikat konfigurieren — optional die Option Neues Zertifikat automatisch generieren (empfohlen) und dann Weiter aus. Mithilfe von Zertifikaten können AWS IoT Sie Ihre Geräte sicher identifizieren.
9. Wählen Sie auf der Seite Richtlinien an Zertifikat anhängen — optional die Richtlinie aus, die Sie in Schritt 1: AWS IoT Richtlinie erstellen erstellt haben, und wählen Sie Ding erstellen aus.
10. Gehen Sie im Dialogfeld Zertifikate und Schlüssel herunterladen wie folgt vor:

    a. Wählen Sie die Download-Links, um das Zertifikat, den öffentlichen Schlüssel und den privaten Schlüssel Ihres Objekts herunterzuladen. Speichern Sie alle drei Dateien in dem

Verzeichnis, das Sie für die Zertifikate Ihres Objekts erstellt haben (zum Beispiel `iot-sitewise-rule-tutorial/device1`).

> **Important**
>
> Dies ist das einzige Mal, dass Sie das Zertifikat und die Schlüssel Ihres Objekts herunterladen können, die Sie benötigen, damit Ihr Gerät erfolgreich eine Verbindung mit AWS IoT herstellen kann.

b. Wählen Sie den Link Herunterladen, um ein Root-CA-Zertifikat herunterzuladen. Speichern Sie das CA-Stammzertifikat der Zertifizierungsstelle in `iot-sitewise-rule-tutorial`. Wir empfehlen Ihnen, Amazon Root CA 1 herunterzuladen.

11. Wählen Sie Erledigt aus.

Sie haben jetzt AWS IoT etwas auf Ihrem Computer registriert. Führen Sie einen der folgenden nächsten Schritte aus:

- Fahren Sie mit Schritt 3 fort: Erstellen eines Geräte-Asset-Modells, ohne zusätzliche AWS IoT Dinge zu erstellen. Sie können dieses Lernprogramm mit nur einem Objekt abschließen.
- Wiederholen Sie die Schritte in diesem Abschnitt auf einem anderen Computer oder Gerät, um weitere AWS IoT -Objekte zu erstellen. Für dieses Tutorial empfehlen wir, diese Option zu befolgen, damit Sie eindeutige CPU- und Speicherauslastungsdaten von mehreren Geräten erfassen können.
- Wiederholen Sie die Schritte in diesem Abschnitt auf demselben Gerät (Ihrem Computer), um weitere AWS IoT -Objekte zu erstellen. Jedes Gerät AWS IoT empfängt ähnliche CPU- und Speichernutzungsdaten von Ihrem Computer. Verwenden Sie daher diesen Ansatz, um zu demonstrieren, dass nicht eindeutige Daten von mehreren Geräten aufgenommen werden.

Schritt 3: Erstellen eines Geräte-Asset-Modells

In diesem Verfahren erstellen Sie ein Asset-Modell, das Ihre Geräte darstellt, die CPU- und Speichernutzungsdaten streamen. AWS IoT SiteWise Um Daten in Anlagen zu verarbeiten, die Gerätegruppen repräsentieren, setzen Asset-Modelle konsistente Informationen für mehrere Anlagen desselben Typs voraus. Weitere Informationen finden Sie unter Modellieren von industriellen Komponenten.

So erstellen Sie ein Komponentenmodell, das ein Gerät darstellt

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Models (Modelle) aus.
3. Wählen Sie Modell erstellen aus.
4. Geben Sie unter Modelldetails einen Namen für Ihr Modell ein. z. B. **`SiteWise Tutorial Device Model`**.
5. Führen Sie unter Measurement definitions (Messungsdefinitionen) die folgenden Schritte aus:

   a. Geben Sie unter Name **`CPU Usage`** ein.

   b. Geben Sie unter Unit (Einheit) **`%`** ein.

   c. Lassen Sie den Data type (Datentyp) bei Double (Doppelt).

   Messungseigenschaften stellen die Rohdatenströme eines Geräts dar. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).
6. Wählen Sie Neue Messung hinzufügen aus, um eine zweite Messeigenschaft hinzuzufügen.
7. Führen Sie in der zweiten Zeile unter Measurement definitions (Messungsdefinitionen) die folgenden Schritte aus:

   a. Geben Sie unter Name **`Memory Usage`** ein.

   b. Geben Sie unter Unit (Einheit) **`%`** ein.

   c. Lassen Sie den Data type (Datentyp) bei Double (Doppelt).
8. Führen Sie unter Metric definitions (Metrikdefinitionen) die folgenden Schritte aus:

   a. Geben Sie unter Name **`Average CPU Usage`** ein.

   b. Geben Sie unter Formula (Formel) **`avg(CPU Usage)`** ein. Wählen Sie CPU Usage aus der Autovervollständigungsliste aus, wenn sie angezeigt wird.

   c. Geben Sie unter Time interval (Zeitintervall) **`5 minutes`** ein.

   Metrikeigenschaften definieren Aggregationsberechnungen, die alle Eingabedatenpunkte über ein Intervall verarbeiten und einen einzelnen Datenpunkt pro Intervall ausgeben. Diese Metrikeigenschaft berechnet alle 5 Minuten die durchschnittliche CPU-Auslastung jedes Geräts. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

9. Wählen Sie Neue Metrik hinzufügen, um eine zweite Metrikeigenschaft hinzuzufügen.
10. Führen Sie in der zweiten Zeile unter Metric definitions (Metrikdefinitionen) die folgenden Schritte aus:

    a. Geben Sie unter Name **`Average Memory Usage`** ein.

    b. Geben Sie unter Formula (Formel) **`avg(Memory Usage)`** ein. Wählen Sie Memory Usage aus der Autovervollständigungsliste aus, wenn sie angezeigt wird.

    c. Geben Sie unter Time interval (Zeitintervall) **`5 minutes`** ein.

    Diese Metrikeigenschaft berechnet alle 5 Minuten die durchschnittliche Speicherbelegung jedes Geräts.
11. (Optional) Fügen Sie weitere zusätzliche Metriken hinzu, die Sie pro Gerät berechnen möchten. Einige interessante Funktionen sind `min` und `max`. Weitere Informationen finden Sie unter Verwenden von Formelausdrücken. In Schritt 4: Erstellen eines Geräteflotten-Asset-Modells erstellen Sie ein übergeordnetes Asset, das anhand von Daten aus Ihrer gesamten Geräteflotte Kennzahlen berechnen kann.
12. Wählen Sie Modell erstellen aus.

Schritt 4: Erstellen eines Geräteflotten-Asset-Modells

In diesem Verfahren erstellen Sie ein Objektmodell, AWS IoT SiteWise das Ihre Sammlung von Geräten symbolisiert. Innerhalb dieses Asset-Modells legen Sie eine Struktur fest, die es Ihnen ermöglicht, zahlreiche Geräte-Assets zu einem übergeordneten Flotten-Asset zu verknüpfen. Anschließend skizzieren Sie Kennzahlen im Flotten-Asset-Modell, um Daten aus allen verbundenen Gerätebeständen zu konsolidieren. Dieser Ansatz bietet Ihnen umfassende Einblicke in die Gesamtleistung Ihrer gesamten Flotte.

So erstellen Sie ein Komponentenmodell, das eine Geräteflotte darstellt:

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Models (Modelle) aus.
3. Wählen Sie Modell erstellen aus.
4. Geben Sie unter Modelldetails einen Namen für Ihr Modell ein. z. B. **`SiteWise Tutorial Device Fleet Model`**.
5. Führen Sie unter Hierarchy definitions (Hierarchiedefinitionen) die folgenden Schritte aus:

a. Geben Sie unter Hierarchy name (Hierarchiename) **`Device`** ein.

b. Wählen Sie unter Hierarchy model (Hierarchiemodell) das Gerätekomponentenmodell (**`SiteWise Tutorial Device Model`**).

Eine Hierarchie definiert eine Beziehung zwischen einem übergeordneten (Flotten-) Komponentenmodell und einem untergeordneten (Geräte-) Komponentenmodell. Übergeordnete Komponenten können auf die Eigenschaftendaten von untergeordneten Komponenten zugreifen. Wenn Sie Komponenten später erstellen, müssen Sie untergeordnete Komponenten gemäß einer Hierarchiedefinition im übergeordneten Komponentenmodell den übergeordneten Komponenten zuordnen. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.

6. Führen Sie unter Metric definitions (Metrikdefinitionen) die folgenden Schritte aus:

a. Geben Sie unter Name **`Average CPU Usage`** ein.

b. Geben Sie unter Formula (Formel) **`avg(Device | Average CPU Usage)`** ein. Wenn die Autovervollständigungsliste angezeigt wird, wählen Sie Device, um eine Hierarchie auszuwählen, und dann Average CPU Usage, um die Metrik aus der zuvor erstellten Gerätekomponente auszuwählen.

c. Geben Sie unter Time interval (Zeitintervall) **`5 minutes`** ein.

Diese Metrikeigenschaft berechnet die durchschnittliche CPU-Auslastung aller Gerätekomponenten, die einer Flottenkomponente über die **`Device`**-Hierarchie zugeordnet sind.

7. Wählen Sie Neue Metrik hinzufügen aus, um eine zweite Metrikeigenschaft hinzuzufügen.

8. Führen Sie in der zweiten Zeile unter Metric definitions (Metrikdefinitionen) die folgenden Schritte aus:

a. Geben Sie unter Name **`Average Memory Usage`** ein.

b. Geben Sie unter Formula (Formel) **`avg(Device | Average Memory Usage)`** ein. Wenn die Autovervollständigungsliste angezeigt wird, wählen Sie Device, um eine Hierarchie auszuwählen, und dann Average Memory Usage, um die Metrik aus der zuvor erstellten Gerätekomponente auszuwählen.

c. Geben Sie unter Time interval (Zeitintervall) **`5 minutes`** ein.

Diese Metrikeigenschaft berechnet die durchschnittliche Speicherbelegung aller Gerätekomponenten, die einer Flottenkomponente über die **`Device`**-Hierarchie zugeordnet sind.

9. (Optional) Fügen Sie weitere zusätzliche Metriken hinzu, die Sie für Ihre gesamte Geräteflotte berechnen möchten.
10. Wählen Sie Modell erstellen aus.

Schritt 5: Geräte-Asset erstellen und konfigurieren

In diesem Verfahren generieren Sie ein Geräte-Asset, das auf Ihrem Geräte-Asset-Modell basiert. Anschließend definieren Sie Eigenschaftsaliase für jede Messungseigenschaft. Ein Eigenschaftsalias ist eine eindeutige Zeichenfolge, die eine Asset-Eigenschaft identifiziert. Später können Sie eine Eigenschaft für den Datenupload identifizieren, indem Sie die Aliase anstelle der Asset-ID und der Eigenschafts-ID verwenden. Weitere Informationen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

So erstellen Sie eine Gerätekomponente und definieren Eigenschaftsaliase

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).
3. Wählen Sie dann Create asset (Komponente erstellen) aus.
4. Wählen Sie unter Modellinformationen das Asset-Modell Ihres Geräts aus. **`SiteWise Tutorial Device Model`**
5. Geben Sie unter Inventarinformationen einen Namen für Ihr Asset ein. z. B. **`SiteWise Tutorial Device 1`**.
6. Wählen Sie dann Create asset (Komponente erstellen) aus.
7. Wählen Sie für Ihre neue Gerätekomponente Edit (Bearbeiten).
8. Geben Sie unter CPU Usage **`/tutorial/device/SiteWiseTutorialDevice1/cpu`** als Eigenschaftenalias ein. Sie nehmen den Namen der AWS IoT Sache in den Eigenschaftsalias auf, sodass Sie mithilfe einer einzigen AWS IoT Regel Daten von all Ihren Geräten aufnehmen können.
9. Geben Sie unter Memory Usage **`/tutorial/device/SiteWiseTutorialDevice1/memory`** als Eigenschaftenalias ein.
10. Wählen Sie Speichern.

Wenn Sie zuvor mehrere AWS IoT Dinge erstellt haben, wiederholen Sie die Schritte 3 bis 10 für jedes Gerät und erhöhen Sie die Zahl im Assetnamen und den Eigenschaftsaliasnamen entsprechend. Beispielsweise sollte der Name der zweiten Gerätekomponente **`SiteWise Tutorial Device 2`** sein und die Eigenschaftsaliase sollten **`/tutorial/device/SiteWiseTutorialDevice2/cpu`** und **`/tutorial/device/SiteWiseTutorialDevice2/memory`** sein.

Schritt 6: Ein Geräteflotten-Asset erstellen und konfigurieren

In diesem Verfahren erstellen Sie ein Geräteflotten-Asset, das aus Ihrem Geräteflotten-Asset-Modell abgeleitet ist. Anschließend verknüpfen Sie Ihre individuellen Geräte-Assets mit dem Flotten-Asset. Diese Zuordnung ermöglicht es, anhand der metrischen Eigenschaften der Flottenanlage Daten von mehreren Geräten zusammenzustellen und zu analysieren. Diese Daten bieten Ihnen einen konsolidierten Überblick über die Gesamtleistung der gesamten Flotte.

So erstellen Sie eine Geräteflottenkomponente und ordnen ihr Gerätekomponenten zu:

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).
3. Wählen Sie dann Create asset (Komponente erstellen) aus.
4. Wählen Sie unter Modellinformationen das Asset-Modell Ihrer Geräteflotte aus**`SiteWise Tutorial Device Fleet Model`**.
5. Geben Sie unter Inventarinformationen einen Namen für Ihr Asset ein. z. B. **`SiteWise Tutorial Device Fleet 1`**.
6. Wählen Sie dann Create asset (Komponente erstellen) aus.
7. Wählen Sie für Ihre neue Geräteflottenkomponente Edit (Bearbeiten).
8. Wählen Sie unter Diesem Asset zugeordnete Assets die Option Verbundenes Asset hinzufügen aus und gehen Sie wie folgt vor:

    a. Wählen Sie unter Hierarchy (Hierarchie) die Option Device aus. Diese Hierarchie identifiziert die hierarchische Beziehung zwischen Geräte- und Geräteflottenkomponenten. Sie haben diese Hierarchie im Geräteflottenkomponentenmodell früher in diesem Tutorial definiert.

    b. Wählen Sie unter Asset (Komponente) Ihre Gerätekomponente, SiteWise Tutorial Device 1, aus.
9. (Optional) Wenn Sie zuvor mehrere Geräte-Assets erstellt haben, wiederholen Sie die Schritte 8 bis 10 für jedes Geräte-Asset, das Sie erstellt haben.

10. Wählen Sie Speichern.

    Sie sollten nun Ihre Gerätekomponenten als Hierarchie sehen.

Schritt 7: Erstellen einer Regel in AWS IoT Core zum Senden von Daten an Geräte-Assets

In diesem Verfahren legen Sie eine Regel in fest AWS IoT Core. Die Regel dient dazu, Benachrichtigungen von Geräteschatten zu interpretieren und die Daten an Ihre Geräteressourcen zu übertragen. AWS IoT SiteWise Jedes Mal, wenn der Shadow Ihres Geräts aktualisiert wird, wird eine MQTT-Nachricht AWS IoT gesendet. Sie können eine Regel erstellen, die aktiv wird, wenn sich Geräteschatten basierend auf der MQTT-Nachricht ändern. In diesem Fall besteht das Ziel darin, die Aktualisierungsnachricht zu verarbeiten, die Eigenschaftswerte zu extrahieren und sie an Ihre Geräteressourcen in zu übertragen. AWS IoT SiteWise

Um eine Regel mit einer AWS IoT SiteWise Aktion zu erstellen

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Nachrichtenweiterleitung und dann Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für Ihre Regel ein und wählen Sie dann Weiter.
5. Geben Sie die folgende SQL-Anweisung ein und wählen Sie dann Weiter.

   ```
   SELECT
     *
   FROM
     '$aws/things/+/shadow/update/accepted'
   WHERE
     startsWith(topic(3), "SiteWiseTutorialDevice")
   ```

   Diese Regelabfrageanweisung funktioniert, weil der Geräte-Schattenservice Schattenaktualisierungen in `$aws/things/thingName/shadow/update/accepted` veröffentlicht. Weitere Informationen zu Device Shadows finden Sie unter Device Shadow Service im AWS IoT Entwicklerhandbuch.

   In der `WHERE`-Klausel verwendet diese Regelabfrageanweisung die `topic(3)`-Funktion, um den Namen des Objekts aus dem dritten Segment des Themas abzurufen. Anschließend filtert die

Anweisung Geräte heraus, die Namen haben, die nicht mit denen der Geräte für das Tutorial übereinstimmen. Weitere Informationen zu AWS IoT SQL finden Sie in der AWS IoT SQL-Referenz im AWS IoT Entwicklerhandbuch.

6. Wählen Sie unter Regelaktionen die Option Nachrichtendaten an Asset-Eigenschaften senden in aus AWS IoT SiteWise und gehen Sie wie folgt vor:

   a. Wählen Sie By property alias (Nach Eigenschaftenalias).

   b. Geben Sie unter Property alias (Eigenschaftenalias) **`/tutorial/device/${topic(3)}/cpu`** ein.

      Die `${...}` Syntax ist eine Ersatzvorlage. AWS IoT wertet den Inhalt in den geschweiften Klammern aus. Diese Substitutionsvorlage ruft den Namen des Objekts aus dem Thema ab, um einen Alias zu erstellen, der für jedes Thema eindeutig ist. Weitere Informationen finden Sie im Entwicklerhandbuch unter AWS IoT Substitutionsvorlagen.

      > **Note**
      >
      > Da ein Ausdruck in einer Substitutionsvorlage getrennt von der `SELECT`-Anweisung ausgewertet wird, können Sie keine Substitutionsvorlage verwenden, um auf einen Alias zu verweisen, der mit einer `AS`-Klausel erstellt wurde. Zusätzlich zu den unterstützten Funktionen und Operatoren können Sie nur in der ursprünglichen Nutzlast vorhandene Informationen referenzieren.

   c. Geben **`${concat(topic(3), "-cpu-", floor(state.reported.timestamp))}`** Sie im Feld Eintrags-ID — optional den Wert ein.

      Eintrags-IDs identifizieren jeden Werteeintragsversuch eindeutig. Wenn ein Eintrag einen Fehler zurückgibt, finden Sie die Eintrags-ID in der Fehlerausgabe, um das Problem zu beheben. Die Substitutionsvorlage in dieser Eintrags-ID kombiniert den Namen des Objekts und den gemeldeten Zeitstempel des Geräts. Beispielsweise könnte die resultierende Eintrags-ID wie `SiteWiseTutorialDevice1-cpu-1579808494` aussehen.

   d. Geben Sie unter Time in seconds (Zeit in Sekunden) **`${floor(state.reported.timestamp)}`** ein.

      Diese Substitutionsvorlage berechnet die Zeit in Sekunden aus dem gemeldeten Zeitstempel des Geräts. In diesem Tutorial melden Geräte Zeitstempel in Sekunden nach Unix-Epoche als Gleitkommazahl.

e. Geben **`${floor((state.reported.timestamp % 1) * 1E9)}`** Sie im Feld Offset in Nanos — optional den Wert ein.

   Diese Substitutionsvorlage berechnet die Verschiebung in Nanosekunden aus der Zeit in Sekunden, indem der Dezimalteil des gemeldeten Zeitstempels des Geräts konvertiert wird.

   > **Note**
   >
   > AWS IoT SiteWise setzt voraus, dass Ihre Daten einen aktuellen Zeitstempel in der Unix-Epochenzeit haben. Wenn Ihre Geräte die Zeit nicht genau melden, können Sie die aktuelle Zeit von der AWS IoT -Regelengine mit timestamp()abrufen. Diese Funktion meldet die Zeit in Millisekunden. Daher müssen Sie die Zeitparameter Ihrer Regelaktion auf die folgenden Werte aktualisieren:
   >
   > - Geben Sie unter Time in seconds (Zeit in Sekunden) **`${floor(timestamp() / 1E3)}`** ein.
   > - Geben Sie unter Offset in Nanos (Verschiebung in Nanosekunden) **`${(timestamp() % 1E3) * 1E6}`** ein.

f. Wählen Sie unter Data type (Datentyp) die Option Double (Doppelt).

   Dieser Datentyp muss mit dem Datentyp der Komponenteneigenschaft übereinstimmen, die Sie im Komponentenmodell definiert haben.

g. Geben Sie unter Value (Wert) **`${state.reported.cpu}`** ein. In Substitutionsvorlagen verwenden Sie den `.`-Operator, um einen Wert aus einer JSON-Struktur abzurufen.

h. Wählen Sie Add entry (Eintrag hinzufügen), um einen neuen Eintrag für die Speicherbelegungseigenschaft hinzuzufügen, und führen Sie die folgenden Schritte für diese Eigenschaft erneut aus:

   i. Wählen Sie By property alias (Nach Eigenschaftenalias).

   ii. Geben Sie unter Property alias (Eigenschaftenalias) **`/tutorial/device/${topic(3)}/memory`** ein.

   iii. Geben Sie im Feld Eintrags-ID — optional den Wert ein. **`${concat(topic(3), "-memory-", floor(state.reported.timestamp))}`**

   iv. Geben Sie unter Time in seconds (Zeit in Sekunden) **`${floor(state.reported.timestamp)}`** ein.

v. Geben **`${floor((state.reported.timestamp % 1) * 1E9)}`** Sie im Feld Offset in Nanos — optional den Wert ein.

vi. Wählen Sie unter Data type (Datentyp) die Option Double (Doppelt).

vii. Geben Sie unter Value (Wert) **`${state.reported.memory}`** ein.

i. Wählen Sie unter IAM-Rolle die Option Neue Rolle erstellen aus, um eine IAM-Rolle für diese Regelaktion zu erstellen. Diese Rolle ermöglicht AWS IoT die Übertragung von Daten auf Eigenschaften in Ihrer Geräteflotte und deren Asset-Hierarchie.

j. Geben Sie einen Rollennamen ein und wählen Sie Create.

7. (Optional) Konfigurieren Sie eine Fehleraktion, die Sie zur Problembehandlung Ihrer Regel verwenden können. Weitere Informationen finden Sie unter Fehlerbehebung bei einer Regel.
8. Wählen Sie Weiter.
9. Überprüfen Sie die Einstellungen und wählen Sie Erstellen, um die Regel zu erstellen.

Schritt 8: Ausführen des Geräteclient-Skripts

In diesem Tutorial verwenden Sie kein echtes Gerät, um Daten zu melden. Stattdessen führen Sie ein Skript aus, um den Geräteschatten AWS IoT Ihres Geräts mit der CPU- und Speicherauslastung zu aktualisieren, um echte Sensordaten nachzuahmen. Um das Skript auszuführen, müssen Sie zuerst die erforderlichen Python Pakete installieren. In diesem Verfahren installieren Sie die erforderlichen Python Pakete und führen dann das Geräteclientskript aus.

So konfigurieren und führen Sie das Geräte-Clientskript aus

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie unten im linken Navigationsbereich Settings (Einstellungen) aus.
3. Speichern Sie Ihren benutzerdefinierten Endpunkt zur Verwendung mit dem Geräte-Clientskript. Sie verwenden diesen Endpunkt, um mit den Schatten Ihres Objekts zu interagieren. Dieser Endpunkt ist eindeutig für Ihr Konto in der aktuellen Region.

   Ihr benutzerdefinierter Endpunkt sollte wie im folgenden Beispiel aussehen.

   ```
   identifier.iot.region.amazonaws.com
   ```

4. Öffnen Sie eine Befehlszeile, und führen Sie den folgenden Befehl aus, um zu dem zuvor erstellten Tutorialverzeichnis zu navigieren.

```
cd iot-sitewise-rule-tutorial
```

5. Führen Sie den folgenden Befehl aus, um das AWS IoT-Geräte-SDK for Python zu installieren:

```
pip3 install AWSIoTPythonSDK
```

Weitere Informationen finden Sie AWS IoT-Geräte-SDK for Pythonim AWS IoT Entwicklerhandbuch

6. Führen Sie den folgenden Befehl aus, um psutil, eine plattformübergreifende Prozess- und Systemdienstprogrammbibliothek, zu installieren.

```
pip3 install psutil
```

Weitere Informationen finden Sie unter psutil im Python-Paketindex.

7. Erstellen Sie eine Datei mit dem Namen `thing_performance.py` im Verzeichnis `iot-sitewise-rule-tutorial`, und kopieren Sie dann den folgenden Python-Code in diese Datei.

```
import AWSIoTPythonSDK.MQTTLib as AWSIoTPyMQTT

import json
import psutil
import argparse
import logging
import time


# Configures the argument parser for this program.
def configureParser():
    parser = argparse.ArgumentParser()
    parser.add_argument(
        "-e",
        "--endpoint",
        action="store",
        required=True,
        dest="host",
        help="Your AWS IoT custom endpoint",
    )
    parser.add_argument(
```

```
        "-r",
        "--rootCA",
        action="store",
        required=True,
        dest="rootCAPath",
        help="Root CA file path",
    )
    parser.add_argument(
        "-c",
        "--cert",
        action="store",
        required=True,
        dest="certificatePath",
        help="Certificate file path",
    )
    parser.add_argument(
        "-k",
        "--key",
        action="store",
        required=True,
        dest="privateKeyPath",
        help="Private key file path",
    )
    parser.add_argument(
        "-p",
        "--port",
        action="store",
        dest="port",
        type=int,
        default=8883,
        help="Port number override",
    )
    parser.add_argument(
        "-n",
        "--thingName",
        action="store",
        required=True,
        dest="thingName",
        help="Targeted thing name",
    )
    parser.add_argument(
        "-d",
        "--requestDelay",
        action="store",
```

```
        dest="requestDelay",
        type=float,
        default=1,
        help="Time between requests (in seconds)",
    )
    parser.add_argument(
        "-v",
        "--enableLogging",
        action="store_true",
        dest="enableLogging",
        help="Enable logging for the AWS IoT Device SDK for Python",
    )
    return parser


# An MQTT shadow client that uploads device performance data to AWS IoT at a
 regular interval.
class PerformanceShadowClient:
    def __init__(
        self,
        thingName,
        host,
        port,
        rootCAPath,
        privateKeyPath,
        certificatePath,
        requestDelay,
    ):
        self.thingName = thingName
        self.host = host
        self.port = port
        self.rootCAPath = rootCAPath
        self.privateKeyPath = privateKeyPath
        self.certificatePath = certificatePath
        self.requestDelay = requestDelay

    # Updates this thing's shadow with system performance data at a regular
 interval.
    def run(self):
        print("Connecting MQTT client for {}...".format(self.thingName))
        mqttClient = self.configureMQTTClient()
        mqttClient.connect()
        print("MQTT client for {} connected".format(self.thingName))
        deviceShadowHandler = mqttClient.createShadowHandlerWithName(
```

```
            self.thingName, True
        )

        print("Running performance shadow client for {}...
\n".format(self.thingName))
        while True:
            performance = self.readPerformance()
            print("[{}]".format(self.thingName))
            print("CPU:\t{}%".format(performance["cpu"]))
            print("Memory:\t{}%\n".format(performance["memory"]))
            payload = {"state": {"reported": performance}}
            deviceShadowHandler.shadowUpdate(
                json.dumps(payload), self.shadowUpdateCallback, 5
            )
            time.sleep(args.requestDelay)

    # Configures the MQTT shadow client for this thing.
    def configureMQTTClient(self):
        mqttClient = AWSIoTPyMQTT.AWSIoTMQTTShadowClient(self.thingName)
        mqttClient.configureEndpoint(self.host, self.port)
        mqttClient.configureCredentials(
            self.rootCAPath, self.privateKeyPath, self.certificatePath
        )
        mqttClient.configureAutoReconnectBackoffTime(1, 32, 20)
        mqttClient.configureConnectDisconnectTimeout(10)
        mqttClient.configureMQTTOperationTimeout(5)
        return mqttClient

    # Returns the local device's CPU usage, memory usage, and timestamp.
    def readPerformance(self):
        cpu = psutil.cpu_percent()
        memory = psutil.virtual_memory().percent
        timestamp = time.time()
        return {"cpu": cpu, "memory": memory, "timestamp": timestamp}

    # Prints the result of a shadow update call.
    def shadowUpdateCallback(self, payload, responseStatus, token):
        print("[{}]".format(self.thingName))
        print("Update request {} {}\n".format(token, responseStatus))


# Configures debug logging for the AWS IoT Device SDK for Python.
def configureLogging():
    logger = logging.getLogger("AWSIoTPythonSDK.core")
```

```
    logger.setLevel(logging.DEBUG)
    streamHandler = logging.StreamHandler()
    formatter = logging.Formatter(
        "%(asctime)s - %(name)s - %(levelname)s - %(message)s"
    )
    streamHandler.setFormatter(formatter)
    logger.addHandler(streamHandler)


# Runs the performance shadow client with user arguments.
if __name__ == "__main__":
    parser = configureParser()
    args = parser.parse_args()
    if args.enableLogging:
        configureLogging()
    thingClient = PerformanceShadowClient(
        args.thingName,
        args.host,
        args.port,
        args.rootCAPath,
        args.privateKeyPath,
        args.certificatePath,
        args.requestDelay,
    )
    thingClient.run()
```

8. Führen Sie `thing_performance.py` über die Befehlszeile mit den folgenden Parametern aus:

   - `-n`, `--thingName` — Der Name Ihres Dings, z. **`SiteWiseTutorialDevice1`** B.
   - `-e`, `--endpoint` — Ihr benutzerdefinierter AWS IoT Endpunkt, den Sie zuvor in diesem Verfahren gespeichert haben.
   - `-r`, `--rootCA` — Der Pfad zu Ihrem AWS IoT Root-CA-Zertifikat.
   - `-c`, `--cert` — Der Pfad zu deinem AWS IoT Ding-Zertifikat.
   - `-k`, `--key` — Der Pfad zu Ihrem privaten Schlüssel AWS IoT für Ihr Ding-Zertifikat.
   - `-d`, `--requestDelay` — (Optional) Die Wartezeit in Sekunden zwischen den einzelnen Device-Shadow-Updates. Standard ist 1 Sekunde.
   - `-v`, `--enableLogging` — (Optional) Wenn dieser Parameter vorhanden ist, druckt das Skript Debug-Meldungen von. AWS IoT-Geräte-SDK for Python

   Ihr Befehl sollte ähnlich wie im folgenden Beispiel aussehen.

```
python3 thing_performance.py \
  --thingName SiteWiseTutorialDevice1 \
  --endpoint identifier.iot.region.amazonaws.com \
  --rootCA AmazonRootCA1.pem \
  --cert device1/thing-id-certificate.pem.crt \
  --key device1/thing-id-private.pem.key
```

Wenn Sie das Skript für zusätzliche AWS IoT Dinge ausführen, aktualisieren Sie den Namen und das Zertifikatsverzeichnis entsprechend.

9. Versuchen Sie, Programme auf Ihrem Gerät zu öffnen und zu schließen, um zu sehen, wie sich die CPU- und Speichernutzung ändern. Das Skript druckt jede Ablesung von CPU- und Speichernutzung. Wenn das Skript Daten erfolgreich zum Geräteschattenservice hochlädt, sollte die Ausgabe des Skripts wie im folgenden Beispiel aussehen.

```
[SiteWiseTutorialDevice1]
CPU:    24.6%
Memory: 85.2%

[SiteWiseTutorialDevice1]
Update request e6686e44-fca0-44db-aa48-3ca81726f3e3 accepted
```

10. Gehen Sie folgendermaßen vor, um zu überprüfen, ob das Skript den Geräteschatten aktualisiert:

    a. Navigieren Sie zur AWS IoT -Konsole.

    b. Wählen Sie im linken Navigationsbereich Alle Geräte und dann Dinge aus.

    c. Wähle dein Ding, SiteWiseTutorialDevice.

    d. Wählen Sie die Registerkarte Geräteschatten, wählen Sie Classic Shadow und vergewissern Sie sich, dass der Shadow-Status wie im folgenden Beispiel aussieht.

```
{
  "reported": {
    "cpu": 24.6,
    "memory": 85.2,
    "timestamp": 1579567542.2835066
  }
}
```

Wenn der Schattenstatus Ihres Dings leer ist oder nicht wie im vorherigen Beispiel aussieht, überprüfen Sie, ob das Skript ausgeführt wird und ob die Verbindung erfolgreich hergestellt wurde AWS IoT. Wenn das Skript beim Herstellen einer Verbindung zu weiterhin zu einem Timeout kommt AWS IoT, überprüfen Sie, ob Ihre Ding-Richtlinie gemäß dieser Anleitung konfiguriert ist.

11. Gehen Sie folgendermaßen vor, um zu überprüfen, ob die Regelaktion Daten an AWS IoT SiteWise sendet:

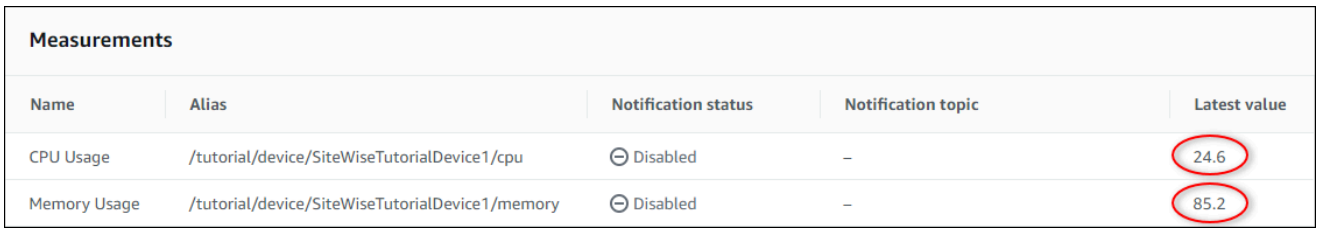
    a. Navigieren Sie zur AWS IoT SiteWise -Konsole.

    b. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).

    c. Wählen Sie den Pfeil neben Ihrer Geräteflottenkomponente (SiteWise Tutorial Device Fleet 1 1), um die Komponentenhierarchie zu erweitern, und wählen Sie dann Ihre Gerätekomponente (SiteWise Tutorial Device 1).

    d. Wählen Sie Measurements (Messungen).

    e. Stellen Sie sicher, dass die Zellen Latest value (Letzter Wert) Werte für die Eigenschaften CPU Usage und Memory Usage aufweisen.



    f. Wenn die Eigenschaften CPU Usage und Memory Usage nicht über die neuesten Werte verfügen, aktualisieren Sie die Seite. Wenn nach einigen Minuten keine Werte angezeigt werden, finden Sie weitere Informationen unter Fehlerbehebung bei einer Regel.

12. Sie haben dieses Tutorial abgeschlossen. Wenn Sie Live-Visualisierungen Ihrer Daten untersuchen möchten, können Sie ein Portal in AWS IoT SiteWise Monitor konfigurieren. Weitere Informationen finden Sie unter Daten überwachen mit AWS IoT SiteWise Monitor. Andernfalls können Sie STRG+C in der Eingabeaufforderung betätigen, um das Geräte-Clientskript zu stoppen. Es ist unwahrscheinlich, dass das Python-Programm so viele Nachrichten sendet, dass Kosten anfallen, aber es hat sich bewährt, das Programm zu beenden, wenn Sie fertig sind.

Schritt 9: Ressourcen nach dem Tutorial bereinigen

Nachdem Sie das Tutorial zum Einlesen von Daten aus AWS IoT Dingen abgeschlossen haben, sollten Sie Ihre Ressourcen bereinigen, um zusätzliche Kosten zu vermeiden.

So löschen Sie hierarchische Objekte in AWS IoT SiteWise

1. Navigieren Sie zur Konsole AWS IoT SiteWise
2. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).
3. Wenn Sie Elemente in löschen AWS IoT SiteWise, müssen Sie zunächst deren Zuordnung aufheben.

   Führen Sie die folgenden Schritte aus, um die Zuordnung Ihrer Gerätekomponenten zu Ihrer Geräteflottenkomponente aufzuheben:

   a. Wählen Sie Ihr Geräteflotten-Asset (SiteWise Tutorial Device Fleet 1) aus.
   b. Wählen Sie Bearbeiten aus.
   c. Wählen Sie unter Assets associated to this asset (Dieser Komponente zugeordnete Komponenten) die Option Disassociate (Zuordnung aufheben) für jede Gerätekomponente, die dieser Geräteflottenkomponente zugeordnet ist.
   d. Wählen Sie Speichern.

      Sie sollten nun Ihre Gerätekomponenten nicht mehr als Hierarchie organisiert sehen.
4. Wählen Sie Ihre Gerätekomponente (SiteWise Tutorial Device 1).
5. Wählen Sie Löschen aus.
6. Geben Sie in das Bestätigungsfeld **`Delete`** ein, und wählen Sie dann Delete (Löschen).
7. Wiederholen Sie die Schritte 4 bis 6 für jedes Geräte-Asset und das Geräteflotten-Asset (SiteWise Tutorial Device Fleet 1).

Um hierarchische Objektmodelle zu löschen AWS IoT SiteWise

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wenn Sie dies noch nicht getan haben, löschen Sie Ihre Geräte- und Geräteflottenkomponenten. Weitere Informationen finden Sie im vorhergehenden Verfahren. Sie können ein Modell nicht löschen, wenn Sie Komponenten haben, die aus diesem Modell erstellt wurden.
3. Wählen Sie im linken Navigationsbereich Models (Modelle) aus.

4. Wählen Sie Ihr Geräteflottenkomponentenmodell (SiteWise Tutorial Device Fleet Model).

   Wenn Sie hierarchische Anlagenmodelle löschen, löschen Sie zunächst das übergeordnete Anlagenmodell.
5. Wählen Sie Löschen aus.
6. Geben Sie in das Bestätigungsfeld **`Delete`** ein, und wählen Sie dann Delete (Löschen).
7. Wiederholen Sie die Schritte 4 bis 6 für Ihr Gerätekomponentenmodell (SiteWise Tutorial Device Model).

Um eine Regel zu deaktivieren oder zu löschen AWS IoT Core

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Nachrichtenweiterleitung und dann Regeln aus.
3. Wählen Sie Ihre Regel aus und klicken Sie auf Löschen.
4. Geben Sie im Bestätigungsdialogfeld den Namen der Regel ein und wählen Sie dann Löschen.

Visualisierung und gemeinsame Nutzung von Windparkdaten in Monitor SiteWise

In diesem Tutorial wird erklärt, wie Industriedaten über verwaltete Webanwendungen, sogenannte Portale, visualisiert und gemeinsam genutzt AWS IoT SiteWise Monitor werden können. Jedes Portal umfasst Projekte, sodass Sie flexibel wählen können, auf welche Daten innerhalb jedes Projekts zugegriffen werden kann. Geben Sie anschließend Personen in Ihrer Organisation an, die auf jedes Portal zugreifen können. Ihre Benutzer melden sich mit AWS IAM Identity Center Konten bei Portalen an, sodass Sie Ihren vorhandenen Identitätsspeicher oder einen von verwalteten Speicher verwenden können AWS.

Sie und Ihre Benutzer mit ausreichenden Berechtigungen können in jedem Projekt Dashboards erstellen, um Ihre industriellen Daten sinnvoll zu visualisieren. Anschließend können Ihre Benutzer diese Dashboards anzeigen, um schnell Einblicke in Ihre Daten zu erhalten und Ihren Betrieb zu überwachen. Sie können administrative oder schreibgeschützte Berechtigungen für jedes Projekt für jeden Benutzer in Ihrem Unternehmen konfigurieren. Weitere Informationen finden Sie unter Daten überwachen mit AWS IoT SiteWise Monitor.

Im Laufe des Tutorials erweitern Sie die AWS IoT SiteWise Demo, indem Sie einen Beispieldatensatz für einen Windpark bereitstellen. Sie konfigurieren ein Portal in SiteWise Monitor, erstellen ein Projekt

und Dashboards zur Visualisierung der Windparkdaten. Das Tutorial behandelt auch die Erstellung zusätzlicher Benutzer sowie die Zuweisung von Berechtigungen, um das Projekt und die zugehörigen Dashboards zu besitzen oder anzusehen.

> **Note**
>
> Wenn Sie SiteWise Monitor verwenden, wird Ihnen pro Benutzer, der sich bei einem Portal anmeldet, eine Gebühr berechnet (pro Monat). In diesem Tutorial erstellen Sie drei Benutzer, aber Sie müssen sich nur mit einem Benutzer anmelden. Nachdem Sie dieses Tutorial abgeschlossen haben, fallen Gebühren für einen Benutzer an. Weitere Informationen finden Sie unter AWS IoT SiteWise -Preisgestaltung.

Themen

Voraussetzungen

Zum Durcharbeiten dieses Tutorials ist Folgendes erforderlich:

- Ein AWS-Konto. Falls Sie noch keines haben, beachten Sie die Informationen unter Einrichtung eines AWS-Konto.
- Ein Entwicklungscomputer, auf demWindows, macOSLinux, oder ausgeführt wird, Unix um auf den zuzugreifen AWS Management Console. Weitere Informationen finden Sie unter Erste Schritte mit AWS Management Console.
- Ein AWS Identity and Access Management (IAM-) Benutzer mit Administratorrechten.
- Eine laufende AWS IoT SiteWise Windpark-Demo. Wenn Sie die Demo einrichten, definiert sie Modelle und Anlagen AWS IoT SiteWise und streamt Daten an sie, um einen Windpark darzustellen. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo verwenden.

- Wenn Sie IAM Identity Center in Ihrem Konto aktiviert haben, melden Sie sich bei Ihrem AWS Organizations Verwaltungskonto an. Weitere Informationen zu finden Sie unter Terminologie und Konzepte für AWS Organizations. Wenn Sie IAM Identity Center nicht aktiviert haben, werden Sie es in diesem Tutorial aktivieren und Ihr Konto als Verwaltungskonto einrichten.

  Wenn Sie sich nicht bei Ihrem AWS Organizations Verwaltungskonto anmelden können, können Sie das Tutorial teilweise abschließen, sofern Sie einen IAM Identity Center-Benutzer in Ihrer Organisation haben. In diesem Fall können Sie das Portal und die Dashboards erstellen, aber Sie können keine neuen IAM Identity Center-Benutzer erstellen, um sie Projekten zuzuweisen.

Schritt 1: Erstellen Sie ein Portal in Monitor SiteWise

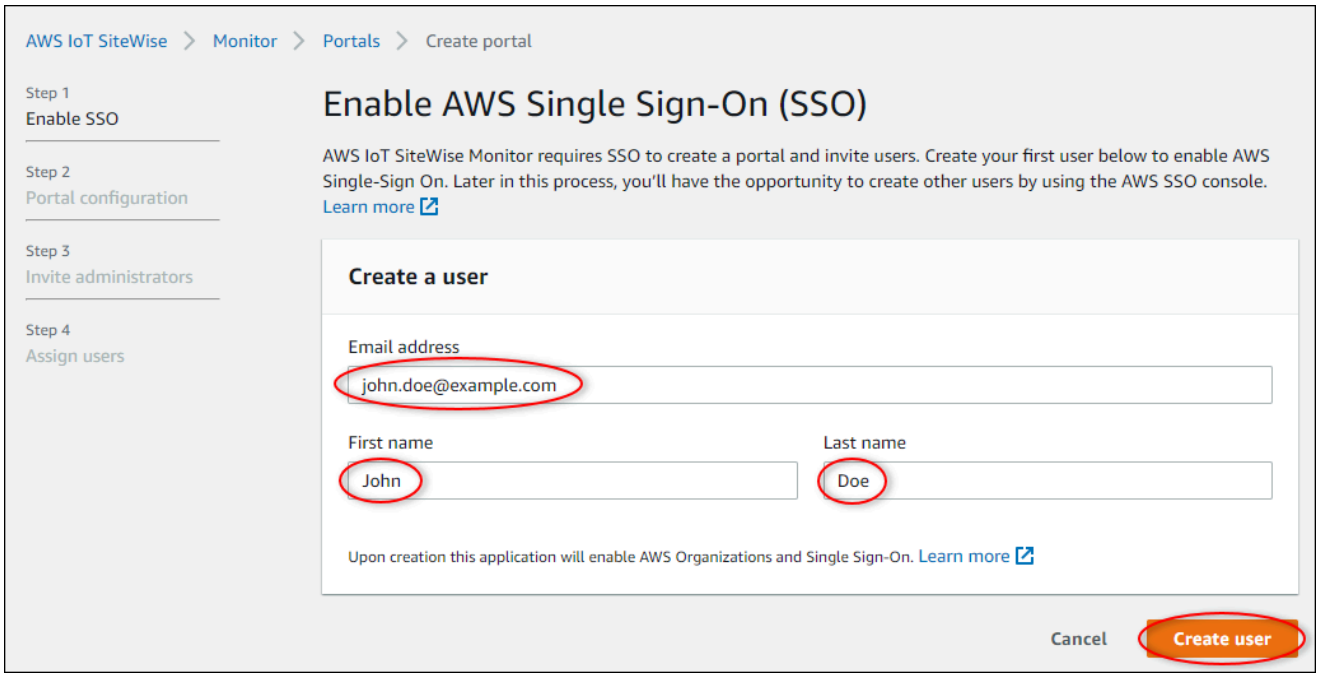
In diesem Verfahren erstellen Sie ein Portal in AWS IoT SiteWise Monitor. Jedes Portal ist eine verwaltete Webanwendung, bei der Sie und Ihre Benutzer sich mit AWS IAM Identity Center Konten anmelden können. Mit IAM Identity Center können Sie den vorhandenen Identitätsspeicher Ihres Unternehmens verwenden oder einen eigenen erstellen, der von verwaltet wird AWS. Die Mitarbeiter Ihres Unternehmens können sich anmelden, ohne einen separaten AWS-Konten Account erstellen zu müssen.

So erstellen Sie ein Portal

1. Melden Sie sich an der AWS IoT SiteWise -Konsole an.
2. Prüfen Sie, AWS IoT SiteWise welche Endgeräte und Kontingente unterstützt werden, und wechseln Sie bei AWS IoT SiteWise Bedarf zwischen den Regionen. Sie müssen die AWS IoT SiteWise Demo in derselben Region ausführen.
3. Wählen Sie im linken Navigationsbereich die Option Portale aus.
4. Wählen Sie Create Portal (Portal erstellen) aus.
5. Wenn Sie IAM Identity Center bereits aktiviert haben, fahren Sie mit Schritt 6 fort. Gehen Sie andernfalls wie folgt vor, um IAM Identity Center zu aktivieren:

   a. Geben Sie auf der Seite Aktivieren AWS IAM Identity Center (SSO) Ihre E-Mail-Adresse, Ihren Vornamen und Nachnamen ein, um einen IAM Identity Center-Benutzer für Sie als Portaladministrator zu erstellen. Verwenden Sie eine E-Mail-Adresse, auf die Sie zugreifen können, damit Sie eine E-Mail erhalten, mit der Sie ein Passwort für Ihren neuen IAM Identity Center-Benutzer festlegen können.

In einem Portal erstellt der Portaladministrator Projekte und weist Benutzer Projekten zu. Sie können später weitere Benutzer erstellen.



b. Wählen Sie Create user (Benutzer erstellen) aus.

6. Führen Sie auf der Seite Portalkonfiguration die folgenden Schritte aus:

   a. Geben Sie einen Namen für Ihr Portal ein, z. B. **`WindFarmPortal`**.

   b. (Optional) Geben Sie eine Beschreibung für Ihr Portal ein. Wenn Sie über mehrere Portale verfügen, verwenden Sie aussagekräftige Beschreibungen, um den Überblick über die Inhalte der einzelnen Portale zu behalten.

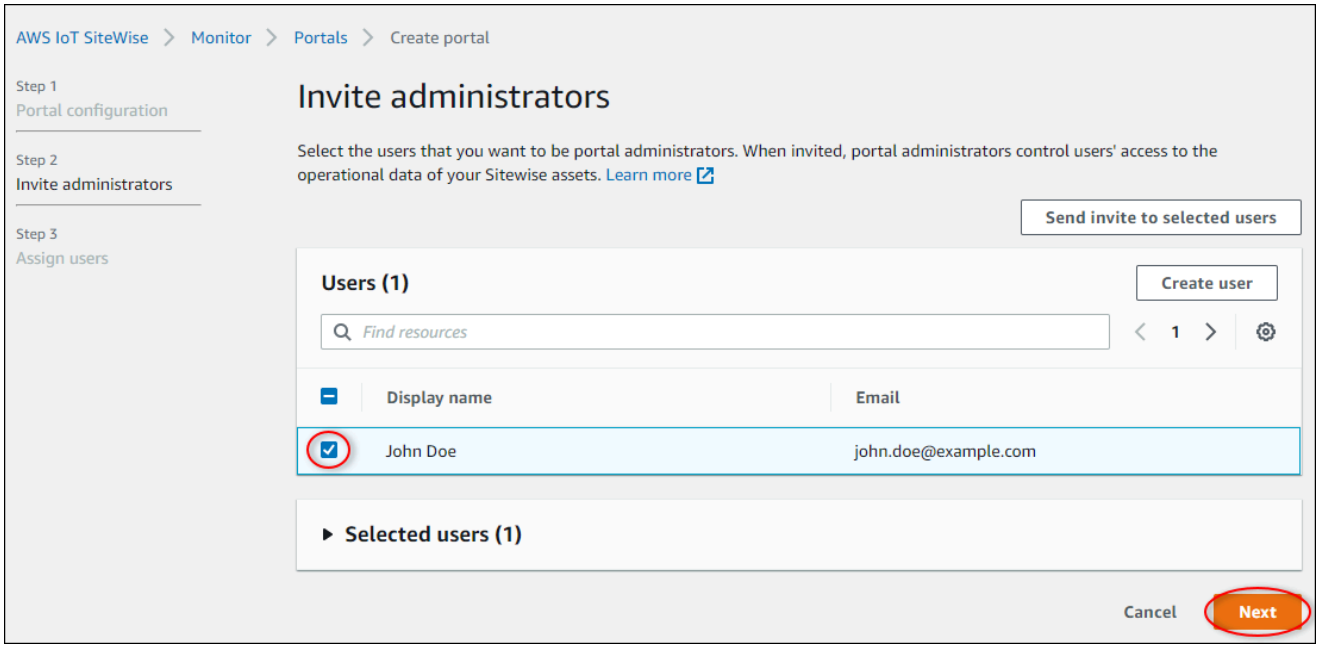
   c. (Optional) Laden Sie ein Bild hoch, das im Portal angezeigt werden soll.

   d. Geben Sie eine E-Mail-Adresse ein, an die sich Portalbenutzer wenden können, wenn sie ein Problem mit dem Portal haben und Hilfe vom AWS Administrator Ihres Unternehmens benötigen, um das Problem zu lösen.

   e. Wählen Sie Create Portal (Portal erstellen) aus.

7. Auf der Seite Administratoren einladen können Sie dem Portal IAM Identity Center-Benutzer als Administratoren zuweisen. Portaladministratoren verwalten Berechtigungen und Projekte innerhalb eines Portals. Gehen Sie auf dieser Seite wie folgt vor:

   a. Wählen Sie einen Benutzer als Portaladministrator aus. Wenn Sie IAM Identity Center zu einem früheren Zeitpunkt in diesem Tutorial aktiviert haben, wählen Sie den Benutzer aus, den Sie erstellt haben.



b. (Optional) Wählen Sie Send invite to selected users (Einladung an ausgewählte Benutzer senden) aus. Ihr E-Mail-Client wird geöffnet und eine Einladung wird im Nachrichtentext angezeigt. Sie können die E-Mail anpassen, bevor Sie sie an die Portaladministratoren senden. Sie können die E-Mail-Nachricht auch später an Ihre Portaladministratoren senden. Wenn Sie SiteWise Monitor zum ersten Mal ausprobieren und der Portaladministrator sein werden, müssen Sie sich keine E-Mail senden.

c. Wählen Sie Weiter aus.

8. Auf der Seite „Benutzer zuweisen“ können Sie dem Portal IAM Identity Center-Benutzer zuweisen. Portaladministratoren können diese Benutzer später als Projekteigentümer oder -betrachter zuweisen. Projekteigentümer können Dashboards in Projekten erstellen. Projektbetrachter haben nur Lesezugriff auf die ihnen zugewiesenen Projekte. Auf dieser Seite können Sie IAM Identity Center-Benutzer erstellen, die Sie dem Portal hinzufügen möchten.

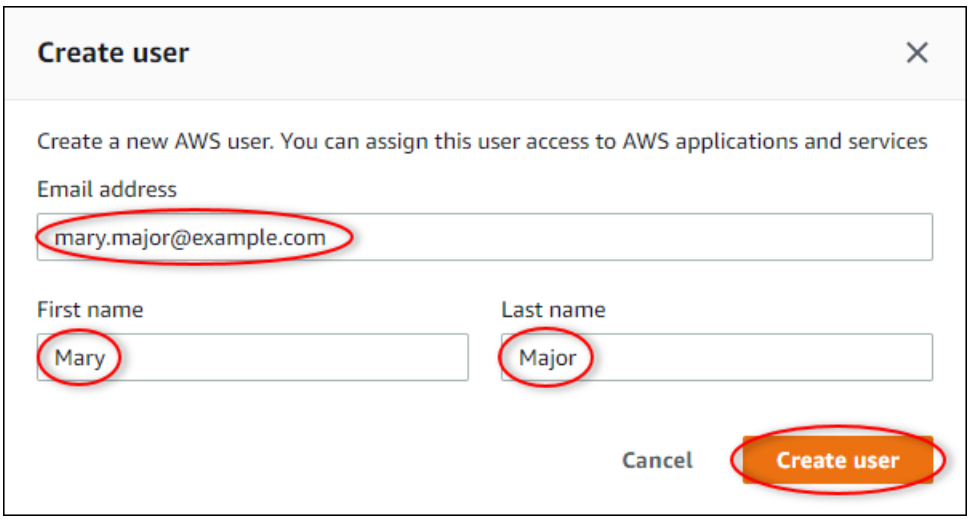
> **Note**
>
> Wenn Sie nicht mit Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie keine IAM Identity Center-Benutzer erstellen. Wählen Sie Benutzer zuweisen aus, um das Portal ohne Portalbenutzer zu erstellen, und überspringen Sie dann diesen Schritt.

Gehen Sie auf dieser Seite wie folgt vor:

a. Führen Sie die folgenden Schritte zweimal aus, um zwei IAM Identity Center-Benutzer zu erstellen:

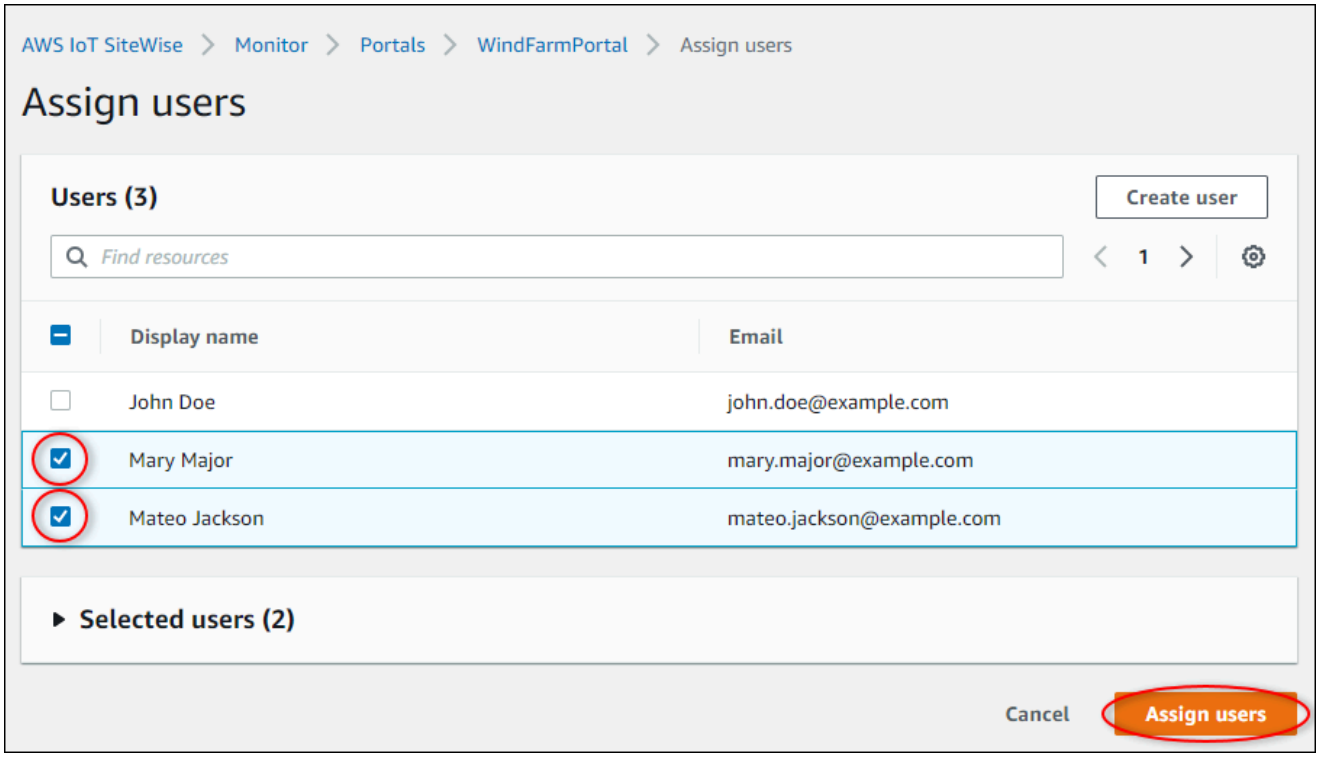
   i. Wählen Sie Benutzer erstellen, um ein Dialogfeld zu öffnen, in dem Sie Details für den neuen Benutzer eingeben können.

   ii. Geben Sie eine E-Mail-Adresse, einen Vornamen und einen Nachnamen für den neuen Benutzer ein. IAM Identity Center sendet dem Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Wenn Sie sich als diese Benutzer beim Portal anmelden möchten, wählen Sie eine E-Mail-Adresse aus, auf die Sie zugreifen können. Jede E-Mail-Adresse muss eindeutig sein. Ihre Benutzer melden sich mit ihrer E-Mail-Adresse als Benutzernamen beim Portal an.



   iii. Wählen Sie Create user (Benutzer erstellen) aus.

b. Wählen Sie die beiden IAM Identity Center-Benutzer aus, die Sie im vorherigen Schritt erstellt haben.



c. Wählen Sie Benutzer zuweisen, um diese Benutzer zum Portal hinzuzufügen.

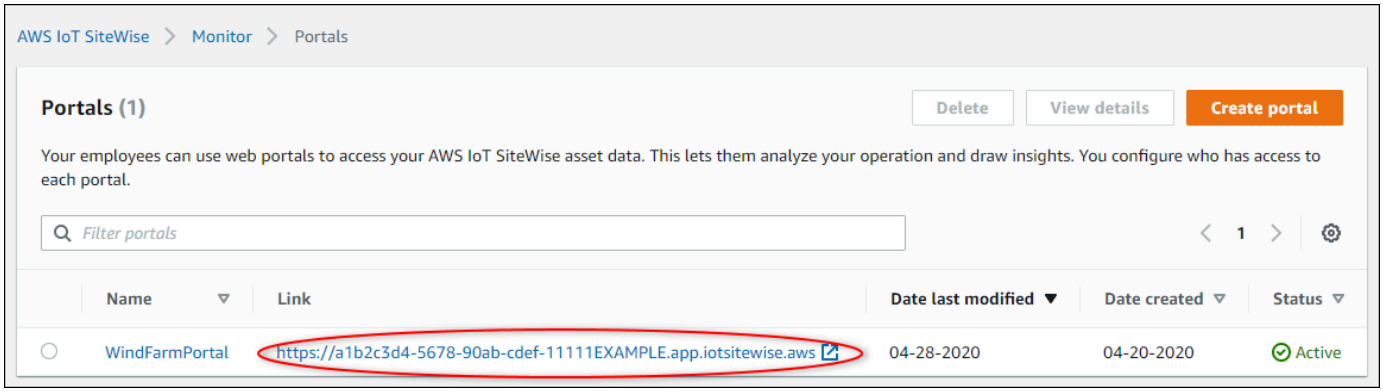
Die Seite „Portale“ wird geöffnet, wobei das neue Portal aufgelistet ist.

Schritt 2: Melden Sie sich bei einem Portal an

In diesem Verfahren melden Sie sich mit dem AWS IAM Identity Center Benutzer, den Sie dem Portal hinzugefügt haben, bei Ihrem neuen Portal an.

So melden Sie sich bei einem Portal an

1. Wählen Sie auf der Seite Portale den Link Ihres neuen Portals aus, um das Portal in einer neuen Registerkarte zu öffnen.



2. Wenn Sie zu Beginn des Tutorials Ihren ersten IAM Identity Center-Benutzer erstellt haben, gehen Sie wie folgt vor, um ein Passwort für Ihren Benutzer zu erstellen:

   a. Überprüfen Sie Ihre E-Mail nach der Betreffzeile Invitation to join AWS IAM Identity Center.

   b. Öffnen Sie diese Einladungs-E-Mail und wählen Sie Accept invitation aus.

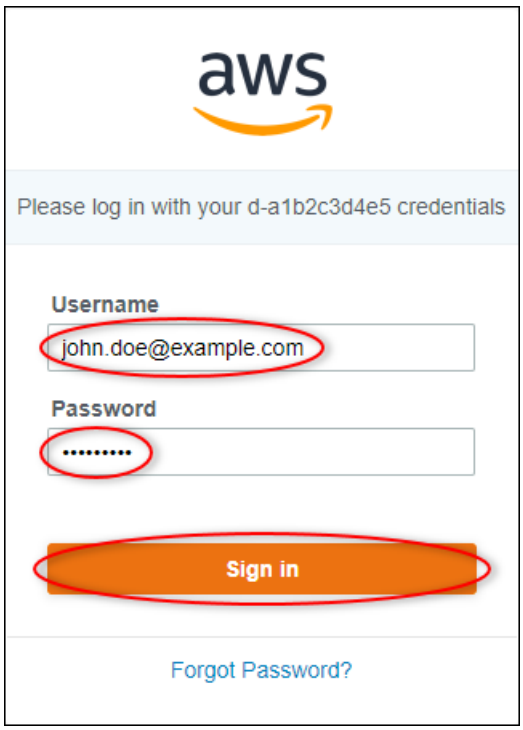
   c. Legen Sie im neuen Fenster ein Passwort für Ihren IAM Identity Center-Benutzer fest.

   Wenn Sie sich später als zweiter und dritter IAM Identity Center-Benutzer, den Sie zuvor erstellt haben, am Portal anmelden möchten, können Sie auch diese Schritte ausführen, um Passwörter für diese Benutzer festzulegen.

   > **Note**
   >
   > Wenn Sie keine E-Mail erhalten haben, können Sie in der IAM Identity Center-Konsole ein Passwort für Ihren Benutzer generieren. Weitere Informationen finden Sie unter Benutzerpasswort zurücksetzen im AWS IAM Identity Center Benutzerhandbuch.

3. Geben Sie Ihr IAM Identity Center ein Usernameund Password. Wenn Sie Ihren IAM Identity Center-Benutzer zu einem früheren Zeitpunkt in diesem Tutorial erstellt haben, Usernameist dies die E-Mail-Adresse des Portal-Administratorbenutzers, den Sie erstellt haben.

   Alle Portalbenutzer, einschließlich des Portaladministrators, müssen sich mit ihren IAM Identity Center-Benutzeranmeldedaten anmelden. Diese Anmeldeinformationen sind in der Regel nicht mit den Anmeldeinformationen identisch, mit denen Sie sich bei der AWS Management Console anmelden.



4. Wählen Sie Sign in.

   Ihr Portal wird geöffnet.

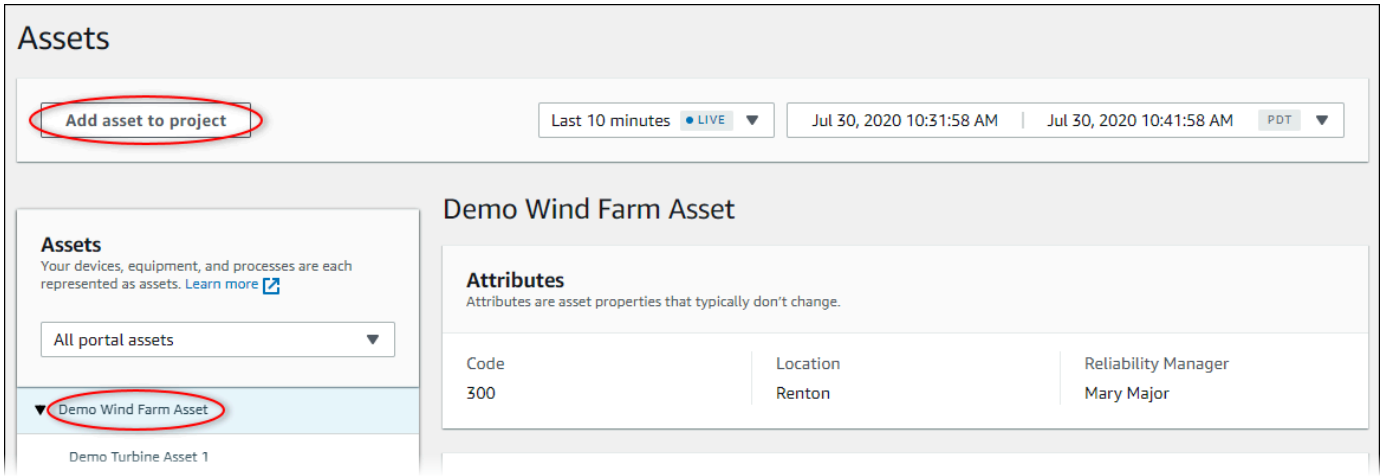
Schritt 3: Erstellen Sie ein Windparkprojekt

In diesem Verfahren erstellen Sie ein Projekt in Ihrem Portal. Projekte sind Ressourcen, die eine Reihe von Berechtigungen, Ressourcen und Dashboards definieren, die Sie konfigurieren können, um Asset-Daten in diesem Projekt zu visualisieren. Mit Projekten definieren Sie, wer Zugriff auf welche Teilmengen Ihrer Operation hat und wie die Daten dieser Teilmengen visualisiert werden. Sie können Portalbenutzer als Eigentümer oder Betrachter für jedes Projekt zuweisen. Projekteigentümer können Dashboards erstellen, um Daten zu visualisieren und das Projekt mit anderen Benutzern zu teilen. Projektbetrachter können Dashboards anzeigen, sie aber nicht bearbeiten. Weitere Informationen zu Rollen in SiteWise Monitor finden Sie unterSiteWise Rollen überwachen.

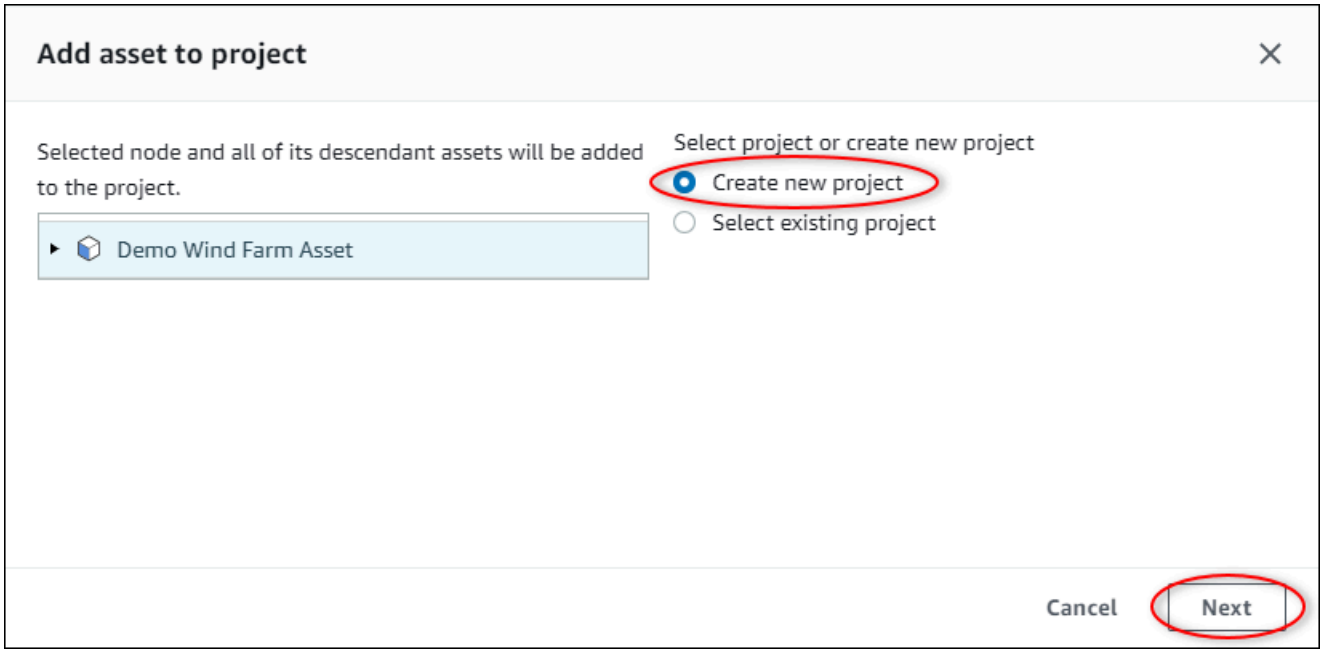
So erstellen Sie ein Windparkprojekt

1. Wählen Sie im linken Navigationsbereich Ihres Portals die Registerkarte Assets aus. Auf der Seite Assets können Sie alle im Portal verfügbaren Assets erkunden und Assets zu Projekten hinzufügen.

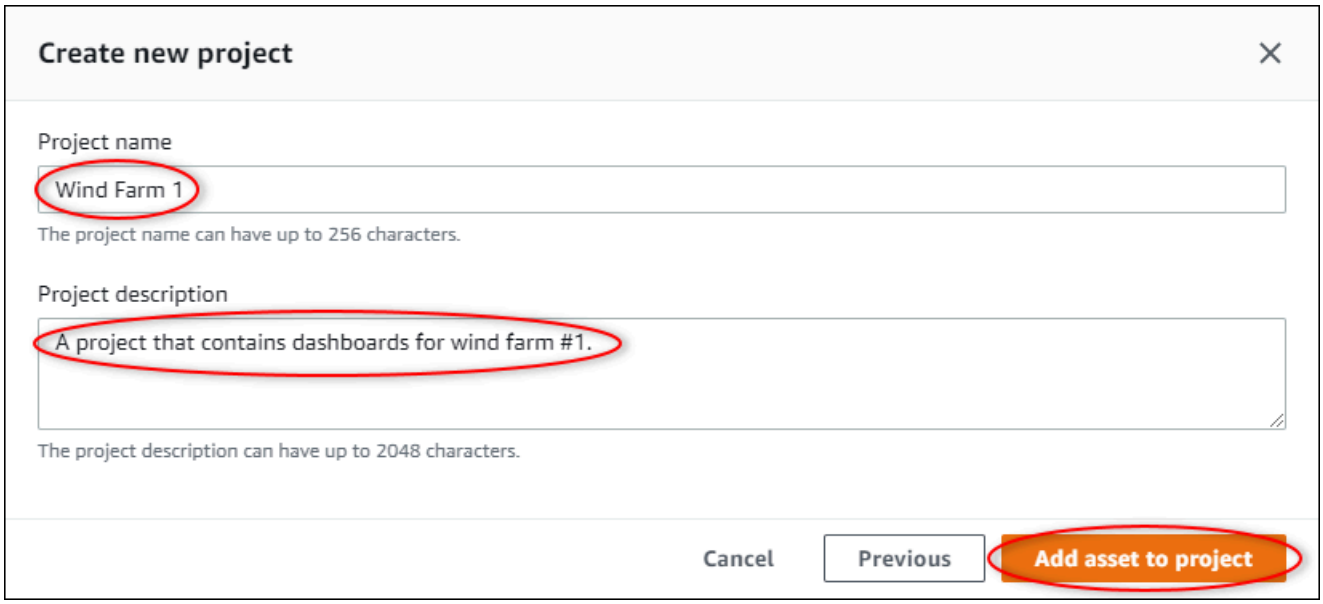
2. Wählen Sie im Komponentenbrowser die Option Demo Wind Farm Asset aus. Wenn Sie ein Asset auswählen, können Sie die aktuellen und historischen Daten dieses Assets untersuchen. Sie können auch drückenShift, um mehrere Vermögenswerte auszuwählen und deren Daten zu vergleichen side-by-side.
3. Wählen Sie oben links die Option Asset zum Projekt hinzufügen aus. Projekte enthalten Dashboards, die Ihre Portalbenutzer anzeigen können, um Ihre Daten zu erkunden. Jedes Projekt hat Zugriff auf eine Teilmenge Ihrer Ressourcen in AWS IoT SiteWise. Wenn Sie einem Projekt eine Komponente hinzufügen, können alle Benutzer mit Zugriff auf dieses Projekt auch auf Daten für diese Komponente und ihre untergeordneten Elemente zugreifen.



4. Wählen Sie im Dialogfeld „Objekt zum Projekt hinzufügen“ die Option „Neues Projekt erstellen“ und anschließend „Weiter“.



5. Geben Sie im Dialogfeld Neues Projekt erstellen einen Projektnamen und eine Projektbeschreibung für Ihr Projekt ein und wählen Sie dann Asset zum Projekt hinzufügen.



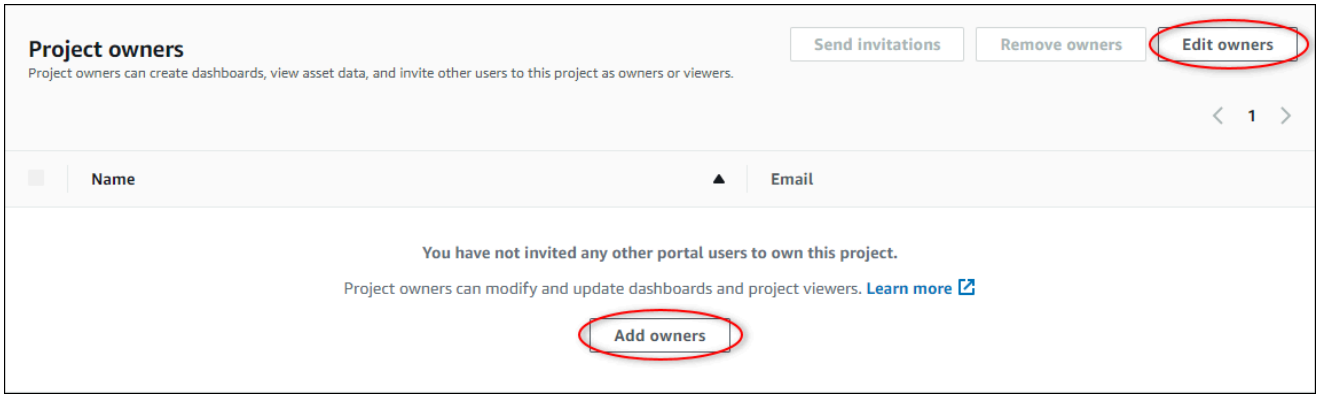
Die Seite Ihres neuen Projekts wird geöffnet.

6. Auf der Projektseite können Sie Portalbenutzer als Eigentümer oder Betrachter dieses Projekts hinzufügen.

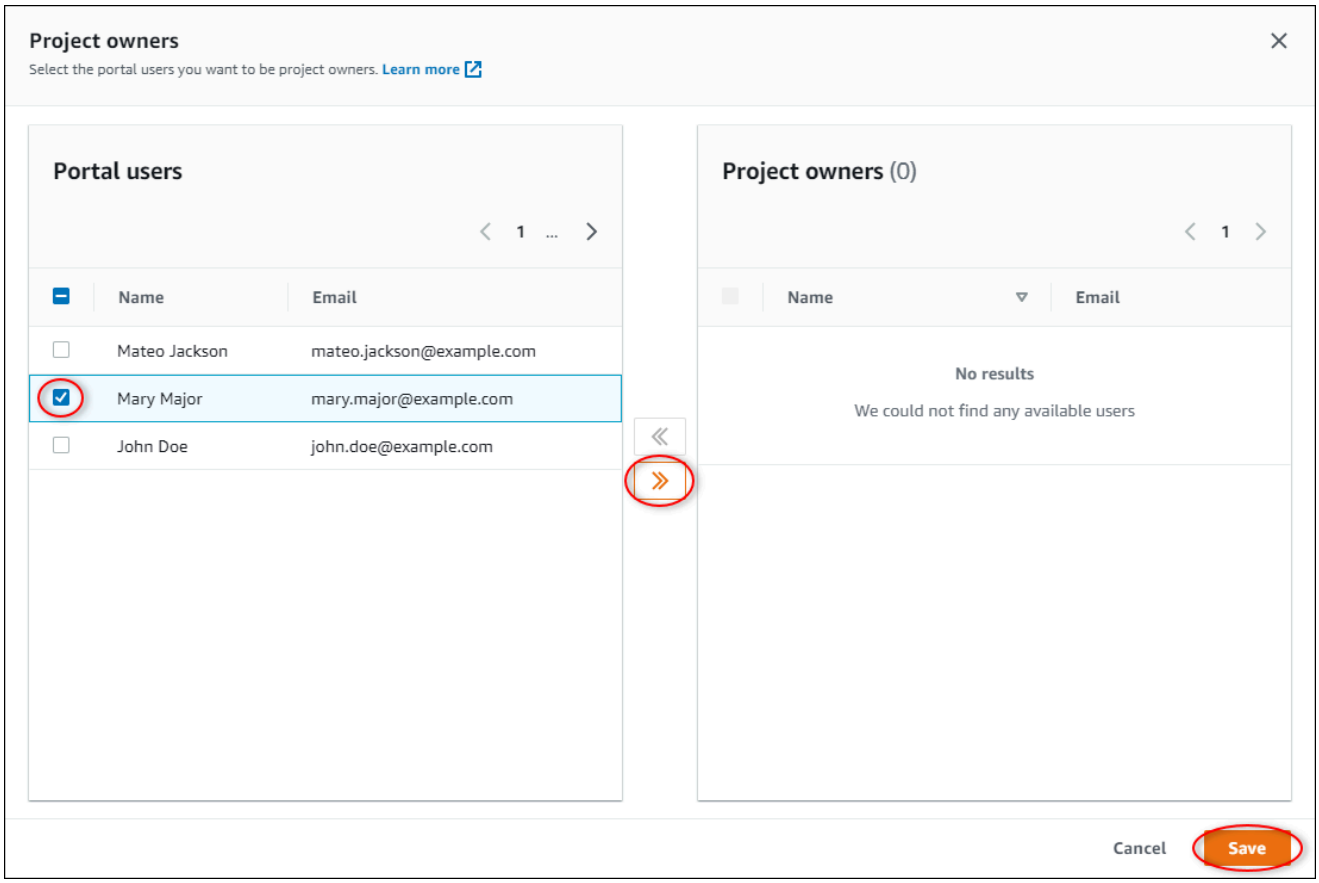
> **Note**
>
> Wenn Sie nicht bei Ihrem AWS Organizations Verwaltungskonto angemeldet sind, haben Sie möglicherweise keine Portalbenutzer, die Sie diesem Projekt zuweisen können. Sie können diesen Schritt also überspringen.

Gehen Sie auf dieser Seite wie folgt vor:

a. Wählen Sie unter Projektinhaber die Option Eigentümer hinzufügen oder Benutzer bearbeiten aus.



b. Wählen Sie den Benutzer, der als Projekteigentümer hinzugefügt werden soll (z. B. Mary Major), und dann das Symbol >> aus.



c. Wählen Sie Speichern.

Ihr IAM Identity Center-Benutzer Mary Majorkann sich bei diesem Portal anmelden, um die Dashboards in diesem Projekt zu bearbeiten und dieses Projekt mit anderen Benutzern in diesem Portal zu teilen.

d. Wählen Sie unter Projekt-Viewer die Option Zuschauer hinzufügen oder Benutzer bearbeiten aus.

e. Wählen Sie den Benutzer aus, der als Projektbetrachter hinzugefügt werden soll (z. B. Mateo Jackson), und wählen Sie dann das Symbol **>>**.

f. Wählen Sie Speichern.

Ihr IAM Identity Center-Benutzer Mateo Jacksonkann sich bei diesem Portal anmelden, um die Dashboards im Windparkprojekt anzusehen, aber nicht zu bearbeiten.

Schritt 4: Erstellen Sie ein Dashboard zur Visualisierung von Windparkdaten

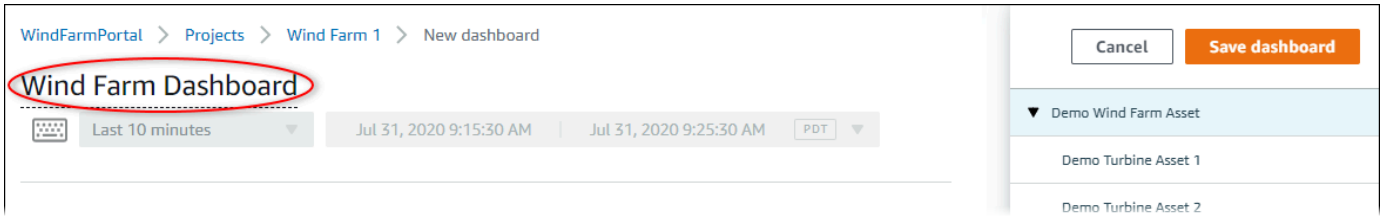
In diesem Verfahren erstellen Sie Dashboards, um die Demo-Windparkdaten zu visualisieren. Dashboards enthalten anpassbare Visualisierungen der Komponentendaten Ihres Projekts. Jede Visualisierung kann einen anderen Typ haben, z. B. ein Liniendiagramm, ein Balkendiagramm oder eine KPI-Anzeige (Key Performance Indicator). Sie können den Visualisierungstyp auswählen, der für Ihre Daten am besten geeignet ist. Projekteigentümer können Dashboards bearbeiten, wohingegen Projektbetrachter nur Dashboards anzeigen können, um Einblicke zu gewinnen.

So erstellen Sie ein Dashboard mit Visualisierungen

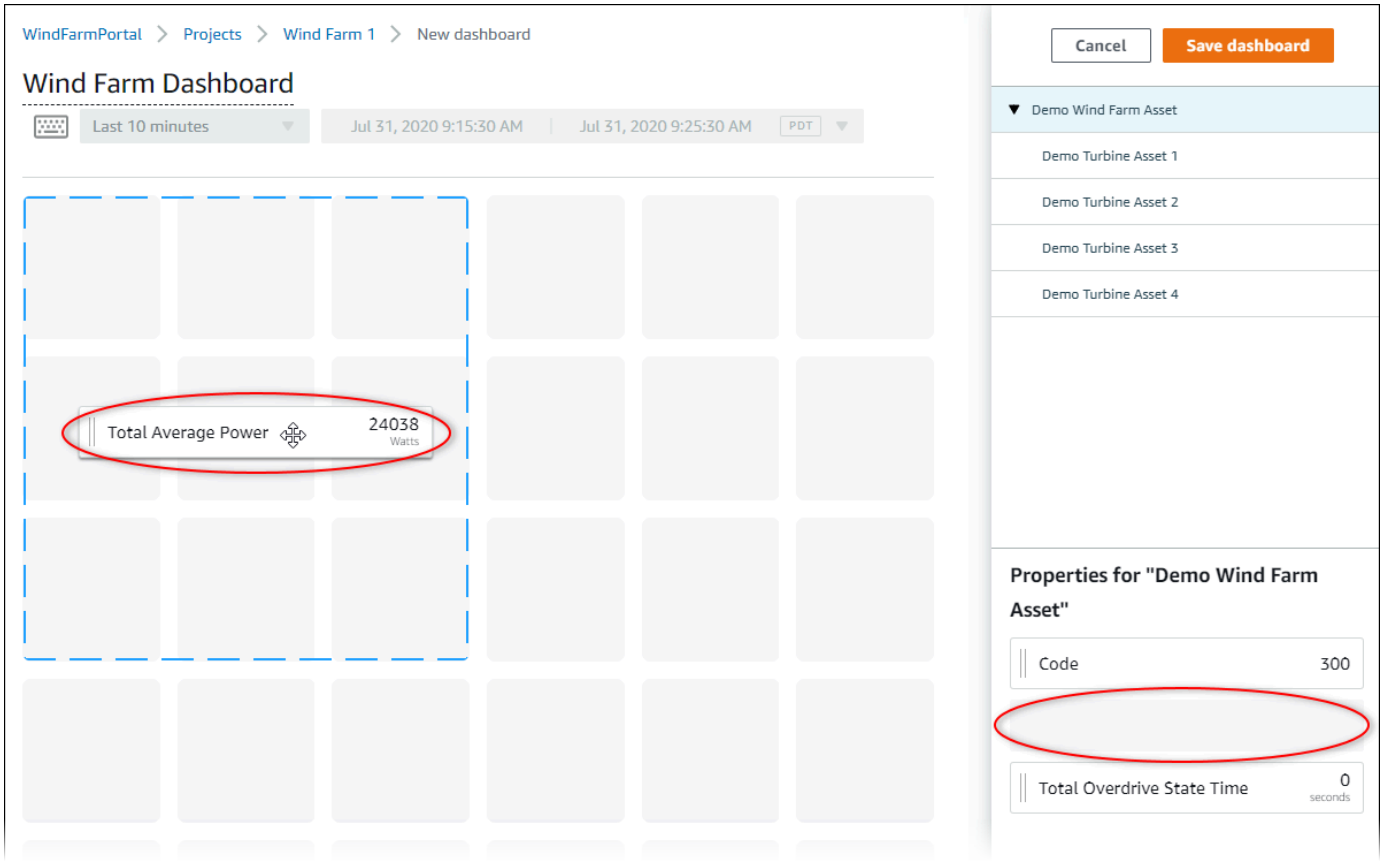
1. Wählen Sie auf der Seite Ihres neuen Projekts die Option Dashboard erstellen aus, um ein Dashboard zu erstellen und dessen Bearbeitungsseite zu öffnen.

   Auf der Bearbeitungsseite eines Dashboards können Sie Komponenteneigenschaften aus der Komponentenhierarchie in das Dashboard ziehen, um Visualisierungen zu erstellen. Anschließend können Sie Titel, Legendentitel, Typ, Größe und Position jeder Visualisierung im Dashboard bearbeiten.

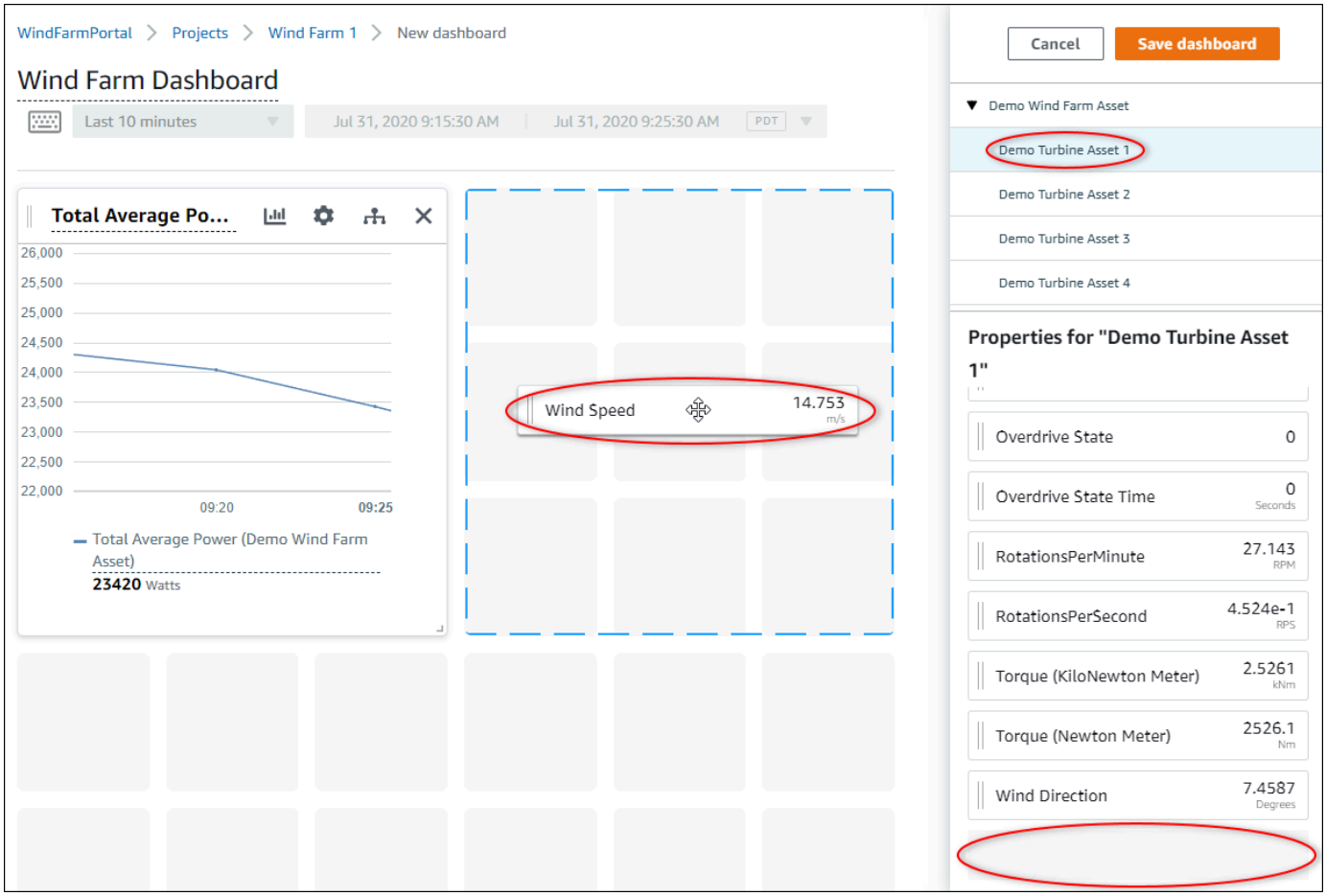
2. Geben Sie einen Namen für Ihr Dashboard ein.



3. Ziehen Sie Total Average Power von der Demo Wind Farm Asset in das Dashboard, um eine Visualisierung zu erstellen.

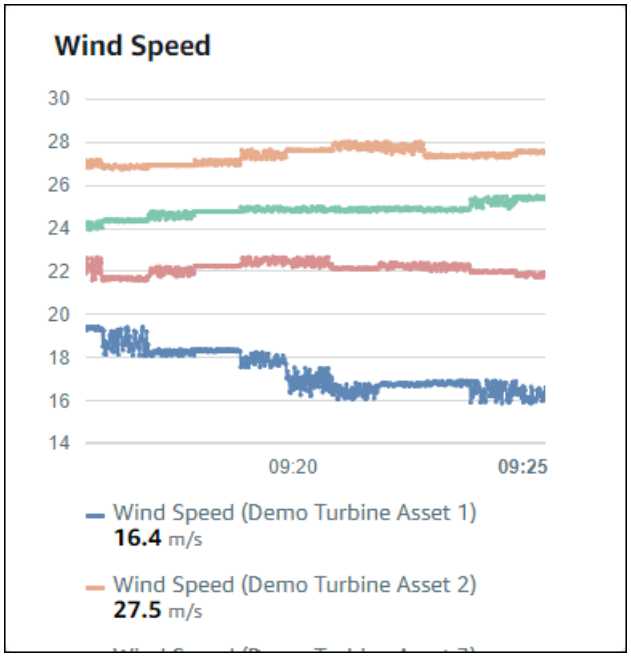


4. Wählen Demo Turbine Asset 1Sie aus, ob die Eigenschaften für diese Anlage angezeigt werden sollen, und ziehen Sie sie dann Wind Speedauf das Dashboard, um eine Visualisierung für die Windgeschwindigkeit zu erstellen.

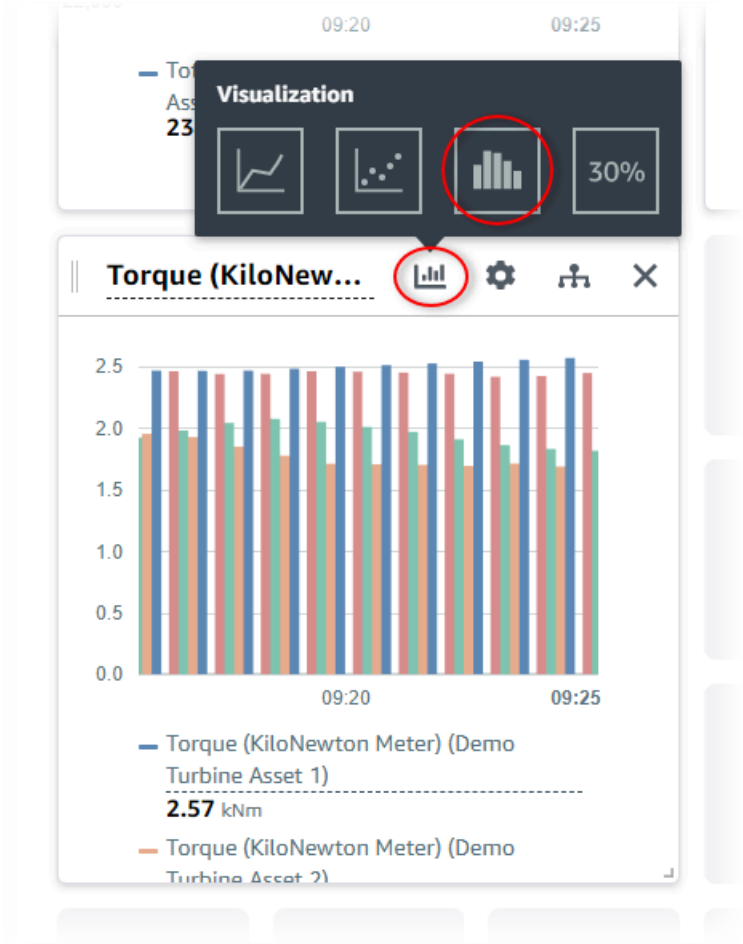


5. Fügen Sie Wind Speed der neuen Visualisierung der Windgeschwindigkeit für jede Demo Turbine Asset 2, 3 und 4 (in dieser Reihenfolge) hinzu.

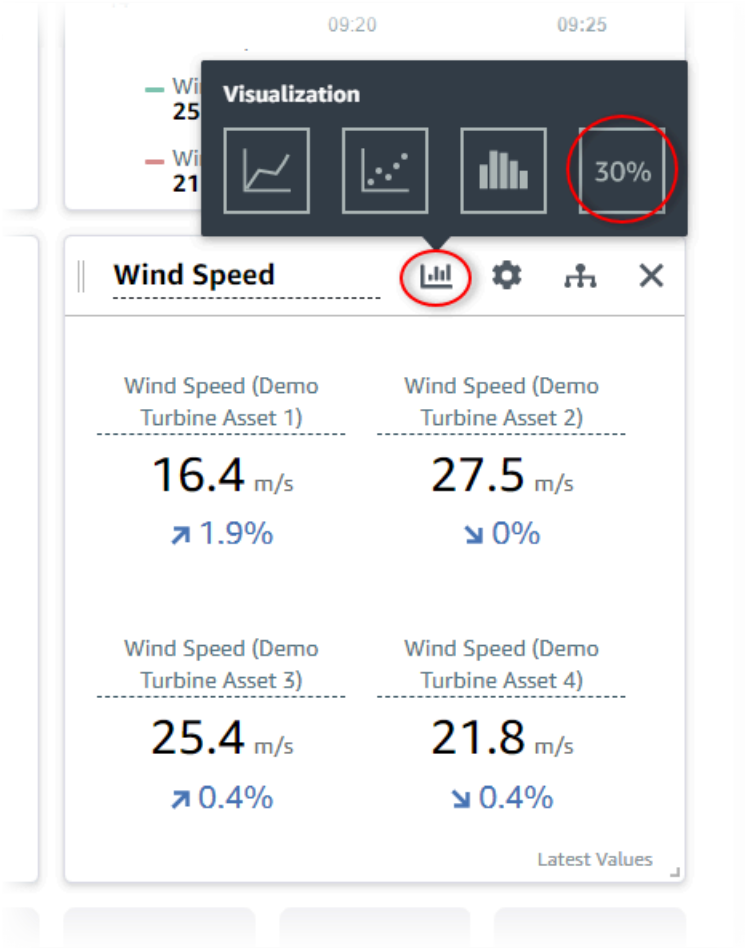
   Ihre Wind Speed-Visualisierung sollte dem folgenden Screenshot ähnlich aussehen.



6. Wiederholen Sie die Schritte 4 und 5 für die Torque (KiloNewton Meter)Eigenschaften der Windturbinen, um eine Visualisierung für das Drehmoment der Windturbine zu erstellen.
7. Wählen Sie das Symbol für den Visualisierungstyp für die Torque (KiloNewton Meter)-Visualisierung und dann das Balkendiagrammsymbol aus.

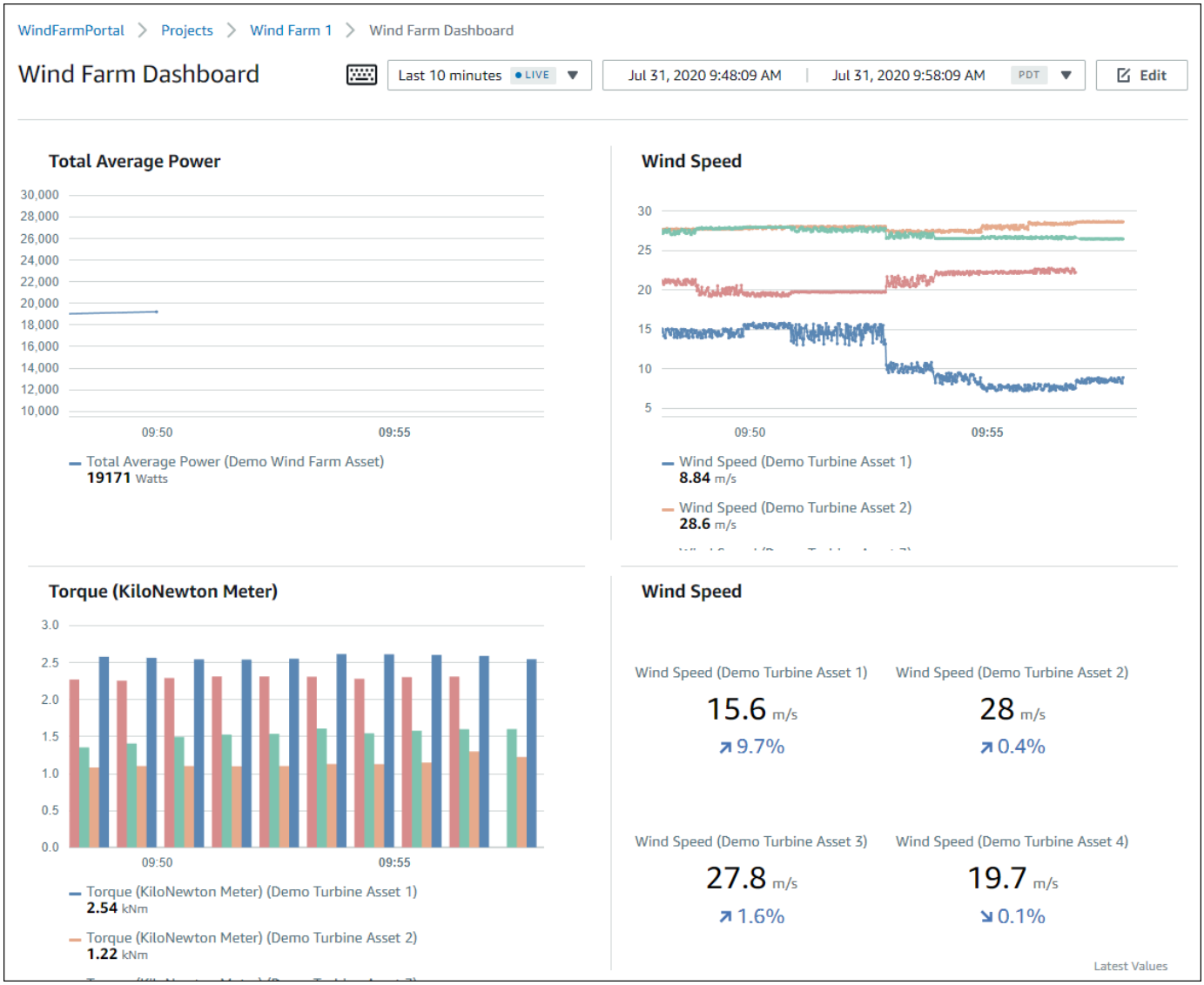


8. Wiederholen Sie die Schritte 4 und 5 für die Wind DirectionEigenschaften der Windturbinen, um eine Visualisierung der Windrichtung zu erstellen.
9. Wählen Sie das Symbol für den Visualisierungstyp für die Wind Direction-Visualisierung und dann das KPI-Diagrammsymbol (30%) aus.



10. (Optional) Nehmen Sie nach Bedarf weitere Änderungen an Titel, Legendentitel, Typ, Größe und Position der Visualisierung vor.
11. Wählen Sie oben rechts Dashboard speichern, um Ihr Dashboard zu speichern.

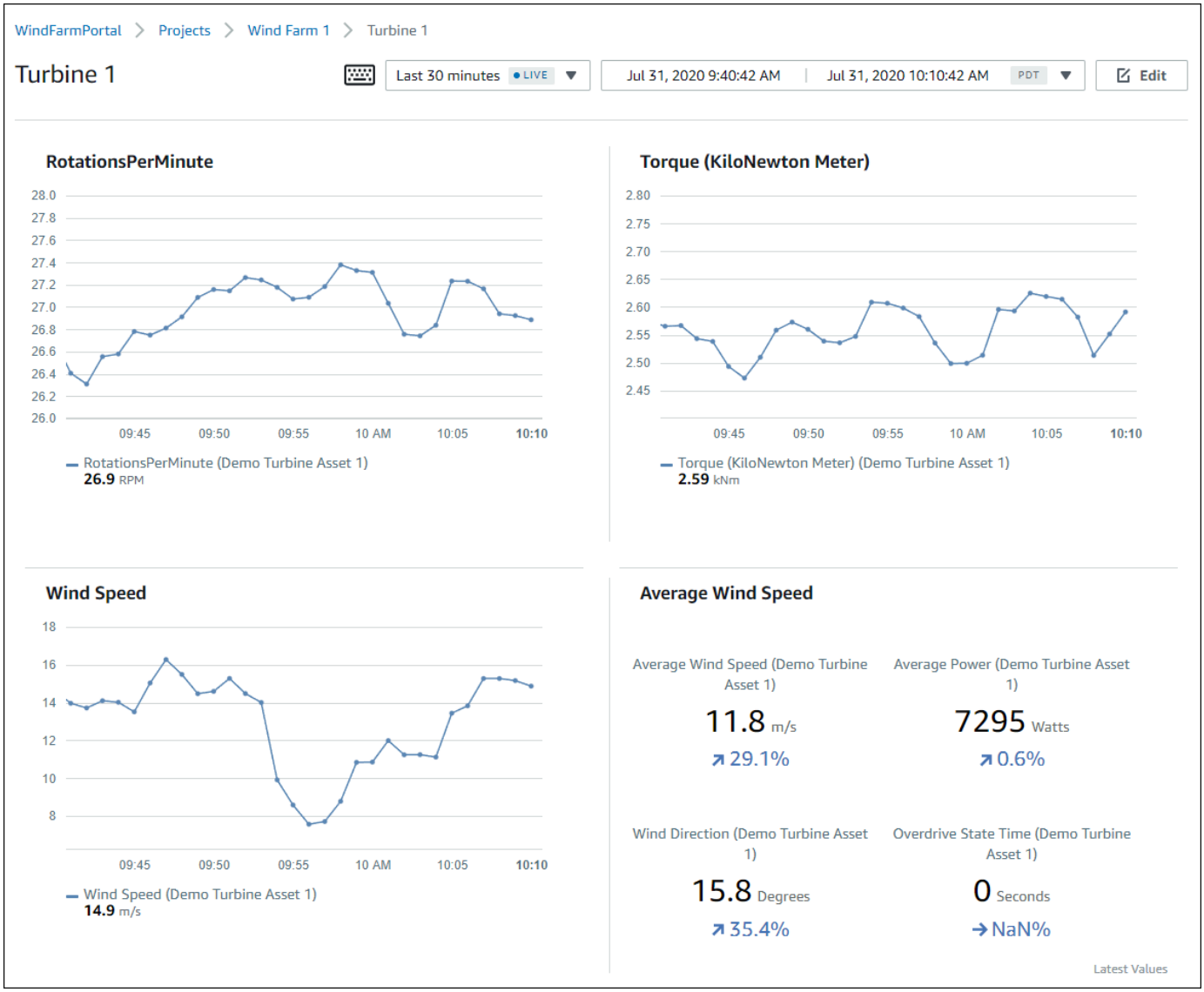
    Ihr Dashboard sollte dem folgenden Screenshot ähnlich aussehen.



12. (Optional) Erstellen Sie für jede Windkraftanlagen-Komponente ein zusätzliches Dashboard.

    Als bewährte Methode empfehlen wir, für jede Komponente ein Dashboard zu erstellen, damit Ihre Projektbetrachter alle Probleme mit den einzelnen Komponenten untersuchen können. Sie können jeder Visualisierung nur bis zu 5 Komponenten hinzufügen. Daher müssen Sie in vielen Szenarien mehrere Dashboards für Ihre hierarchischen Komponenten erstellen.

    Ein Dashboard für eine Demo-Windkraftanlage könnte ähnlich dem folgenden Screenshot aussehen.



13. (Optional) Ändern Sie die Zeitachse oder wählen Sie Datenpunkte in einer Visualisierung aus, um die Daten im Dashboard zu erkunden. Weitere Informationen finden Sie im AWS IoT SiteWise Monitor Anwendungsleitfaden unter Dashboards anzeigen.

Schritt 5: Erkunden Sie das Portal

In diesem Verfahren können Sie das Portal als Benutzer mit weniger Berechtigungen als ein AWS IoT SiteWise Portaladministrator erkunden.

Um das Portal zu erkunden und das Tutorial zu beenden

- (Optional) Wenn Sie dem Projekt weitere Benutzer als Eigentümer oder Betrachter hinzugefügt haben, können Sie sich als diese Benutzer beim Portal anmelden. Auf diese Weise können Sie das Portal als Benutzer mit weniger Berechtigungen als ein Portaladministrator erkunden.

  > **Important**
  >
  > Ihnen wird für jeden Benutzer, der sich bei einem Portal anmeldet, eine Gebühr berechnet. Weitere Informationen finden Sie unter AWS IoT SiteWise -Preisgestaltung.

  Gehen Sie wie folgt vor, um das Portal als andere Benutzer zu erkunden:

  a. Wählen Sie unten links im Portal Abmelden aus, um die Webanwendung zu beenden.
  b. Wählen Sie oben rechts im IAM Identity Center-Anwendungsportal Abmelden, um sich von Ihrem IAM Identity Center-Benutzer abzumelden.
  c. Melden Sie sich beim Portal als der IAM Identity Center-Benutzer an, den Sie als Projektinhaber oder Projektbetrachter zugewiesen haben. Weitere Informationen finden Sie unter Schritt 2: Melden Sie sich bei einem Portal an.

Sie haben das Tutorial abgeschlossen. Wenn Sie mit der Erkundung Ihres Demo-Windparks in SiteWise Monitor fertig sind, folgen Sie dem nächsten Verfahren, um Ihre Ressourcen zu bereinigen.

Schritt 6: Bereinigen Sie die Ressourcen nach dem Tutorial

Nachdem Sie das Tutorial abgeschlossen haben, können Sie Ihre Ressourcen bereinigen. Es fallen keine Gebühren für AWS IoT SiteWise an, wenn sich Benutzer nicht bei Ihrem Portal anmelden, aber Sie können Ihr Portal und Ihre AWS-IAM-Identity-Center-Verzeichnis -Benutzer löschen. Ihre Demo-Windparkkomponenten werden am Ende der Dauer gelöscht, die Sie beim Erstellen der Demo gewählt haben, oder Sie können die Demo manuell löschen. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo löschen.

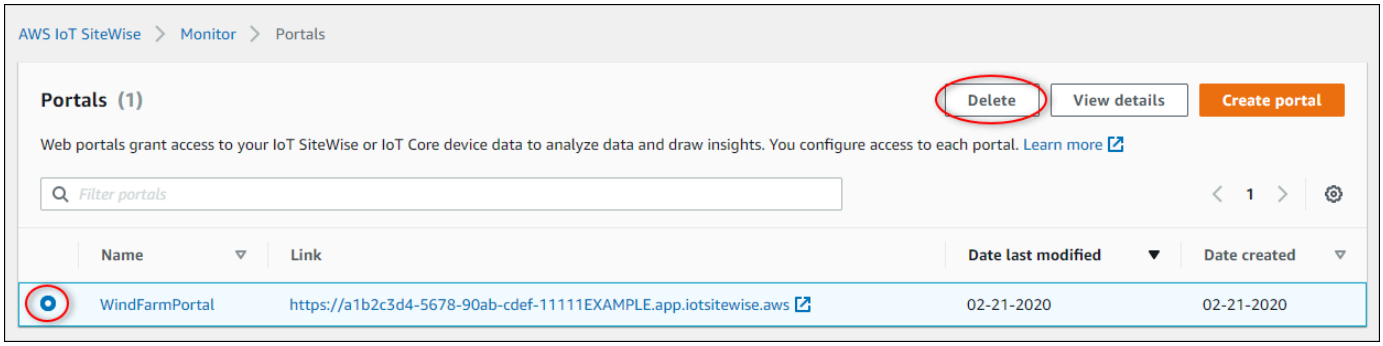
Gehen Sie wie folgt vor, um Ihre Portal- und IAM Identity Center-Benutzer zu löschen.

So löschen Sie ein Portal

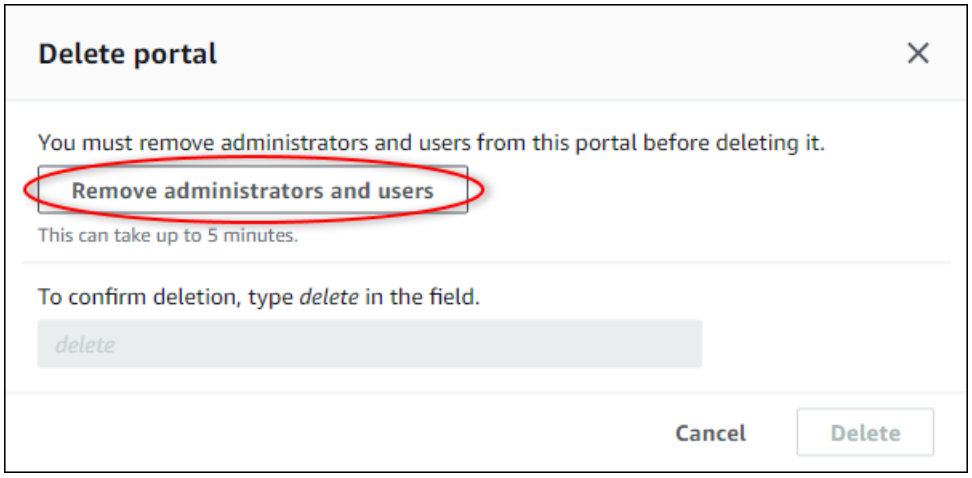
1. Navigieren Sie zur AWS IoT SiteWise -Konsole.

2. Wählen Sie im linken Navigationsbereich die Option Portale aus.
3. Wählen Sie Ihr Portal WindFarmPortalund anschließend Löschen aus.

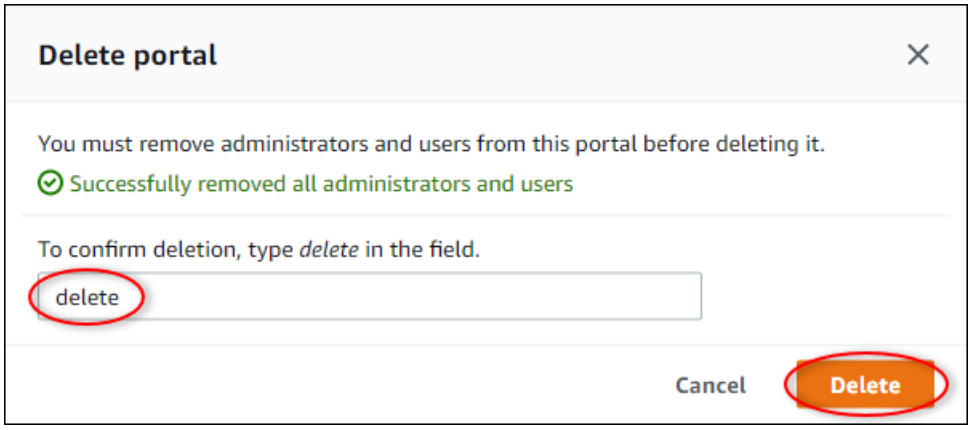
   Wenn Sie ein Portal oder ein Projekt löschen, sind die Komponenten, die gelöschten Projekten zugeordnet sind, nicht betroffen.



4. Wählen Sie im Dialogfeld Portal löschen die Option Administratoren und Benutzer entfernen aus.

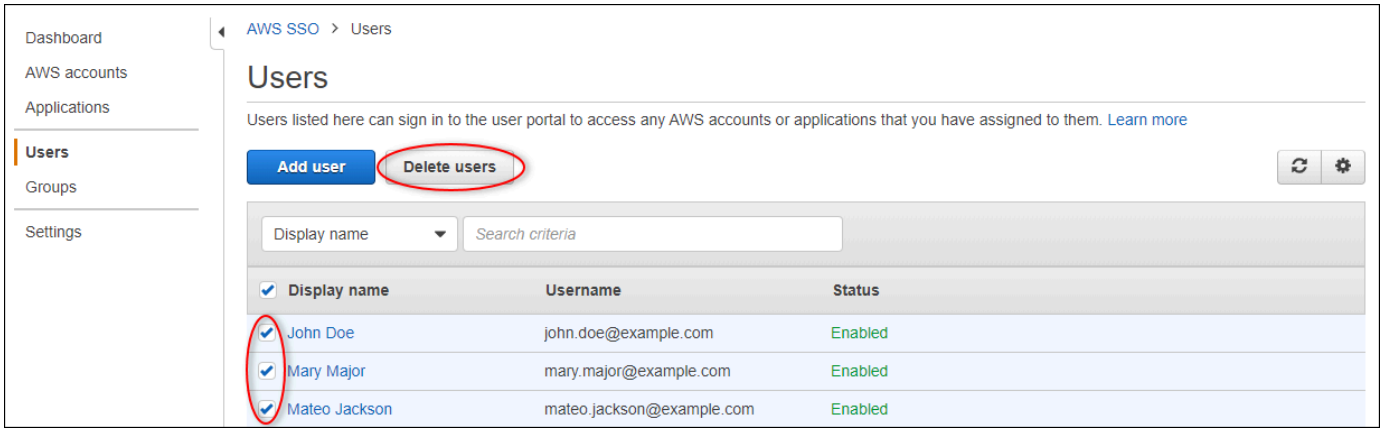


5. Geben Sie **`delete`** ein, um das Löschen zu bestätigen, und wählen Sie dann Löschen.

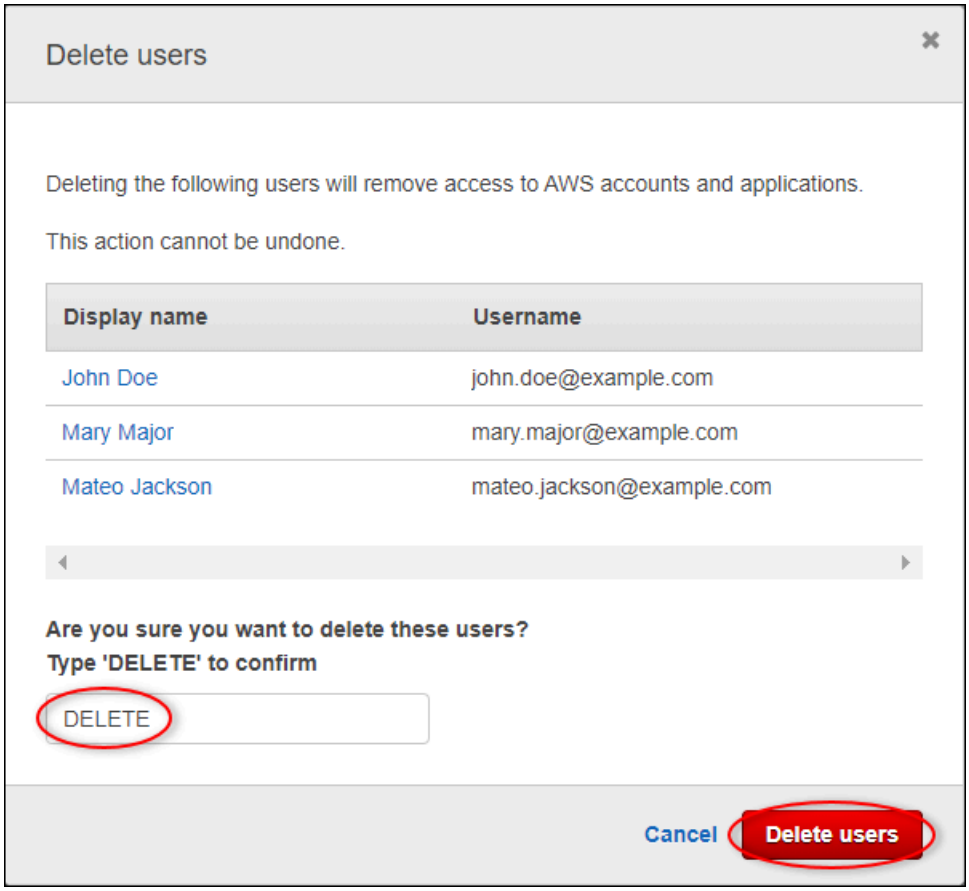


Um IAM Identity Center-Benutzer zu löschen

1. Navigieren Sie zur IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Benutzer aus.
3. Aktivieren Sie das Kontrollkästchen für jeden zu löschenden Benutzer und wählen Sie Benutzer löschen aus.



4. Geben **DELETE**Sie im Dialogfeld „Benutzer löschen“ den Text ein und wählen Sie dann Benutzer löschen aus.



Veröffentlichung von Eigenschaftswertaktualisierungen in Amazon DynamoDB

In diesem Tutorial wird eine bequeme Methode zum Speichern Ihrer Daten mithilfe von Amazon DynamoDB vorgestellt, sodass Sie einfacher auf historische Asset-Daten zugreifen können, ohne die API wiederholt abfragen zu müssen. AWS IoT SiteWise Nachdem Sie dieses Tutorial abgeschlossen haben, können Sie benutzerdefinierte Software erstellen, die Ihre Anlagendaten nutzt, z. B. eine Live-Karte der Windgeschwindigkeit und -richtung in einem gesamten Windpark. Wenn Sie Ihre Daten überwachen und visualisieren möchten, ohne eine benutzerdefinierte Softwarelösung zu implementieren, finden Sie weitere Informationen unterDaten überwachen mit AWS IoT SiteWise Monitor.

In diesem Tutorial bauen Sie auf der AWS IoT SiteWise Demo auf, die einen Beispieldatensatz für einen Windpark enthält. Sie konfigurieren Eigenschaftswertaktualisierungen aus der Windpark-Demo, um Daten über AWS IoT Kernregeln an eine von Ihnen DynamoDB DynamoDB-Tabelle zu senden. Wenn Sie Eigenschaftswertaktualisierungen aktivieren, AWS IoT SiteWise sendet Ihre Daten AWS IoT Core in MQTT-Nachrichten an. Definieren Sie dann AWS IoT Core-Regeln, die je nach Inhalt dieser Nachrichten Aktionen ausführen, z. B. die DynamoDB-Aktion. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten.

Themen

Voraussetzungen

Zum Durcharbeiten dieses Tutorials ist Folgendes erforderlich:

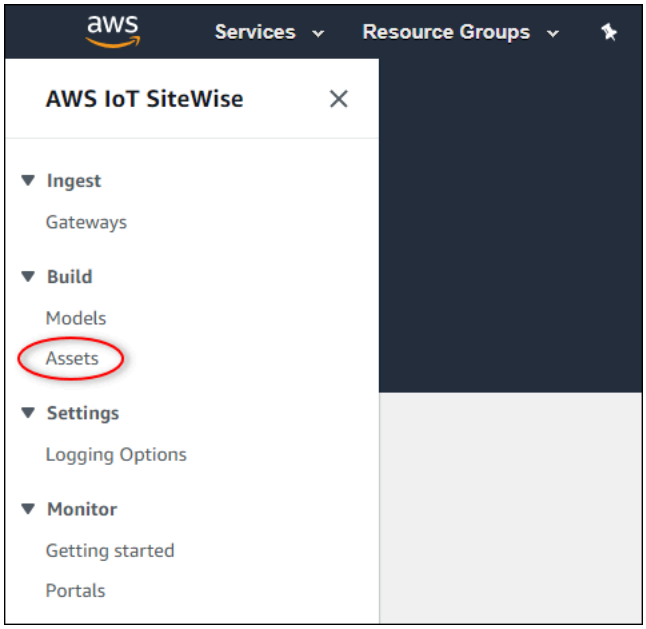
- Ein Konto AWS . Falls Sie noch keines haben, beachten Sie die Informationen unter Einrichtung eines AWS-Konto.
- Ein Entwicklungscomputer, auf dem Windows, macOS, Linux oder Unix ausgeführt wird, um auf die zuzugreifen AWS Management Console. Weitere Informationen finden Sie unter Erste Schritte mit AWS Management Console.
- Ein IAM-Benutzer mit Administratorberechtigungen.
- Eine laufende AWS IoT SiteWise Windpark-Demo. Wenn Sie die Demo einrichten, definiert sie Modelle und Anlagen AWS IoT SiteWise und streamt Daten an sie, um einen Windpark darzustellen. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo verwenden.

Schritt 1: Konfigurieren Sie AWS IoT SiteWise die Konfiguration, um Aktualisierungen von Eigenschaftswerten zu veröffentlichen

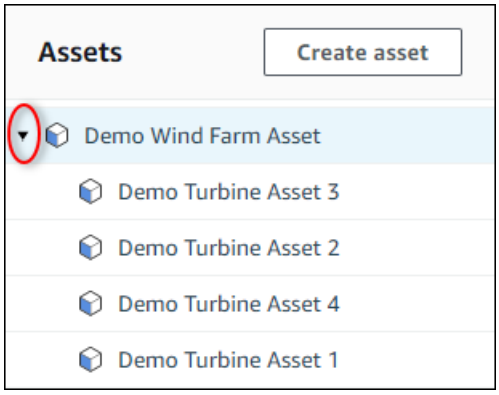
In diesem Verfahren aktivieren Sie Benachrichtigungen über Eigenschaftswerte für die Eigenschaften Wind Speed Ihrer Demo-Turbinenkomponenten. Nachdem Sie Benachrichtigungen über Eigenschaftswerte aktiviert haben, AWS IoT SiteWise veröffentlicht es jedes Wertaktupdate in einer MQTT-Nachricht in AWS IoT Core.

So aktivieren Sie Benachrichtigungen über Eigenschaftswerte für Komponenteneigenschaften:

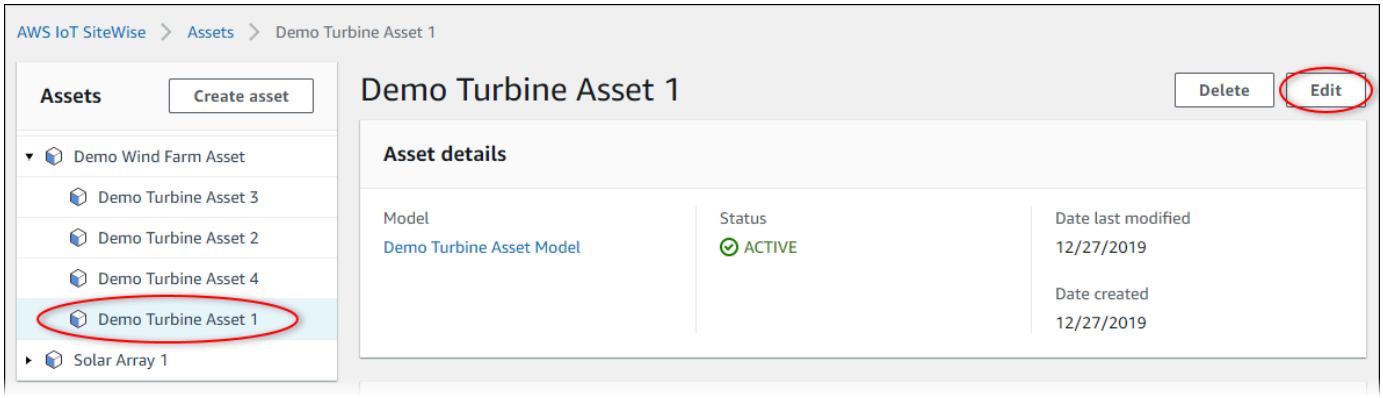
1. Melden Sie sich an der AWS IoT SiteWise -Konsole an.
2. Überprüfen Sie die AWS IoT SiteWise Endpunkte und Kontingente, auf denen dies unterstützt AWS IoT SiteWise wird, und wechseln Sie AWS gegebenenfalls zwischen den Regionen. Wechseln Sie zu einer Region, in der Sie die AWS IoT SiteWise Demo ausführen.
3. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).



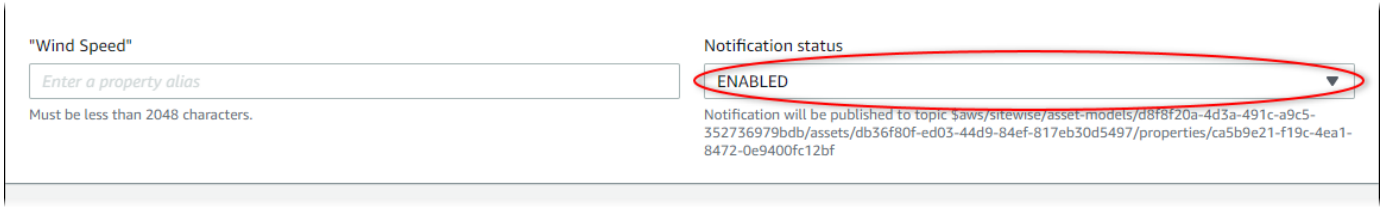
4. Wählen Sie den Pfeil neben Demo Wind Farm Asset aus, um die Hierarchie der Windparkkomponente zu erweitern.



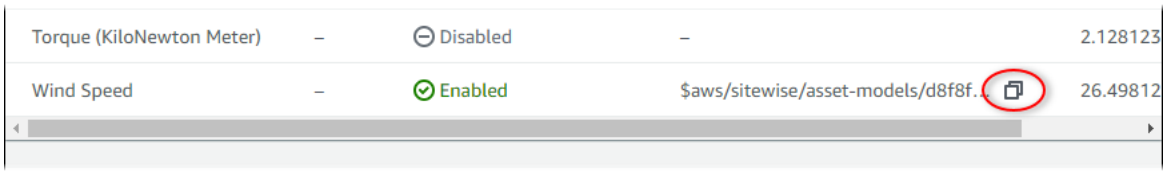
5. Wählen Sie eine Demoturbine und Edit (Bearbeiten) aus.



6. Ändern Sie den Benachrichtigungsstatus der Wind SpeedUnterkunft auf AKTIVIERT.



7. Wählen Sie unten auf der Seite die Option Save asset (Komponente speichern) aus.
8. Wiederholen Sie die Schritte 5 bis 7 für jede Demo-Turbinenkomponente.
9. Wählen Sie eine Demoturbine aus (z. B. Demo Turbine Asset 1).
10. Wählen Sie Measurements (Messungen).
11. Wählen Sie das Kopiersymbol neben der Eigenschaft Wind Speed aus, um das Benachrichtigungsthema in die Zwischenablage zu kopieren. Speichern Sie das Benachrichtigungsthema zur späteren zu verwendende Verwendung in diesem Tutorial. Sie müssen nur das Benachrichtigungsthema einer Turbine aufzeichnen.



Das Benachrichtigungsthema sollte wie im folgenden Beispiel aussehen.

```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

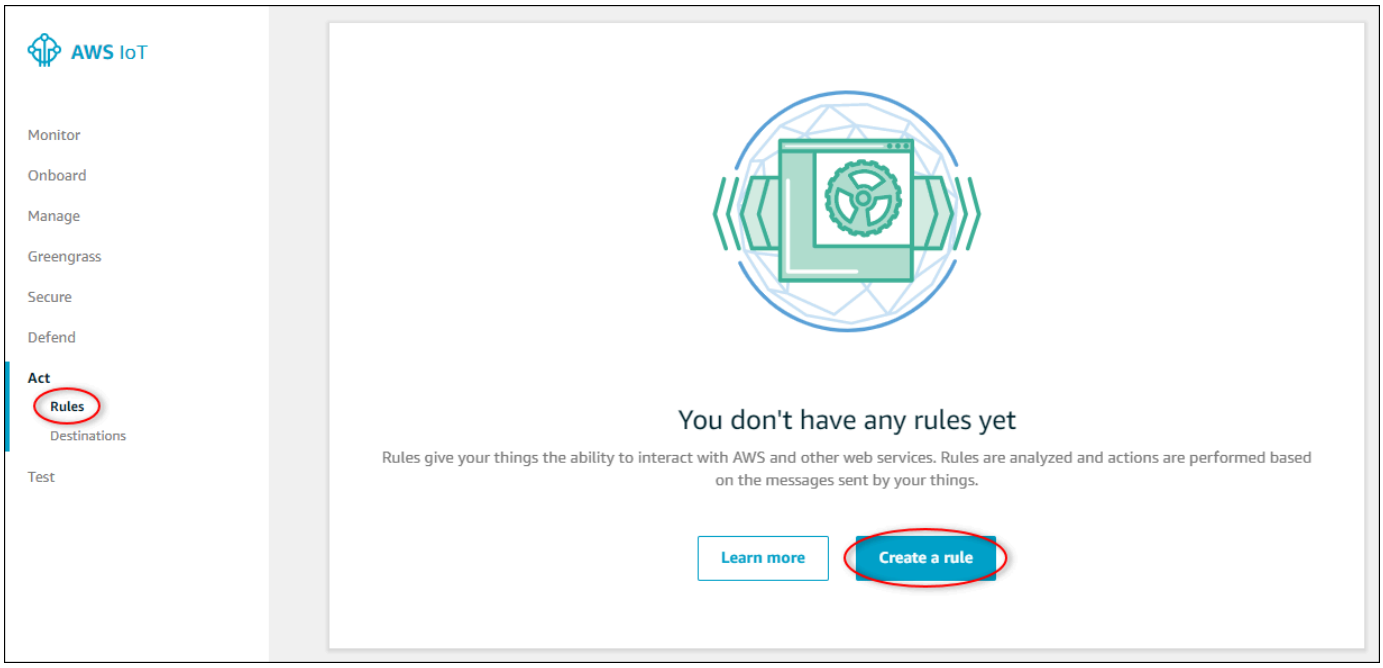
Schritt 2: Erstellen Sie eine Regel in AWS IoT Core

In diesem Verfahren erstellen Sie eine Regel in AWS IoT Core, die die Benachrichtigungen über Eigenschaftswerte analysiert und Daten in eine Amazon DynamoDB-Tabelle einfügt. AWS IoT Kernregeln analysieren MQTT-Nachrichten und führen Aktionen aus, die auf dem Inhalt und dem Thema jeder Nachricht basieren. Anschließend erstellen Sie eine Regel mit einer DynamoDB-Aktion, um Daten in eine DynamoDB-Tabelle einzufügen, die Sie im Rahmen dieses Tutorials erstellen.

So erstellen Sie eine Regel mit einer DynamoDB-Aktion

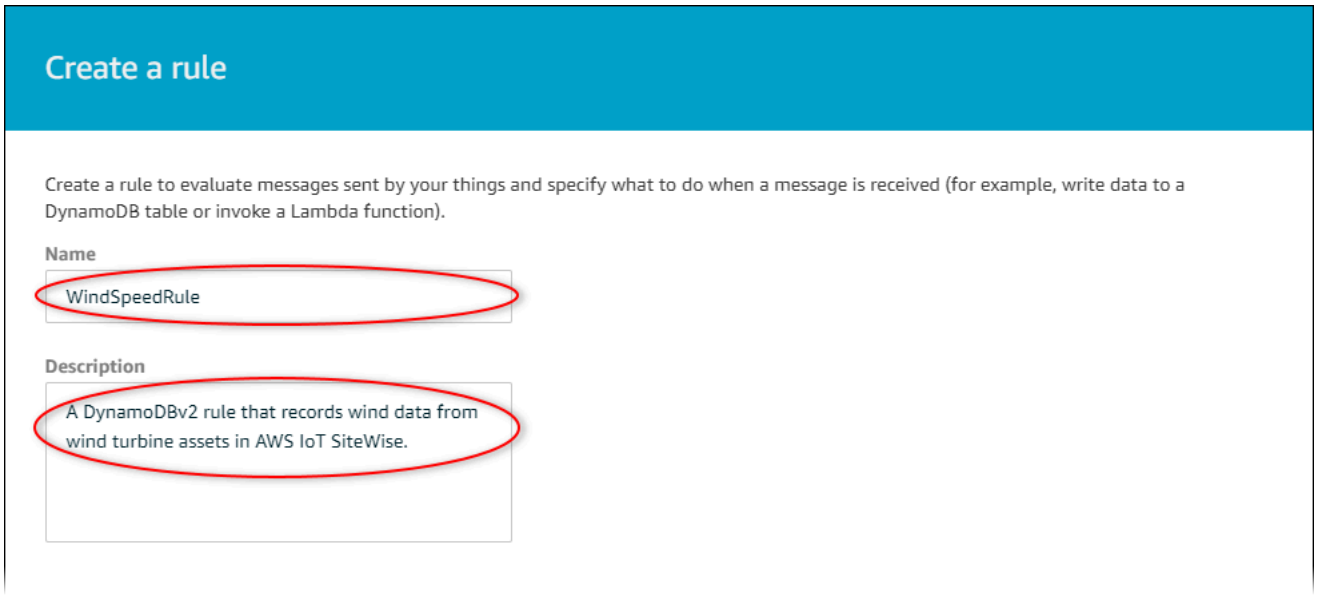
1. Navigieren Sie zur AWS IoT -Konsole. Wenn die Schaltfläche Get started (Erste Schritte) angezeigt wird, wählen Sie sie aus.

2. Wählen Sie im linken Navigationsbereich Act (Agieren) und dann Rules (Regeln) aus.



3. Wenn das Dialogfeld You don't have any rules yet (Sie haben noch keine Regeln) angezeigt wird, wählen Sie Create a rule (Regel erstellen) aus. Wählen Sie andernfalls Erstellen.

4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.



5. Suchen Sie das Benachrichtigungsthema, das Sie zuvor in diesem Tutorial gespeichert haben.

```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE
```

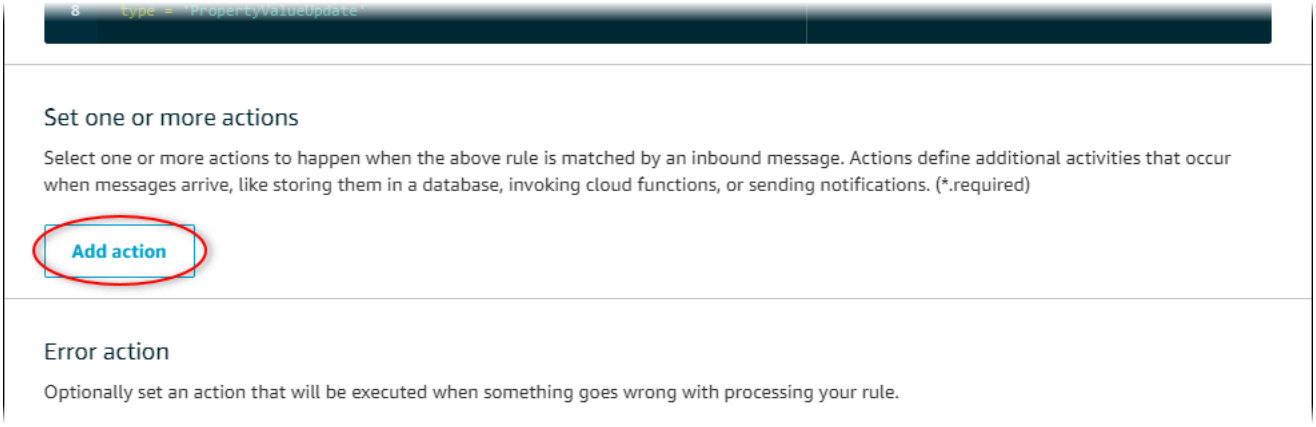
Ersetzen Sie die Asset-ID (die ID danach`assets/`) im Thema durch eine`+`. Dadurch wird die Eigenschaft Windgeschwindigkeit für alle Demo-Windturbinenanlagen ausgewählt. Der `+`-Themenfilter akzeptiert alle Knoten einer einzelnen Ebene in einem Thema. Ihr Thema sollte wie das folgende Beispiel aussehen.

```
$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE
```

6. Geben Sie die folgende Regelabfrageanweisung ein. Ersetzen Sie das Thema im `FROM`-Abschnitt durch Ihr Benachrichtigungsthema.

```
SELECT
  payload.assetId AS asset,
  (SELECT VALUE (value.doubleValue) FROM payload.values) AS windspeed,
  timestamp() AS timestamp
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

7. Wählen Sie unter Set one or more actions (Festlegen einer oder mehrerer Aktionen) die Option Add action (Aktion hinzufügen) aus.



8. Wählen Sie auf der Seite Aktion auswählen die Option Nachricht in mehrere Spalten einer DynamoDB-Tabelle aufteilen (DynamoDBv2).

9. Klicken Sie unten auf der Seite auf Configure action (Aktion konfigurieren).
10. Wählen Sie auf der Seite Configure action die Option Create a new resource.

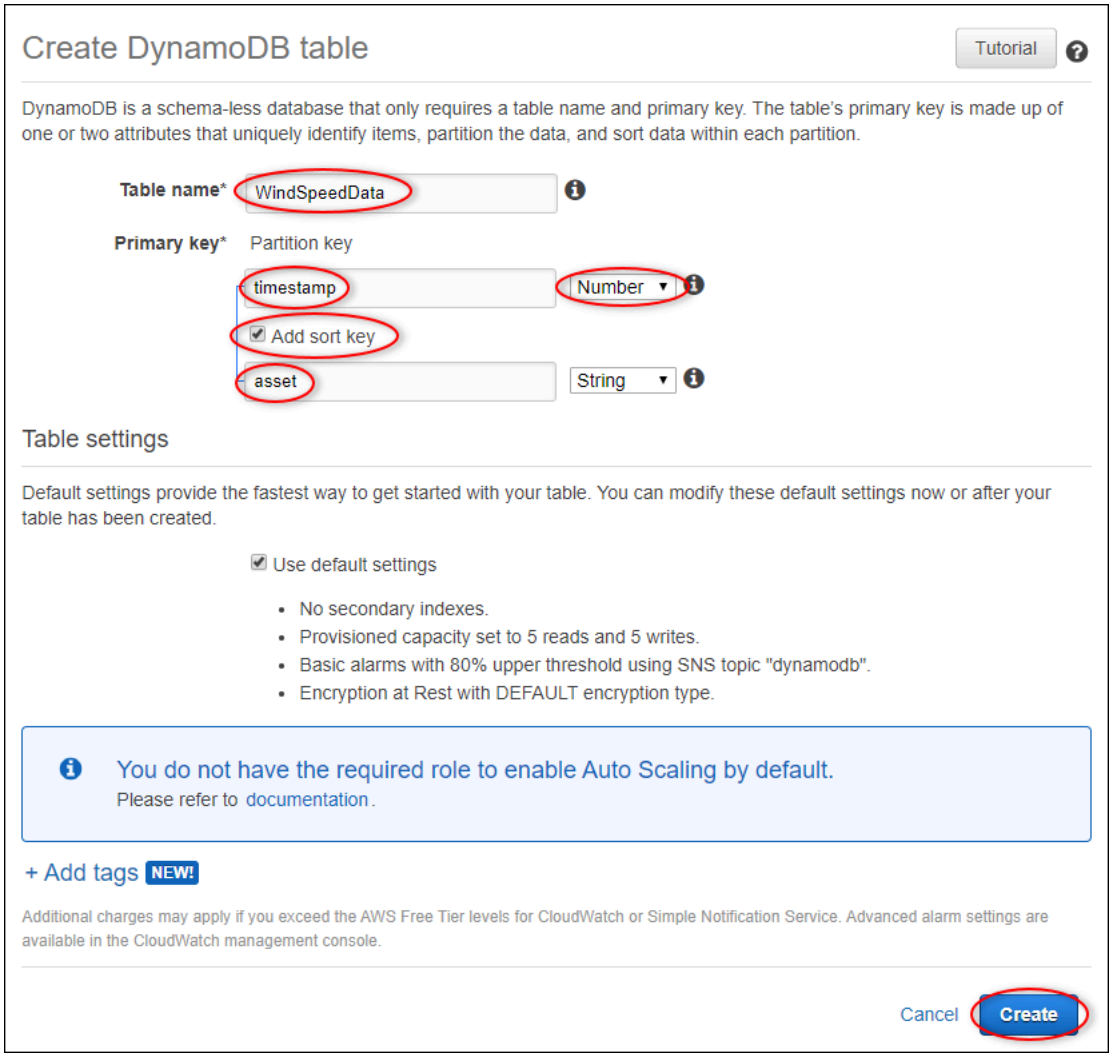
    Die DynamoDB-Konsole wird auf einer neuen Registerkarte geöffnet. Halten Sie die Registerkarte „Regelaktion“ geöffnet, während Sie die folgenden Schritte ausführen.

Schritt 3: DynamoDB-Tabelle erstellen

In diesem Verfahren erstellen Sie eine Amazon DynamoDB-Tabelle, um Windgeschwindigkeitdaten aus der Regelaktion zu empfangen.

So erstellen Sie eine DynamoDB-Tabelle

1. Wählen Sie im Dashboard der DynamoDB-Konsole die Option Tabelle erstellen aus.
2. Geben Sie einen Namen für Ihre App an.



3. Führen Sie für Primary key (Primärschlüssel) die folgenden Schritte aus:

   a. Geben Sie „**`timestamp`**“ als Partitionsschlüssel ein.

   b. Wählen Sie den Typ Number (Nummer) aus.

   c. Aktivieren Sie das Kontrollkästchen Add sort key (Sortierschlüssel hinzufügen).

   d. Geben Sie **`asset`** als Sortierschlüssel ein, und belassen Sie den Standardsortierschlüsseltyp auf String (Zeichenfolge).

4. Wählen Sie Erstellen.

   Wenn die Meldung Table is being created (Tabelle wird erstellt) nicht mehr angezeigt wird, ist Ihre Tabelle bereit.

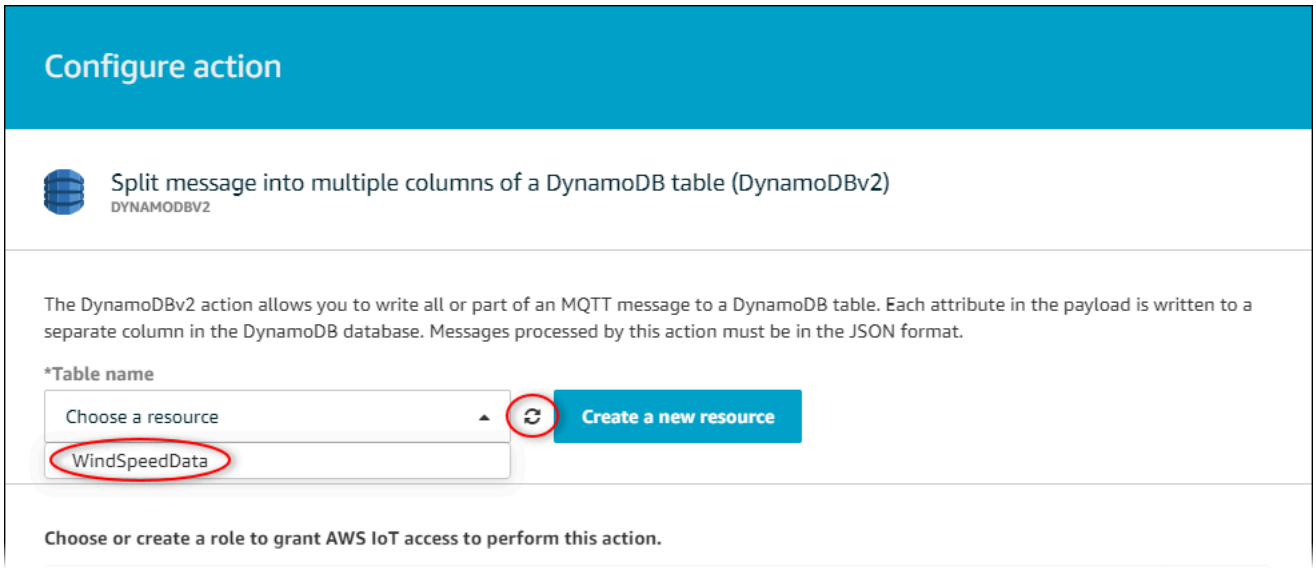
5. Kehren Sie mit der Seite Configure action (Aktion konfigurieren) zur Registerkarte zurück. Lassen Sie die Registerkarte DynamoDB geöffnet, während Sie die folgenden Verfahren ausführen.

Schritt 4: DynamoDB-Regelaktion konfigurieren

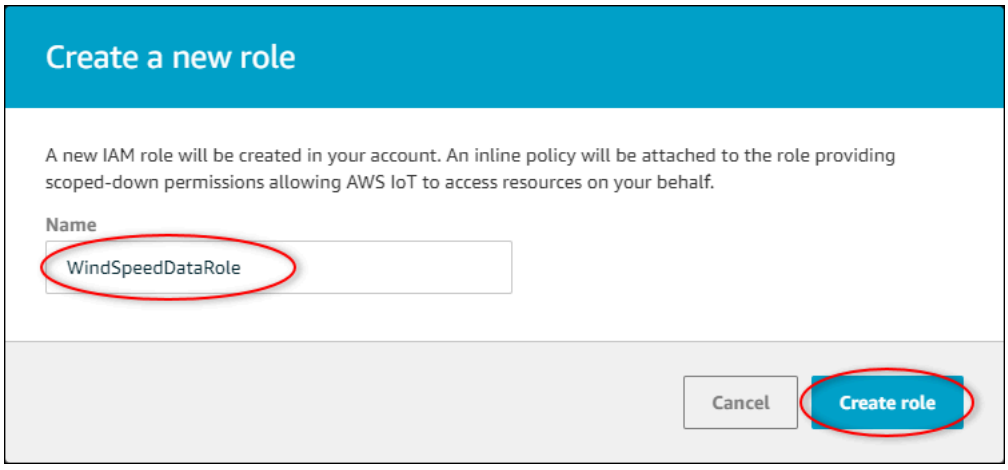
In diesem Verfahren konfigurieren Sie die Amazon DynamoDB DynamoDB-Regelaktion so, dass Daten aus Eigenschaftswertaktualisierungen in Ihre neue DynamoDB-Tabelle eingefügt werden.

So konfigurieren Sie die DynamoDB-Regelaktion

1. Aktualisieren Sie auf der Aktionsseite „Konfiguration“ die Liste mit den Tabellennamen und wählen Sie Ihre neue DynamoDB-Tabelle aus.



2. Wählen Sie „Rolle erstellen“, um eine IAM-Rolle zu erstellen, die AWS IoT Core Zugriff auf die Ausführung der Regelaktion gewährt.
3. Geben Sie einen Rollennamen ein und klicken Sie auf Create Role (Rolle erstellen).



4. Wählen Sie Aktion hinzufügen aus.

5. Wählen Sie am unteren Rand der Seite Create rule (Regel erstellen) aus, um die Regelerstellung abzuschließen.

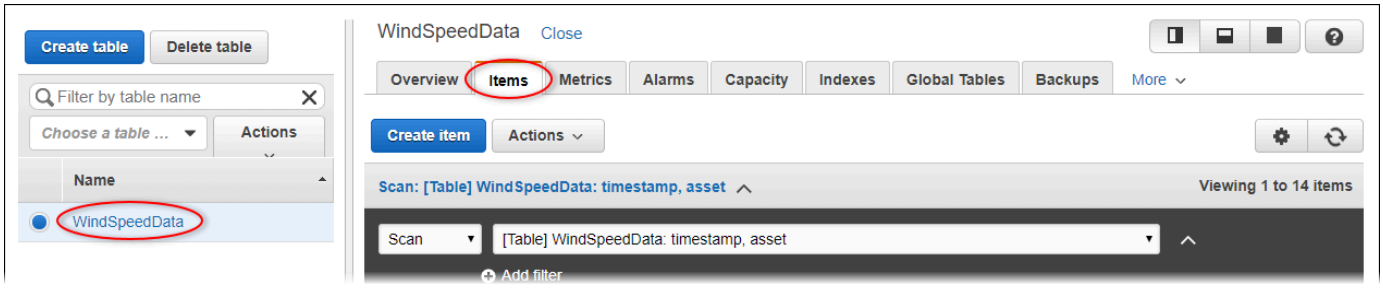
   Ihre Demo-Asset-Daten sollten nun in Ihrer DynamoDB-Tabelle erscheinen.

Schritt 5: Erkunden Sie Daten in DynamoDB

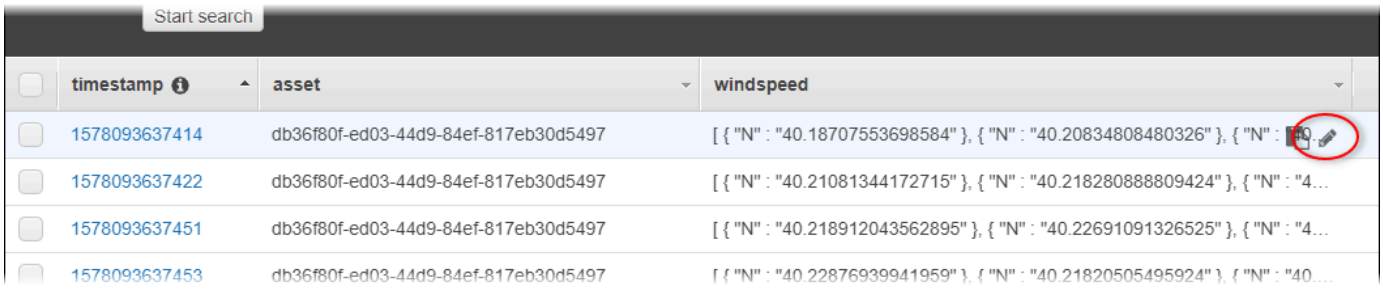
In diesem Verfahren untersuchen Sie die Windgeschwindigkeitsdaten der Demo-Assets in Ihrer neuen Amazon DynamoDB-Tabelle.

Um Asset-Daten in DynamoDB zu untersuchen

1. Kehren Sie zu der Registerkarte mit der geöffneten DynamoDB-Tabelle zurück.
2. Wählen Sie in der zuvor erstellten Tabelle die Registerkarte Items (Elemente) aus, um die Daten in der Tabelle anzuzeigen. Aktualisieren Sie die Seite, wenn keine Zeilen in der Tabelle angezeigt werden. Wenn nach einigen Minuten keine Zeilen angezeigt werden, finden Sie weitere Informationen unter Fehlerbehebung bei einer Regel.

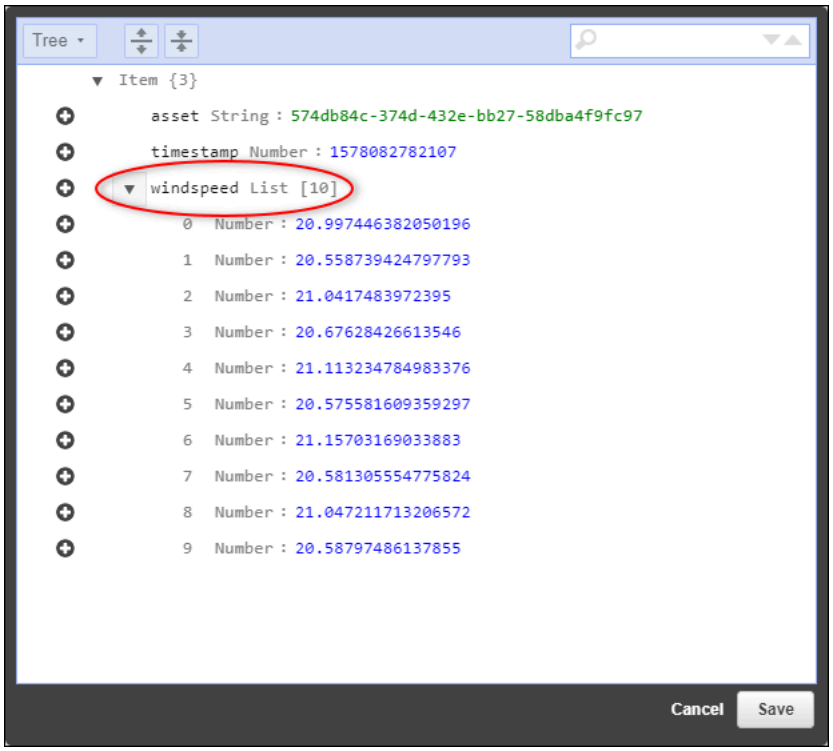


3. Wählen Sie in einer Zeile in der Tabelle das Bearbeitungssymbol aus, um die Daten zu erweitern.



4. Wählen Sie den Pfeil neben der Struktur windspeed aus, um die Liste der Datenpunkte für die Windgeschwindigkeit zu erweitern. Jede Liste enthält eine Reihe von Datenpunkten zur Windgeschwindigkeit, an die die AWS IoT SiteWise Windpark-Demo gesendet hat. Möglicherweise benötigen Sie ein anderes Datenformat, wenn Sie eine Regelaktion für

Ihre eigene Verwendung einrichten. Weitere Informationen finden Sie unter Abfragen von Benachrichtigungsmeldungen für Komponenteneigenschaften.



Nachdem Sie das Tutorial abgeschlossen haben, deaktivieren oder löschen Sie die Regel und löschen Sie Ihre DynamoDB-Tabelle, um zusätzliche Gebühren zu vermeiden. Informationen zum Bereinigen Ihrer Ressourcen finden Sie unter. Schritt 6: Ressourcen nach dem Tutorial bereinigen

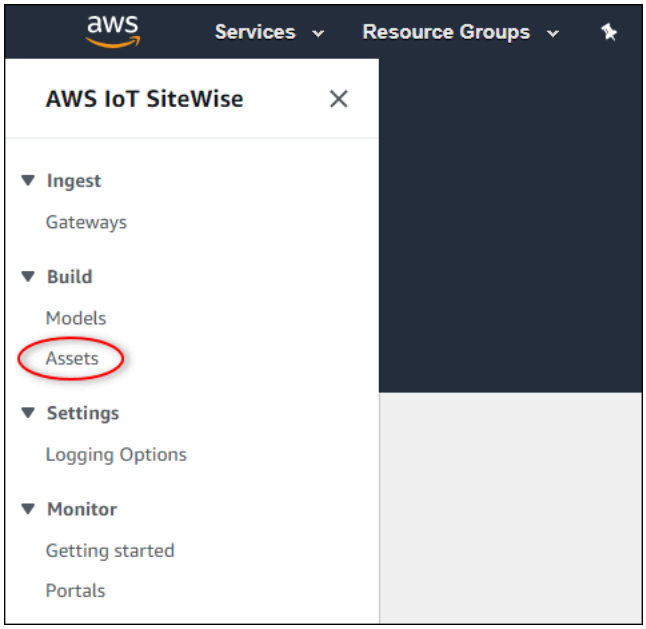
Schritt 6: Ressourcen nach dem Tutorial bereinigen

Nachdem Sie das Tutorial abgeschlossen haben, bereinigen Sie Ihre Ressourcen, um zusätzliche Kosten zu vermeiden. Ihre Demo-Windpark-Assets werden am Ende der Dauer gelöscht, die Sie bei der Erstellung der Demo ausgewählt haben. Sie können die Demo auch manuell löschen. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo löschen.

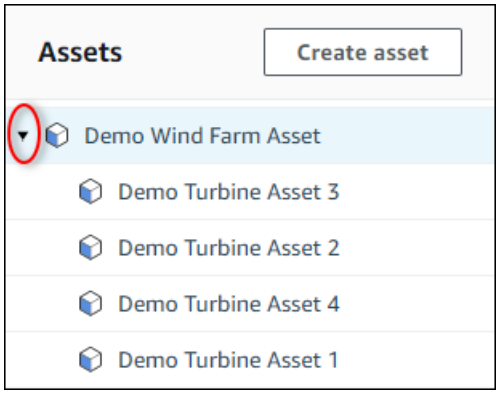
Gehen Sie wie folgt vor, um Benachrichtigungen zur Aktualisierung von Eigenschaftswerten zu deaktivieren (falls Sie die Demo nicht gelöscht haben), Ihre AWS IoT Regel zu deaktivieren oder zu löschen und Ihre DynamoDB-Tabelle zu löschen.

So deaktivieren Sie Aktualisierungsbenachrichtigungen für Komponenteneigenschaften:

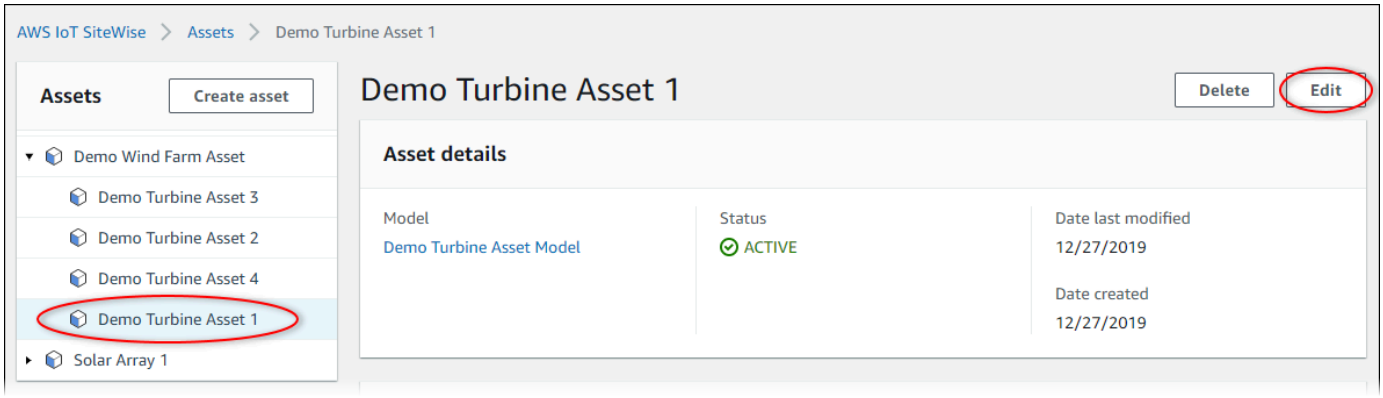
1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im linken Navigationsbereich auf Assets (Komponenten).



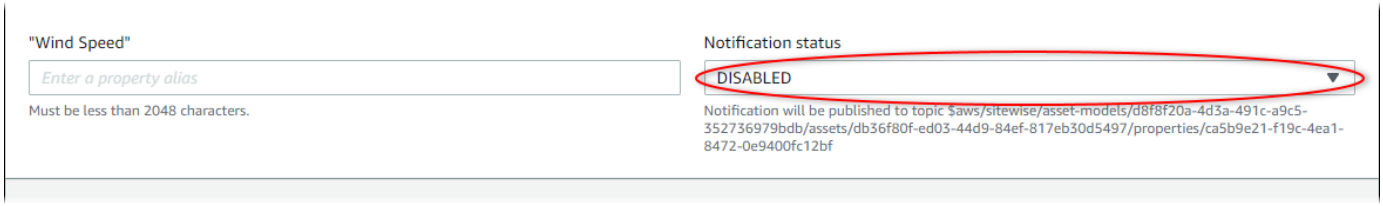
3. Wählen Sie den Pfeil neben Demo Wind Farm Asset aus, um die Hierarchie der Windparkkomponente zu erweitern.



4. Wählen Sie eine Demoturbine und Edit (Bearbeiten) aus.



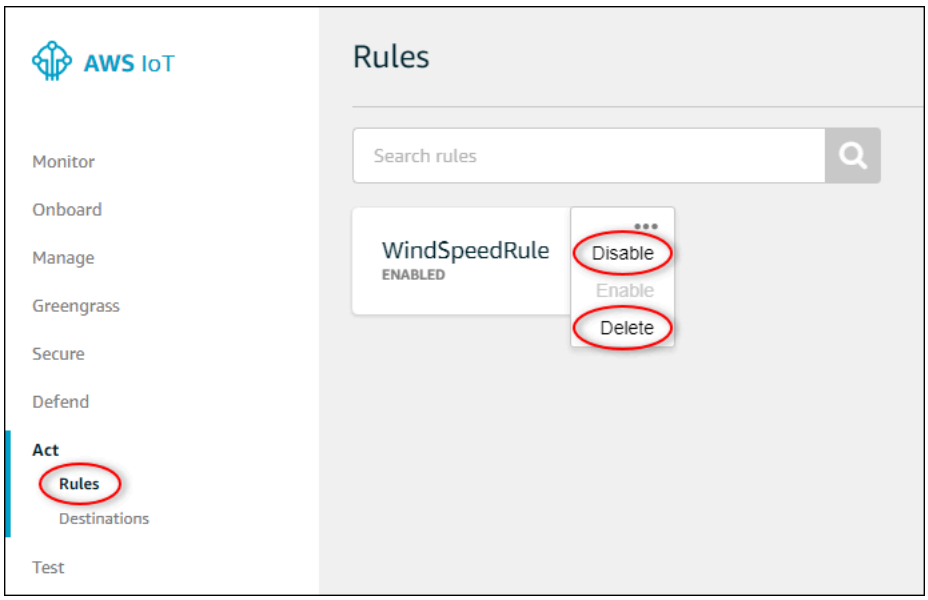
5. Ändern Sie den Benachrichtigungsstatus der Wind SpeedUnterkunft auf DEAKTIVIERT.



6. Wählen Sie unten auf der Seite die Option Save asset (Komponente speichern) aus.
7. Wiederholen Sie die Schritte 4 bis 6 für jede Demo-Turbinenkomponente.

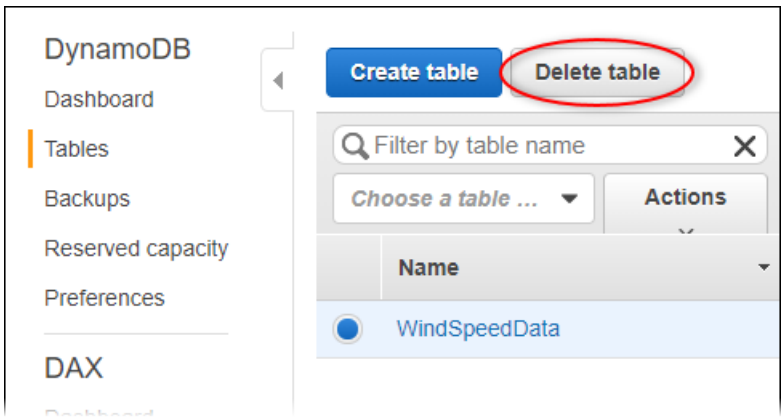
Um eine Regel zu deaktivieren oder zu löschen in AWS IoT Core

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Act (Agieren) und dann Rules (Regeln) aus.
3. Wählen Sie das Menü Ihrer Regel und Disable (Deaktivieren) oder Delete (Löschen) aus.

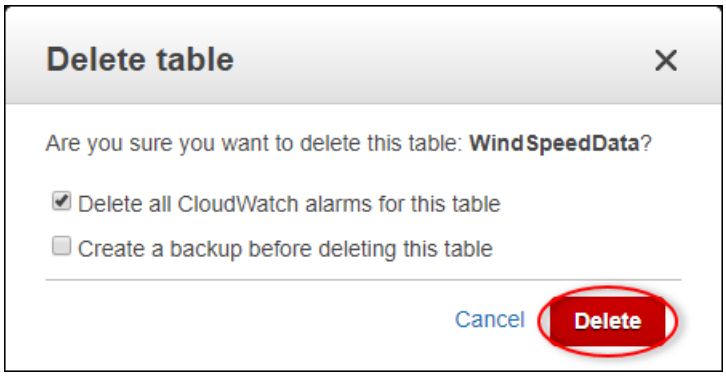


So löschen Sie eine DynamoDB-Tabelle

1. Navigieren Sie zur DynamoDB-Konsole.
2. Wählen Sie im linken Navigationsbereich Tables (Tabellen) aus.
3. Wählen Sie die Tabelle aus, die Sie zuvor erstellt haben, WindSpeedData.
4. Wählen Sie Delete Table (Tabelle löschen).



5. Wählen Sie im Dialogfeld Delete table (Tabelle löschen) die Option Delete (Löschen).



Daten aufnehmen zu AWS IoT SiteWise

AWS IoT SiteWise wurde entwickelt, um Industriedaten effizient zu sammeln und mit entsprechenden Ressourcen zu korrelieren, die verschiedene Aspekte industrieller Abläufe repräsentieren. Diese Dokumentation konzentriert sich auf die praktischen Aspekte der Datenerfassung und bietet mehrere Methoden AWS IoT SiteWise, die auf unterschiedliche industrielle Anwendungsfälle zugeschnitten sind. Anweisungen zum Aufbau Ihrer virtuellen industriellen Operationen finden Sie unter Modellieren von industriellen Komponenten.

Sie können Industriedaten AWS IoT SiteWise mit einer der folgenden Optionen an senden:

- AWS IoT SiteWise Edge — Verwenden Sie das SiteWise Edge-Gateway als Vermittler zwischen AWS IoT SiteWise und Ihren Datenservern. AWS IoT SiteWise stellt AWS IoT Greengrass Komponenten bereit, die Sie auf jeder Plattform bereitstellen können, die AWS IoT Greengrass zur Einrichtung eines SiteWise Edge-Gateways ausgeführt werden kann. Diese Option unterstützt die Verknüpfung mit dem OPC-UA-Serverprotokoll.
- AWS IoT SiteWise API — Verwenden Sie die AWS IoT SiteWise API, um Daten aus einer anderen Quelle hochzuladen. Verwenden Sie unsere BatchPutAssetPropertyValueStreaming-API für die Aufnahme innerhalb von Sekunden oder die stapelorientierte CreateBulkImportJobAPI, um eine kostengünstige Aufnahme in größeren Chargen zu ermöglichen.
- AWS IoT Kernregeln — Verwenden Sie AWS IoT Kernregeln, um Daten aus MQTT-Nachrichten hochzuladen, die von einer Sache oder einem anderen Dienst veröffentlicht wurden. AWS IoT AWS
- AWS IoT Events Aktionen — Verwenden Sie AWS IoT Events Aktionen, die durch bestimmte Ereignisse in ausgelöst wurden. AWS IoT Events Diese Methode eignet sich für Szenarien, in denen das Hochladen von Daten an Ereignisse gebunden ist.
- AWS IoT Greengrass Stream Manager — Verwenden Sie AWS IoT Greengrass Stream Manager, um Daten aus lokalen Datenquellen mit einem Edge-Gerät hochzuladen. Diese Option eignet sich für Situationen, in denen Daten von lokalen oder Edge-Standorten stammen.

Diese Methoden bieten eine Reihe von Lösungen für die Verwaltung von Daten aus verschiedenen Quellen. Machen Sie sich mit den Einzelheiten der einzelnen Optionen vertraut, um sich ein umfassendes Bild von den Möglichkeiten der Datenaufnahme zu machen. AWS IoT SiteWise

Verwaltung von Datenströmen

Bevor Sie mit der Erstellung von Anlagenmodellen und Anlagen beginnen AWS IoT SiteWise, richten Sie zunächst Ihre Datenquellen so ein, dass Informationen direkt von Ihren Industrieanlagen an die Plattform gesendet werden. AWS IoT SiteWise ist darauf ausgelegt, automatisch Datenströme zu generieren, die Ihre Rohdaten sammeln. Jeder der Datenströme wird durch einen eindeutigen Alias identifiziert, was es einfacher macht, den Ursprung der einzelnen Daten zu verfolgen.

Stellen Sie sich zum Beispiel einen Windpark vor, der ein AWS IoT SiteWise Edge-Gateway verwendet, um Daten zur Lufttemperatur, zur Propellerdrehzahl und zur Ausgangsleistung in Zeitreihen von einem OPC-UA-Server zu senden. AWS IoT SiteWise Der `server1-windfarm/3/turbine/7/temperature` Datenstream-Alias identifiziert Temperaturwerte, die von Turbine #7 im Windpark #3 stammen. `server1`ist der Name der OPC-UA-Datenquelle. Das `server1` Präfix wird für alle Datenströme verwendet, die von diesem Server kommen, und hilft dabei, Daten nach ihrer Quelle zu organisieren.

Nachdem Sie die Asset-Modelle und Assets erstellt haben, organisieren Sie den Datenfluss, indem Sie jeden Datenstrom bestimmten Asset-Eigenschaften zuordnen. Diese Zuordnung ermöglicht es, AWS IoT SiteWise die Daten nicht nur zu sammeln, sondern auch entsprechend der Struktur Ihrer Anlagen zu verarbeiten. Bei Bedarf können Sie auch die Verbindung zwischen Datenströmen und Asset-Eigenschaften entfernen.

Derzeit können Sie Datenströme nur Messungen zuordnen. Bei Messungen handelt es sich um eine Art von Anlageneigenschaft, die die rohen Sensordatenströme von Geräten darstellt, z. B. Temperaturwerte mit Zeitstempel oder Werte für Umdrehungen pro Minute (U/min) mit Zeitstempel.

Wenn diese Messungen Metriken oder Transformationen definieren, lösen die eingehenden Daten spezifische Berechnungen aus. Es ist wichtig zu beachten, dass eine Anlageneigenschaft jeweils nur mit einem Datenstrom verknüpft werden kann.

> **Note**
>
> Eine Anlageneigenschaft kann nicht mehreren Datenströmen gleichzeitig zugeordnet werden.

AWS IoT SiteWise verwendet `TimeSeries` die Ressource Amazon Resource Name (ARN), um Ihre Lagergebühren zu ermitteln. Weitere Informationen finden Sie unter AWS IoT SiteWise - Preisgestaltung.

In den folgenden Abschnitten erfahren Sie, wie Sie die AWS IoT SiteWise Konsole oder API zur Verwaltung von Datenströmen verwenden.

Themen

Verwalten von Daten-Streams

Gehen Sie wie folgt vor, um mit der Verwaltung von Datenströmen zu beginnen.

> **Note**
>
> Wenn Sie mit der Zeit AWS IoT SiteWise nach dem 24. November 2021 noch nicht vertraut sind, können Sie diesen Abschnitt überspringen. Kunden, die AWS IoT SiteWise vor diesem Datum mit der Nutzung begonnen haben, müssen die Serviceeinstellungen so konfigurieren AWS IoT SiteWise , dass Daten ohne Bestandsmodelle und Vermögenswerte aufgenommen werden können.

- Stellen Sie sicher, dass Ihre IAM-Rolle über die im folgenden Beispiel gezeigten Berechtigungen verfügt.

  Example IAM-Benutzerrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PutAssetPropertyValuesAssetPropertyOnly",
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "arn:aws:iotsitewise:*:*:asset/*"
        },
        {
            "Sid": "PutAssetPropertyValuesPropertyAliasAllowed",
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "arn:aws:iotsitewise:*:*:time-series/*"
        }
    ]
```

```
}
```

> **Important**
>
> Gehen Sie wie folgt vor, bevor Sie Daten in einen Datenstrom aufnehmen.
>
> - Die `time-series` Ressource muss autorisiert sein, wenn Sie einen Eigenschaftsalias verwenden, um den Datenstrom zu identifizieren.
> - Die `asset` Ressource muss autorisiert sein, wenn Sie eine Asset-ID verwenden, um das Asset zu identifizieren, das die zugehörige Asset-Eigenschaft enthält.

Weitere Informationen zur Konfiguration von IAM-Richtlinien finden Sie unter Verwaltung von IAM-Richtlinien im IAM-Benutzerhandbuch.

- Konfigurieren Sie die Einstellungen für die Datenaufnahme so, dass Datenstreams akzeptiert werden können AWS IoT SiteWise , die nicht mit Asset-Eigenschaften verknüpft sind.

Themen

Einstellungen für die Datenaufnahme konfigurieren

Console

Konfigurieren AWS IoT SiteWise Sie mithilfe der Konsole so, dass Datenstreams akzeptiert werden, die nicht mit Asset-Eigenschaften verknüpft sind. AWS IoT SiteWise

So konfigurieren Sie Einstellungen für die Datenaufnahme (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Datenaufnahme aus.
3. Wählen Sie auf der Seite Datenaufnahme die Option Bearbeiten aus.
4. Wählen Sie im Abschnitt Getrennte Datenaufnahme die Option Datenaufnahme für Datenstreams aktivieren aus, die nicht mit Asset-Eigenschaften verknüpft sind.

> **Important**
>
> Nachdem Sie AWS IoT SiteWise die Konfiguration so konfiguriert haben, dass Datenstreams akzeptiert werden, die nicht mit Asset-Eigenschaften verknüpft sind, können Sie diese Einstellung nicht mehr deaktivieren.

5. Wählen Sie Speichern.
6. Wählen Sie unter Aufnahme getrennter Daten aktivieren die Option Aktualisieren aus. Der Status für Getrennte Datenaufnahme lautet Aktiv. Es kann einige Minuten dauern, bis dieser Vorgang abgeschlossen ist.

AWS CLI

Konfigurieren AWS IoT SiteWise Sie mithilfe des PutStorageConfigurationAPI-Vorgangs so, dass Datenströme akzeptiert werden, die nicht mit Asset-Eigenschaften verknüpft sind. Im folgenden Abschnitt wird der verwendet AWS CLI.

Um die Einstellungen für die Datenaufnahme zu konfigurieren ()AWS CLI

1. Führen Sie den folgenden Befehl aus AWS IoT SiteWise , um den Empfang von Datenströmen zu konfigurieren, die nicht mit Asset-Eigenschaften verknüpft sind.

> **Important**
>
> Nachdem Sie AWS IoT SiteWise die Konfiguration so konfiguriert haben, dass Datenströme akzeptiert werden, die nicht mit Asset-Eigenschaften verknüpft sind, können Sie diese Einstellung nicht deaktivieren.

```
aws iotsitewise put-storage-configuration \
                                  -\-storage-type SITEWISE_DEFAULT_STORAGE \
                                  -\-disassociated-data-storage ENABLED
```

Sie können das so `storageType` konfigurieren`MULTI_LAYER_STORAGE`. Weitere Informationen finden Sie unter Verwaltung des Datenspeichers.

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "configurationStatus": {
                "state": "UPDATE_IN_PROGRESS"
            }
        }
```

Dieser Vorgang kann einige Minuten dauern.

2. Führen Sie den folgenden Befehl aus, um die Informationen zur Speicherkonfiguration abzurufen.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "configurationStatus": {
                "state": "ACTIVE"
            },
            "lastUpdateDate": "2021-11-16T15:54:14-07:00"
        }
```

Verwaltung von Datenströmen

Verwalten Sie Ihre Datenströme mit dem AWS-IoT-SiteWise-Konsole oder AWS CLI.

Console

Verwenden Sie die AWS IoT SiteWise Konsole, um Ihre Datenströme zu verwalten.

Um Datenströme zu verwalten (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Datenströme aus.

3. (Optional) Um Tags hinzuzufügen oder zu aktualisieren, wählen Sie den zu bearbeitenden Datenstream aus und wählen Sie dann Tags verwalten aus.

   Wählen Sie auf der Seite „Tags bearbeiten“ die Option Tag hinzufügen aus. Geben Sie im Feld Schlüssel den Namen des zu verwendenden Tags ein.

   Wählen Sie Speichern.

4. (Optional) In der Datenstromtabelle können Sie Datenströme auf folgende Weise filtern.

   - Wählen Sie im ersten Dropdownmenü Alias-Präfix oder Asset-ID aus.
     - Alias-Präfix — Das Alias-Präfix des Datenstroms. Sie können diese Option wählen, wenn Ihre Zieldatenströme ein Alias-Präfix haben.
     - Asset-ID — Die ID des Assets, in dem die Asset-Eigenschaft erstellt wurde. Sie können diese Option wählen, wenn Ihre Zieldatenströme mit einer Anlageneigenschaft verknüpft sind.
   - Wählen Sie im zweiten Dropdownmenü Alle Datenströme, Zugeordnete Datenströme oder Getrennte Datenströme aus.
     - Alle Datenströme — Datenströme, die mit einer Anlageneigenschaft verknüpft sind oder nicht.
     - Zugeordnete Datenströme — Datenströme, die einer Anlageneigenschaft zugeordnet sind.
     - Getrennte Datenströme — Datenströme, die keiner Anlageneigenschaft zugeordnet sind.

5. Wählen Sie die Datenströme aus, die Sie verwalten. AWS IoT SiteWise zeigt die von Ihnen ausgewählten Datenströme in einem Diagramm unten auf der Seite an. Wenn Sie mehr als 10 auswählen, zeigt das Diagramm nur die ersten 10 an.

6. (Optional) Konfigurieren Sie das Diagramm auf folgende Weise.

   a. Wählen Sie für die Aggregationsfunktion eine der folgenden Optionen aus.

      - Anzahl der Datenpunkte — Die Gesamtzahl der Datenpunkte für die angegebenen Variablen im aktuellen Zeitintervall.
      - Durchschnitt — Der Mittelwert der Werte der angegebenen Variablen im aktuellen Zeitintervall.
      - Summe — Die Summe der Werte der angegebenen Variablen im aktuellen Zeitintervall.

- Minimum — Das Minimum der Werte der angegebenen Variablen im aktuellen Zeitintervall.
- Maximum — Das Maximum der Werte der angegebenen Variablen im aktuellen Zeitintervall.

Weitere Informationen finden Sie unter Verwenden von Aggregationsfunktionen in Formelausdrücken.

b. Wählen Sie für Zeitbereiche eine der folgenden Optionen aus.

- Letzte 1 Stunde — Das Diagramm zeigt aggregierte Daten der letzten Stunde.
- Letzte 2 Stunden — Das Diagramm zeigt aggregierte Daten der letzten zwei Stunden.
- Letzte 3 Stunden — Das Diagramm zeigt aggregierte Daten der letzten drei Stunden.
- Letzte 4 Stunden — Das Diagramm zeigt aggregierte Daten der letzten vier Stunden.

c. Wählen Sie für Zeitintervall eine der folgenden Optionen aus.

- 1 Minute — Aggregiert Daten jede Minute über den angegebenen Zeitraum.
- 1 Stunde — Aggregiert Daten jede Stunde über den angegebenen Zeitraum.

7. Wählen Sie Datenströme verwalten aus.
8. Führen Sie im Abschnitt Datenstromzuordnungen aktualisieren in der Spalte Messname eine der folgenden Aktionen aus.

- Wenn der Datenstrom mit einer Messung verknüpft ist, löschen Sie die Zuordnung, indem Sie auf das Schließen-Symbol klicken.
- Wenn der Datenstrom keiner Messung zugeordnet ist, wählen Sie Messung auswählen.

9. Navigieren Sie in der Tabelle „Messung auswählen“ zum Ziel-Asset und wählen Sie dann die Messung aus, die Sie verknüpfen möchten.
10. (Optional) Geben Sie im Abschnitt Aliasnamen für Asset-Eigenschaften aktualisieren für jede Messung einen eindeutigen Alias ein.
11. Wählen Sie Aktualisieren.

In der Spalte Status kann einer der folgenden Werte angezeigt werden.

- Ausstehend — Sie aktualisieren die Datenstream-Zuordnung oder den Alias der Asset-Eigenschaft.

- Absenden — Ihre Änderung an der Zuordnung oder dem Alias für die Asset-Eigenschaft wird gespeichert.
- Fehler — Ihre Anfrage zur Aktualisierung der Datenstream-Zuordnung oder des Alias für die Messung AWS IoT SiteWise konnte nicht bearbeitet werden.
- Erfolgreich — Sie haben die Datenstream-Zuordnung oder den Alias für die Messung erfolgreich aktualisiert.

AWS CLI

Verwenden Sie die folgenden API-Operationen, um Ihre Datenströme zu verwalten. Die Codebeispiele verwenden die AWS CLI.

- AssociateTimeSeriesToAssetProperty— Ordnet einen Datenstrom (Zeitreihe) einer Anlageneigenschaft zu.
- DisassociateTimeSeriesFromAssetProperty— Trennt einen Datenstrom von einer Anlageneigenschaft.
- DeleteTimeSeries— Löscht einen Datenstrom.
- DescribeTimeSeries— Ruft Informationen über einen Datenstrom ab.
- ListTimeSeries— Ruft eine paginierte Liste von Datenströmen ab.

AssociateTimeSeriesToAssetProperty

Führen Sie den folgenden Befehl aus, um einen Datenstrom mit einer Asset-Eigenschaft zu verknüpfen.

> **Important**
>
> Die angegebene Asset-Eigenschaft darf derzeit keinem Datenstrom zugeordnet sein.

- *`data-stream-alias`*Ersetzen Sie es durch den Alias des Datenstroms, den Sie verknüpfen.
- Ersetzen Sie *`Asset-ID`* durch die ID des Assets, in dem die Asset-Eigenschaft erstellt wurde.
- Ersetzen Sie *`Property-ID`* durch die ID der Asset-Eigenschaft.

```
aws iotsitewise associate-time-series-to-asset-property \
```

```
                        --alias data-stream-alias \
                        --assetId asset-ID \
                        --propertyId property-ID
```

DisassociateTimeSeriesFromAssetProperty

Führen Sie den folgenden Befehl aus, um einen Datenstrom von einer Asset-Eigenschaft zu trennen.

- *data-stream-alias*Ersetzen Sie ihn durch den Alias des Datenstroms, dessen Zuordnung Sie aufheben möchten.
- Ersetzen Sie *Asset-ID* durch die ID des Assets, in dem die Asset-Eigenschaft erstellt wurde.
- Ersetzen Sie *Property-ID* durch die ID der Asset-Eigenschaft.

```
aws iotsitewise disassociate-time-series-from-asset-property \
                        --alias data-stream-alias \
                        --assetId asset-ID \
                        --propertyId property-ID
```

DeleteTimeSeries

Führen Sie den folgenden Befehl aus, um einen Datenstrom zu löschen.

*data-stream-alias*Ersetzen Sie ihn durch den Alias des Datenstroms, den Sie löschen möchten.

```
aws iotsitewise delete-time-series --alias data-stream-alias
```

Gehen Sie wie folgt vor, um einen Datenstrom zu identifizieren:

- Wenn der Datenstrom keiner Asset-Eigenschaft zugeordnet ist, geben Sie den Wert `alias` des Datenstroms an.
- Wenn der Datenstrom mit einer Anlageneigenschaft verknüpft ist, geben Sie eine der folgenden Optionen an:
  - Der `alias` des Datenstroms.
  - Das `assetId` und`propertyId`, das die Eigenschaft der Anlage identifiziert.

DescribeTimeSeries

Verwenden Sie den `DescribeTimeSeries` API-Vorgang, um zu überprüfen, ob Sie einen Datenstrom erfolgreich verknüpft oder getrennt haben.

Führen Sie den folgenden Befehl aus, um Informationen über einen Datenstrom abzurufen.

```
aws iotsitewise describe-time-series --alias data-stream-alias
```

Gehen Sie wie folgt vor, um einen Datenstrom zu identifizieren:

- Wenn der Datenstrom keiner Asset-Eigenschaft zugeordnet ist, geben Sie den Wert `alias` des Datenstroms an.
- Wenn der Datenstrom mit einer Anlageneigenschaft verknüpft ist, geben Sie eine der folgenden Optionen an:
  - Der `alias` des Datenstroms.
  - Das `assetId` und`propertyId`, das die Eigenschaft der Anlage identifiziert.

ListTimeSeries

Verwenden Sie den `ListTimeSeries` API-Vorgang, um zu überprüfen, ob Sie einen Datenstrom erfolgreich gelöscht haben.

Führen Sie den folgenden Befehl aus, um eine paginierte Liste von Datenströmen abzurufen.

```
aws iotsitewise list-time-series
```

Daten mithilfe der AWS IoT SiteWise API aufnehmen

Verwenden Sie die AWS IoT SiteWise API, um Industriedaten mit Zeitstempel an die Attribut- und Messeigenschaften Ihrer Anlagen zu senden. Die API akzeptiert eine Nutzlast, die timestamp-quality-value (TQV-) Strukturen enthält.

Verwenden Sie den BatchPutAssetPropertyValueVorgang, um Ihre Daten hochzuladen. Mit diesem Vorgang können Sie mehrere Dateneinträge gleichzeitig hochladen, um Daten von mehreren Geräten zu sammeln und alles in einer einzigen Anfrage zu senden.

> **Important**
>
> Der BatchPutAssetPropertyValueVorgang unterliegt den folgenden Kontingenten:

- Bis zu 10 Einträge pro Anfrage.
- Bis zu 10 Eigenschaftswerte (TQV-Datenpunkte) pro Eintrag.
- AWS IoT SiteWise lehnt alle Daten ab, deren Zeitstempel mehr als 7 Tage in der Vergangenheit oder mehr als 10 Minuten in der future liegt.

Weitere Informationen zu diesen Kontingenten finden Sie BatchPutAssetPropertyValuein der AWS IoT SiteWise API-Referenz.

Um eine Anlageneigenschaft zu identifizieren, geben Sie eine der folgenden Optionen an:

- Das `assetId` Ende `propertyId` der Anlageneigenschaft, an die Daten gesendet werden.
- The`propertyAlias`, bei dem es sich um einen Datenstream-Alias handelt (z. B.`/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Informationen zum Festlegen von Eigenschaftsaliasnamen finden Sie unterZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Im folgenden Beispiel wird veranschaulicht, wie die Messwerte einer Windkraftanlage für die Temperatur und die Umdrehungen pro Minute (U/min) aus Nutzlasten, die in einer JSON-Datei gespeichert sind, gesendet werden.

```
aws iotsitewise batch-put-asset-property-value --cli-input-json file://batch-put-payload.json
```

Die Beispielnutzlast in `batch-put-payload.json` hat folgenden Inhalt.

```
{
  "entries": [
    {
      "entryId": "unique entry ID",
      "propertyAlias": "/company/windfarm/3/turbine/7/temperature",
      "propertyValues": [
        {
          "value": {
            "integerValue": 38
          },
```

```
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "unique entry ID",
      "propertyAlias": "/company/windfarm/3/turbine/7/rpm",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 15.09
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          },
          "quality": "GOOD"
        }
      ]
    }
  ]
}
```

Jeder Eintrag in der Nutzlast enthält eine `entryId`, die Sie als eindeutige Zeichenfolge definieren können. Bei fehlgeschlagenen Anforderungseinträgen enthält jeder Fehler die `entryId` der entsprechenden Anforderung, woran Sie erkennen können, welche Anforderungen zu wiederholen sind.

Jede Struktur in der Liste von `propertyValues` ist eine timestamp-quality-value (TQV-) Struktur, die a `valuetimestamp`, a und optional a enthält. `quality`

- `value`— Eine Struktur, die je nach Typ der festzulegenden Eigenschaft eines der folgenden Felder enthält:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`
- `timestamp`— Eine Struktur, die die aktuelle Unix-Epoche in Sekunden enthält,`timeInSeconds`. Sie können den `offsetInNanos` Schlüssel auch in der `timestamp` Struktur angeben, wenn

Sie über zeitlich genaue Daten verfügen. AWS IoT SiteWise lehnt alle Datenpunkte ab, deren Zeitstempel älter als 7 Tage in der Vergangenheit oder neuer als 10 Minuten in der future sind.

- `quality`— (Optional) Eine der folgenden Qualitätszeichenfolgen:
  - `GOOD`— (Standard) Die Daten sind von keinen Problemen betroffen.
  - `BAD`— Die Daten sind von einem Problem wie einem Sensorausfall betroffen.
  - `UNCERTAIN`— Die Daten sind von einem Problem wie einer Sensorungenauigkeit betroffen.

  Weitere Informationen zum AWS IoT SiteWise Umgang mit Datenqualität bei Berechnungen finden Sie unter Datenqualität in Formelausdrücken.

Daten mithilfe AWS IoT Core von Regeln aufnehmen

Senden Sie Daten AWS IoT SiteWise an AWS IoT Dinge und andere AWS Dienste mithilfe von Regeln in AWS IoT Core. Regeln transformieren MQTT-Nachrichten und führen Aktionen aus, um mit AWS Diensten zu interagieren. Die AWS IoT SiteWise Regelaktion leitet Nachrichtendaten von der API an den BatchPutAssetPropertyValueVorgang weiter. AWS IoT SiteWise Weitere Informationen finden Sie unter Regeln und AWS IoT SiteWise Maßnahmen im AWS IoT Entwicklerhandbuch.

Ein Tutorial, in dem die Schritte beschrieben werden, die zum Einrichten einer Regel erforderlich sind, die Daten über Geräteschatten aufnimmt, finden Sie unterDaten von AWS IoT Dingen aufnehmen.

Sie können Daten auch AWS IoT SiteWise an andere AWS Dienste senden. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten.

Themen

- Gewährung AWS IoT des erforderlichen Zugriffs
- Konfiguration der AWS IoT SiteWise Regelaktion
- Kostensenkung mit Basic Ingest

Gewährung AWS IoT des erforderlichen Zugriffs

Sie verwenden IAM-Rollen, um die AWS Ressourcen zu steuern, auf die jede Regel Zugriff hat. Bevor Sie eine Regel erstellen, müssen Sie eine IAM-Rolle mit einer Richtlinie erstellen, die es der Regel ermöglicht, Aktionen für die erforderliche AWS Ressource auszuführen. AWS IoT nimmt diese Rolle bei der Ausführung einer Regel an.

Wenn Sie die Regelaktion in der AWS IoT Konsole erstellen, können Sie ein Root-Asset auswählen, um eine Rolle zu erstellen, die Zugriff auf eine ausgewählte Asset-Hierarchie hat. Weitere Informationen zum manuellen Definieren einer Rolle für eine Regel finden Sie im AWS IoT Entwicklerhandbuch unter Gewährung AWS IoT der erforderlichen Zugriffs - und Pass-Rollenberechtigungen.

Für die AWS IoT SiteWise Regelaktion müssen Sie eine Rolle definieren, die den `iotsitewise:BatchPutAssetPropertyValue` Zugriff auf die Asset-Eigenschaften ermöglicht, an die die Regel Daten sendet. Um die Sicherheit zu erhöhen, können Sie in der `Condition` Eigenschaft einen Pfad zur AWS IoT SiteWise Asset-Hierarchie angeben.

Die folgende Beispielvertrauensrichtlinie ermöglicht den Zugriff auf eine bestimmte Komponente und ihre untergeordneten Elemente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iotsitewise:assetHierarchyPath": [
            "/root node asset ID",
            "/root node asset ID/*"
          ]
        }
      }
    }
  ]
}
```

Entfernen Sie das `Condition` aus der Richtlinie, um Zugriff auf all Ihre Ressourcen zu gewähren. Die folgende Beispielvertrauensrichtlinie ermöglicht den Zugriff auf alle Ihre Komponenten in der aktuellen Region.

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

```
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "*"
    }
  ]
}
```

Konfiguration der AWS IoT SiteWise Regelaktion

Die AWS IoT SiteWise Regelaktion sendet Daten aus der MQTT-Nachricht, die die Regel initiiert hat, an die Asset-Eigenschaften in. AWS IoT SiteWise Sie können mehrere Dateneinträge gleichzeitig in verschiedene Asset-Eigenschaften hochladen, um Updates für alle Sensoren eines Geräts in einer Nachricht zu senden. Sie können für jede Dateneingabe auch mehrere Datenpunkte gleichzeitig hochladen.

> **Note**
>
> Wenn Sie AWS IoT SiteWise mit der Regelaktion Daten an senden, müssen Ihre Daten alle Anforderungen des `BatchPutAssetPropertyValue` Vorgangs erfüllen. Beispielsweise darf der Zeitstempel Ihrer Daten nicht früher als 7 Tage vor der aktuellen Unix-Epoche liegen. Weitere Informationen finden Sie unter Erfassen von Daten mit der AWS IoT SiteWise -API.

Für jede Dateneingabe in der Regelaktion identifizieren Sie eine Komponenteneigenschaft und geben den Zeitstempel, die Qualität und den Wert jedes Datenpunkts für diese Komponenteneigenschaft an. Die Regelaktion erwartet Zeichenfolgen für alle Parameter.

Zur korrekten Identifizierung einer Komponenteneigenschaft in einer Eingabe können Sie eine der folgenden Angaben machen:

- Die Asset ID (Komponenten-ID) (`assetId`) und die Property ID (Eigenschaften-ID) (`propertyId`) der Komponenteneigenschaft, an die Sie Daten senden. Sie können die Asset-ID und die Property-ID mithilfe der finden. AWS-IoT-SiteWise-Konsole Wenn Sie die Asset-ID kennen, können Sie den AWS CLI to call verwenden, DescribeAssetum die Immobilien-ID zu ermitteln.
- Das Property alias (Eigenschaftsalias) (`propertyAlias`), bei dem es sich um ein Datenstrom-Alias handelt (z. B. `/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Weitere Informationen zur Festlegung von Eigenschaftsaliasnamen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Verwenden Sie für den Zeitstempel in jedem Eintrag den von Ihrem Gerät gemeldeten Zeitstempel oder den von bereitgestellten Zeitstempel. AWS IoT Core Der Zeitstempel hat zwei Parameter:

- Zeit in Sekunden (`timeInSeconds`) — Die Unix-Epoche in Sekunden, zu der der Sensor oder das Gerät die Daten gemeldet hat.
- Offset in Nanos (`offsetInNanos`) — (Optional) Der Abstand zwischen Nanosekunden und der Zeit in Sekunden.

Important

Wenn Ihr Zeitstempel eine Zeichenfolge ist, einen Dezimalteil hat oder nicht in Sekunden angegeben ist, wird die Anfrage AWS IoT SiteWise zurückgewiesen. Sie müssen den Zeitstempel in Sekunden und Nanosekunden-Offset konvertieren. Verwenden Sie Funktionen der AWS IoT Regel-Engine, um den Zeitstempel zu konvertieren. Weitere Informationen finden Sie hier:

- Abrufen von Zeitstempeln für Geräte, die keine genaue Uhrzeit melden
- Konvertierung von Zeitstempeln im Zeichenkettenformat

Sie können Ersatzvorlagen für mehrere Parameter in der Aktion verwenden, um Berechnungen durchzuführen, Funktionen aufzurufen und Werte aus der Nachrichtennutzlast abzurufen. Weitere Informationen finden Sie im Entwicklerhandbuch unter Substitutionsvorlagen.AWS IoT

Note

Da ein Ausdruck in einer Substitutionsvorlage getrennt von der `SELECT`-Anweisung ausgewertet wird, können Sie keine Substitutionsvorlage verwenden, um auf einen Alias zu verweisen, der mit einer `AS`-Klausel erstellt wurde. Zusätzlich zu den unterstützten Funktionen und Operatoren können Sie nur in der ursprünglichen Nutzlast vorhandene Informationen referenzieren.

Themen

- Abrufen von Zeitstempeln für Geräte, die keine genaue Uhrzeit melden
- Konvertierung von Zeitstempeln im Zeichenkettenformat
- Konvertierung von Zeitstempelzeichenfolgen mit einer Genauigkeit von Nanosekunden

- Beispiele für Regelkonfigurationen
- Problembehandlung bei der -Regelaktion

Abrufen von Zeitstempeln für Geräte, die keine genaue Uhrzeit melden

Wenn Ihr Sensor oder Ihre Ausrüstung keine genauen Zeitdaten meldet, rufen Sie mit timestamp () die aktuelle Unix-Epochenzeit von der AWS IoT Regel-Engine ab. Diese Funktion gibt die Zeit in Millisekunden aus. Sie müssen den Wert also in Zeit in Sekunden und den Offset in Nanosekunden umrechnen. Verwenden Sie dazu die folgenden Konvertierungen:

- Verwenden Sie für Time in seconds (Zeit in Sekunden) (`timeInSeconds`) **`${floor(timestamp() / 1E3)}`**, um die Zeit von Millisekunden in Sekunden zu konvertieren.
- Verwenden Sie für Offset in nanos (Verschiebung in Nanosekunden) (`offsetInNanos`) **`${(timestamp() % 1E3) * 1E6}`**, um den Nanosekunden-Versatz des Zeitstempels zu berechnen.

Konvertierung von Zeitstempeln im Zeichenkettenformat

Wenn Ihr Sensor oder Ihre Ausrüstung Zeitdaten im Zeichenkettenformat meldet (z. B.`2020-03-03T14:57:14.699Z`), verwenden Sie time_to_epoch (String, String). Diese Funktion gibt den Zeitstempel und das Formatmuster als Parameter ein und gibt die Zeit in Millisekunden aus. Dann müssen Sie die Zeit in Zeit in Sekunden und den Offset in Nanosekunden umrechnen. Verwenden Sie dazu die folgenden Konvertierungen:

- Verwenden Sie für Time in seconds (`timeInSeconds`), **`${floor(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") / 1E3)}`** um die Zeitstempelzeichenfolge in Millisekunden und dann in Sekunden zu konvertieren.
- Verwenden Sie für Offset in nanos (`offsetInNanos`), um den Nanosekunden-Offset der Zeitstempelzeichenfolge **`${(time_to_epoch("2020-03-03T14:57:14.699Z", "yyyy-MM-dd'T'HH:mm:ss'Z'") % 1E3) * 1E6}`** zu berechnen.

> **Note**
>
> Die `time_to_epoch` Funktion unterstützt Zeitstempelzeichenfolgen mit einer Genauigkeit von bis zu Millisekunden. Um Zeichenketten mit Mikro- oder Nanosekundengenauigkeit zu

konvertieren, konfigurieren Sie eine AWS Lambda Funktion, die Ihre Regel aufruft, um den Zeitstempel in numerische Werte umzuwandeln. Weitere Informationen finden Sie unter Konvertierung von Zeitstempelzeichenfolgen mit einer Genauigkeit von Nanosekunden.

Konvertierung von Zeitstempelzeichenfolgen mit einer Genauigkeit von Nanosekunden

Wenn Ihr Gerät Zeitstempelinformationen im Zeichenkettenformat mit einer Genauigkeit im Nanosekundenbereich sendet (z. B.`2020-03-03T14:57:14.699728491Z`), gehen Sie wie folgt vor, um Ihre Regelaktion zu konfigurieren. Sie können eine AWS Lambda Funktion erstellen, die den Zeitstempel aus einer Zeichenfolge in Zeit in Sekunden (**`timeInSeconds`**) und Offset in Nanos () umwandelt. `offsetInNanos` Verwenden Sie dann aws_lambda (FunctionArn, inputJson) in Ihren Regelaktionsparametern, um diese Lambda-Funktion aufzurufen und die Ausgabe in Ihrer Regel zu verwenden.

> **Note**
>
> Dieser Abschnitt enthält erweiterte Anweisungen, die davon ausgehen, dass Sie mit dem Erstellen der folgenden Ressourcen vertraut sind:
>
> - Lambda-Funktionen. Weitere Informationen finden Sie unter Erstellen einer Lambda-Funktion mit der Konsole oder Verwenden von Lambda mit der AWS CLI im AWS Lambda Entwicklerhandbuch.
> - AWS IoT Regeln mit der AWS IoT SiteWise Regelaktion. Weitere Informationen finden Sie unter Daten mithilfe AWS IoT Core von Regeln aufnehmen.

Um eine AWS IoT SiteWise Regelaktion zu erstellen, die Zeitstempelzeichenfolgen analysiert

1. Erstellen Sie eine Lambda-Funktion mit den folgenden Eigenschaften:
   - Funktionsname — Verwenden Sie einen beschreibenden Funktionsnamen (z. B.**`ConvertNanosecondTimestampFromString`**).
   - Runtime — Verwenden Sie eine Python-3-Runtime wie Python 3.11 (`python3.11`).
   - Berechtigungen — Erstellen Sie eine Rolle mit grundlegenden Lambda-Berechtigungen (AWS LambdaBasicExecutionRole).
   - Ebenen — Fügen Sie die AWS SDKPandas-Python311-Ebene hinzu, die von der Lambda-Funktion verwendet werden soll. `numpy`

- Funktionscode — Verwenden Sie den folgenden Funktionscode, der ein Zeichenkettenargument mit dem Namen `timestamp` verwendet und Werte für diesen Zeitstempel ausgibt. `timeInSeconds` `offsetInNanos`

```
import json
import math
import numpy

# Converts a timestamp string into timeInSeconds and offsetInNanos in Unix epoch
 time.
# The input timestamp string can have up to nanosecond precision.
def lambda_handler(event, context):
    timestamp_str = event['timestamp']
    # Parse the timestamp string as nanoseconds since Unix epoch.
    nanoseconds = numpy.datetime64(timestamp_str, 'ns').item()
    time_in_seconds = math.floor(nanoseconds / 1E9)
    # Slice to avoid precision issues.
    offset_in_nanos = int(str(nanoseconds)[-9:])
    return {
        'timeInSeconds': time_in_seconds,
        'offsetInNanos': offset_in_nanos
    }
```

Diese Lambda-Funktion gibt Zeitstempelzeichenfolgen im Format ISO 8601 unter Verwendung von datetime64 von ein. NumPy

> **Note**
>
> Wenn Ihre Zeitstempelzeichenfolgen nicht im ISO 8601-Format vorliegen, können Sie eine Lösung implementieren, die das Zeitstempelformat definiert. pandas Weitere Informationen finden Sie unter pandas.to_datetime.

2. Wenn Sie die AWS IoT SiteWise Aktion für Ihre Regel konfigurieren, verwenden Sie die folgenden Ersatzvorlagen für Zeit in Sekunden (**`timeInSeconds`**) und Offset in Nanos (). `offsetInNanos` Diese Ersetzungsvorlagen gehen davon aus, dass Ihre Nachrichtennutzlast die Zeitstempelzeichenfolge in `timestamp` enthält. Die `aws_lambda`-Funktion verwendet eine JSON-Struktur für ihren zweiten Parameter, so dass Sie die folgenden Ersetzungsvorlagen bei Bedarf ändern können.

   - Verwenden Sie für Zeit in Sekunden (`timeInSeconds`) die folgende Ersetzungsvorlage.

```
${aws_lambda('arn:aws:lambda:region:account-
id:function:ConvertNanosecondTimestampFromString', {'timestamp':
 timestamp}).timeInSeconds}
```

- Verwenden Sie für Verschiebung in Nanosekunden (`offsetInNanos`) die folgende Ersetzungsvorlage.

```
${aws_lambda('arn:aws:lambda:region:account-
id:function:ConvertNanosecondTimestampFromString', {'timestamp':
 timestamp}).offsetInNanos}
```

Ersetzen Sie für jeden Parameter *`Region`* und *`Konto-ID durch Ihre Region und Konto-ID`*. AWS Wenn Sie einen anderen Namen für Ihre Lambda-Funktion verwendet haben, ändern Sie diesen ebenfalls.

3. Erteilen Sie mit der AWS IoT Erlaubnis Berechtigungen zum Aufrufen Ihrer Funktion. `lambda:InvokeFunction` Weitere Informationen finden Sie unter aws_lambda(functionArn, inputJson).
4. Testen Sie Ihre Regel (verwenden Sie z. B. den AWS IoT MQTT-Testclient) und stellen Sie sicher, dass die von Ihnen AWS IoT SiteWise gesendeten Daten empfangen werden.

   Wenn Ihre Regel nicht wie erwartet funktioniert, finden Sie weitere Informationen unter Problembehandlung und AWS IoT SiteWise Regelaktion.

> **Note**
>
> Diese Lösung ruft die Lambda-Funktion zweimal für jede Zeitstempelzeichenfolge auf. Sie können eine weitere Regel erstellen, um die Anzahl der Lambda-Funktionsaufrufen zu reduzieren, wenn Ihre Regel mehrere Datenpunkte verarbeitet, die in jeder Nutzlast denselben Zeitstempel haben.
> Erstellen Sie dazu eine Regel mit einer Aktion zum erneuten Veröffentlichen, die Lambda aufruft und die ursprüngliche Nutzlast mit der in und konvertierten Zeitstempelzeichenfolge veröffentlicht. `timeInSeconds` `offsetInNanos` Erstellen Sie dann eine Regel mit einer AWS IoT SiteWise Regelaktion, um die konvertierte Payload zu verwenden. Mit diesem Ansatz reduzieren Sie die Häufigkeit, mit der die Regel Lambda aufruft, erhöhen jedoch die

Anzahl der ausgeführten AWS IoT Regelaktionen. Berücksichtigen Sie die Preise für jeden Service, wenn Sie diese Lösung auf Ihren Anwendungsfall anwenden.

Beispiele für Regelkonfigurationen

Dieser Abschnitt enthält Beispielregelkonfigurationen zum Erstellen einer Regel mit einer AWS IoT SiteWise Aktion.

Example Beispielregelaktion, die Eigenschaftsaliasse als Nachrichtenthemen verwendet

Im folgenden Beispiel wird eine Regel mit einer AWS IoT SiteWise Aktion erstellt, die das Thema (über topic ()) als Eigenschaftsalias zur Identifizierung von Asset-Eigenschaften verwendet. Verwenden Sie dieses Beispiel, um eine Regel für die Aufnahme von Daten vom Typ Doppeltyp für alle Windturbinen in allen Windparks zu definieren. Für dieses Beispiel müssen Sie Eigenschaftsaliasnamen für die Eigenschaften aller Turbinenanlagen definieren. Sie müssten eine zweite, ähnliche Regel definieren, um Daten vom Typ Ganzzahl aufzunehmen.

```
aws iot create-topic-rule \
  --rule-name SiteWiseWindFarmRule \
  --topic-rule-payload file://sitewise-rule-payload.json
```

Die Beispielnutzlast in `sitewise-rule-payload.json` hat folgenden Inhalt.

```
{
  "sql": "SELECT * FROM '/company/windfarm/+/turbine/+/+' WHERE type = 'double'",
  "description": "Sends data to the wind turbine asset property with the same alias as
 the topic",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
  "actions": [
    {
      "iotSiteWise": {
        "putAssetPropertyValueEntries": [
          {
            "propertyAlias": "${topic()}",
            "propertyValues": [
              {
                "timestamp": {
                  "timeInSeconds": "${timeInSeconds}"
```

```
                },
                "value": {
                  "doubleValue": "${value}"
                }
              }
            ]
          }
        ],
        "roleArn": "arn:aws:iam::account-id:role/MySiteWiseActionRole"
      }
    }
  ]
}
```

Senden Sie mit dieser Regelaktion die folgende Nachricht als Thema für die Datenaufnahme an einen Alias für eine Windenergieanlage (z. B.`/company/windfarm/3/turbine/7/temperature`).

```
{
  "type": "double",
  "value": "38.3",
  "timeInSeconds": "1581368533"
}
```

Example Beispielregelaktion, die timestamp() verwendet, um die Zeit zu bestimmen

Im folgenden Beispiel wird eine Regel mit einer AWS IoT SiteWise Aktion erstellt, die eine Anlageneigenschaft anhand von IDs identifiziert und mithilfe von timestamp () die aktuelle Uhrzeit bestimmt.

```
aws iot create-topic-rule \
  --rule-name SiteWiseAssetPropertyRule \
  --topic-rule-payload file://sitewise-rule-payload.json
```

Die Beispielnutzlast in `sitewise-rule-payload.json` hat folgenden Inhalt.

```
{
  "sql": "SELECT * FROM 'my/asset/property/topic'",
  "description": "Sends device data to an asset property",
  "ruleDisabled": false,
  "awsIotSqlVersion": "2016-03-23",
```

```
  "actions": [
    {
      "iotSiteWise": {
        "putAssetPropertyValueEntries": [
          {
            "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "propertyValues": [
              {
                "timestamp": {
                  "timeInSeconds": "${floor(timestamp() / 1E3)}",
                  "offsetInNanos": "${(timestamp() % 1E3) * 1E6}"
                },
                "value": {
                  "doubleValue": "${value}"
                }
              }
            ]
          }
        ],
        "roleArn": "arn:aws:iam::account-id:role/MySiteWiseActionRole"
      }
    }
  ]
}
```

Senden Sie mit dieser Regelaktion die folgende Nachricht an den, `my/asset/property/topic` um Daten aufzunehmen.

```
{
  "type": "double",
  "value": "38.3"
}
```

Problembehandlung bei der -Regelaktion

Um Ihre AWS IoT SiteWise Regelaktion zu beheben AWS IoT Core, konfigurieren Sie CloudWatch Protokolle oder konfigurieren Sie eine Aktion zum erneuten Veröffentlichen von Fehlern für Ihre Regel. Weitere Informationen finden Sie unter Problembehandlung und AWS IoT SiteWise Regelaktion.

Kostensenkung mit Basic Ingest

AWS IoT Core bietet eine Funktion namens Basic Ingest, mit der Sie Daten versenden können, AWS IoT Core ohne dass Messaging-Kosten anfallen.AWS IoT Basic Ingest optimiert den Datenfluss für große Datenerfassungsworkloads, indem der Publish/Subscribe-Message Broker aus dem Erfassungspfad entfernt wird. Sie können Basic Ingest verwenden, wenn Sie wissen, an welche Regeln Ihre Nachrichten weitergeleitet werden sollen.

Um Basic Ingest zu verwenden, senden Sie Nachrichten direkt an eine bestimmte Regel mit einem speziellen Thema, `$aws/rules/rule-name`. Um beispielsweise eine Nachricht an eine Regel mit dem Namen `SiteWiseWindFarmRule` zu senden, senden Sie eine Nachricht an das Thema `$aws/rules/SiteWiseWindFarmRule`.

Wenn Ihre Regelaktion Substitutionsvorlagen verwendet, die topic(Decimal) (Thema (Dezimal)) enthalten, können Sie das ursprüngliche Thema am Ende des speziellen Basic Ingest-Themas übergeben, z. B. `$aws/rules/rule-name/original-topic`. Wenn Sie beispielsweise Basic Ingest mit dem Aliasbeispiel für Windparks aus dem vorherigen Abschnitt verwenden möchten, können Sie Nachrichten an das folgende Thema senden.

```
$aws/rules/SiteWiseWindFarmRule//company/windfarm/3/turbine/7/temperature
```

> **Note**
>
> Das obige Beispiel enthält einen zweiten Schrägstrich (`//`), weil das Basic Ingest-Präfix (`$aws/rules/rule-name/`) aus dem Thema AWS IoT entfernt wird, das für die Regelaktion sichtbar ist. In diesem Beispiel erhält die Regel das Thema `/company/windfarm/3/turbine/7/temperature`.

Weitere Informationen finden Sie im Entwicklerhandbuch unter Senkung der Messaging-Kosten durch einfaches Ingest.AWS IoT

Daten werden aufgenommen von AWS IoT Events

Mit AWS IoT Events können Sie komplexe Anwendungen zur Ereignisüberwachung für Ihre IoT-Flotte in der AWS Cloud erstellen. Verwenden Sie die SiteWise IoT-Aktion in AWS IoT Events , um Daten an Asset-Eigenschaften zu senden AWS IoT SiteWise , wenn ein Ereignis eintritt.

AWS IoT Events wurde entwickelt, um die Entwicklung von Anwendungen zur Ereignisüberwachung für IoT-Geräte und -Systeme in der AWS Cloud zu optimieren. Mit Hilfe AWS IoT Events können Sie:

- Erkennen Sie Änderungen, Anomalien oder spezifische Bedingungen in Ihrer IoT-Flotte und reagieren Sie darauf.
- Steigern Sie Ihre betriebliche Effizienz und ermöglichen Sie ein proaktives Management Ihres IoT-Ökosystems.

Durch die Integration mit AWS IoT SiteWise Through the AWS IoT SiteWise Action werden die Funktionen AWS IoT Events erweitert, sodass Sie die Eigenschaften Ihrer Anlagen als Reaktion AWS IoT SiteWise auf bestimmte Ereignisse automatisch aktualisieren können. Diese Interaktion kann die Datenaufnahme und -verwaltung vereinfachen. Sie kann Ihnen auch umsetzbare Erkenntnisse liefern.

Weitere Informationen finden Sie in den folgenden Themen im AWS IoT Events Entwicklerhandbuch:

- Was ist AWS IoT Events?
- AWS IoT Events -Aktionen
- SiteWise IoT-Aktion

Verwenden des AWS IoT Greengrass Stream-Managers

AWS IoT Greengrass Stream Manager ist eine Integrationsfunktion, die die Übertragung von Datenströmen aus lokalen Quellen in die AWS Cloud erleichtert. Er fungiert als Zwischenschicht, die Datenflüsse verwaltet und es Geräten, die am Netzwerkrand betrieben werden, ermöglicht, Daten zu sammeln und zu speichern, bevor sie an sie gesendet werden AWS IoT SiteWise, um sie weiter zu analysieren und zu verarbeiten.

Fügen Sie ein Datenziel hinzu, indem Sie eine lokale Quelle auf der AWS IoT SiteWise Konsole konfigurieren. Sie können den Stream Manager auch in Ihrer benutzerdefinierten AWS IoT Greengrass Lösung verwenden, um AWS IoT SiteWise Daten aufzunehmen.

> **Note**
>
> Um Daten aus OPC-UA-Quellen aufzunehmen, konfigurieren Sie ein AWS IoT SiteWise Edge-Gateway, das auf läuft. AWS IoT Greengrass Weitere Informationen finden Sie unter Verwenden von SiteWise Edge-Gateways.

Weitere Informationen zur Konfiguration eines Ziels für lokale Quelldaten finden Sie unter. Konfigurieren von Datenquellen

Weitere Informationen zum Ingestieren von Daten mithilfe des Stream-Managers in einer benutzerdefinierten AWS IoT Greengrass Lösung finden Sie in den folgenden Themen im AWS IoT Greengrass Version 2 Entwicklerhandbuch:

- Was ist AWS IoT Greengrass?
- Datenströme auf dem AWS IoT Greengrass Core verwalten
- Exportieren von Daten in AWS IoT SiteWise Asset-Eigenschaften

Daten mithilfe der CreateBulkImportJob API aufnehmen

Verwenden Sie die `CreateBulkImportJob` API, um große Datenmengen aus Amazon S3 zu importieren. Ihre Daten müssen im CSV-Format in Amazon S3 gespeichert werden. Datendateien können die folgenden Spalten haben.

> **Note**
>
> Um eine Anlageneigenschaft zu identifizieren, geben Sie eine der folgenden Optionen an.
>
> - Das `ASSET_ID` Ende `PROPERTY_ID` der Anlageneigenschaft, an die Sie Daten senden.
> - The`ALIAS`, bei dem es sich um einen Datenstream-Alias handelt (z. B.`/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Weitere Informationen zur Festlegung von Eigenschaftsaliasnamen finden Sie unter the section called “Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften”.

- `ALIAS`— Der Alias, der die Eigenschaft identifiziert, z. B. ein OPC-UA-Serverdatenstream-Pfad (zum Beispiel`/company/windfarm/3/turbine/7/temperature`). Weitere Informationen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.
- `ASSET_ID`— Die ID des Assets.
- `PROPERTY_ID`— Die ID der Anlageeigenschaft.
- `DATA_TYPE`— Der Datentyp der Eigenschaft kann einer der folgenden sein.
  - `STRING`— Eine Zeichenfolge mit bis zu 1024 Byte.

  - `INTEGER`— Eine 32-Bit-Ganzzahl mit Vorzeichen im Bereich [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`— Eine Fließkommazahl mit einem Bereich [-10^100, 10^100] und einer doppelten IEEE-754-Genauigkeit.
  - `BOOLEAN`— `true` oder. `false`
- `TIMESTAMP_SECONDS`— Der Zeitstempel des Datenpunkts in der Unix-Epochenzeit.
- `TIMESTAMP_NANO_OFFSET`— Der Nanosekunden-Offset, aus dem konvertiert wurde. `TIMESTAMP_SECONDS`
- `QUALITY`— (Fakultativ) Die Qualität des Vermögenswerts. Der Wert kann einer der folgenden sein.
  - `GOOD`— (Standard) Die Daten sind von keinen Problemen betroffen.
  - `BAD`— Die Daten sind von einem Problem wie einem Sensorausfall betroffen.
  - `UNCERTAIN`— Die Daten sind von einem Problem wie einer Sensorungenauigkeit betroffen.

  Weitere Informationen zum AWS IoT SiteWise Umgang mit Datenqualität bei Berechnungen finden Sie unter Datenqualität in Formelausdrücken.
- `VALUE`— Der Wert der Vermögenseigenschaft.

Example Datendatei (en) im CSV-Format

```
asset_id,property_id,DOUBLE,1635201373,0,GOOD,1.0
asset_id,property_id,DOUBLE,1635201374,0,GOOD,2.0
asset_id,property_id,DOUBLE,1635201375,0,GOOD,3.0
```

```
unmodeled_alias1,DOUBLE,1635201373,0,GOOD,1.0
unmodeled_alias1,DOUBLE,1635201374,0,GOOD,2.0
unmodeled_alias1,DOUBLE,1635201375,0,GOOD,3.0
unmodeled_alias1,DOUBLE,1635201376,0,GOOD,4.0
unmodeled_alias1,DOUBLE,1635201377,0,GOOD,5.0
unmodeled_alias1,DOUBLE,1635201378,0,GOOD,6.0
unmodeled_alias1,DOUBLE,1635201379,0,GOOD,7.0
unmodeled_alias1,DOUBLE,1635201380,0,GOOD,8.0
unmodeled_alias1,DOUBLE,1635201381,0,GOOD,9.0
unmodeled_alias1,DOUBLE,1635201382,0,GOOD,10.0
```

AWS IoT SiteWise stellt die folgenden API-Operationen bereit, um einen Massenimportauftrag zu erstellen und Informationen über einen vorhandenen Auftrag abzurufen.

- CreateBulkImportJob— Erstellt einen neuen Massenimportauftrag.

- DescribeBulkImportJob— Ruft Informationen über einen Massenimportjob ab.
- ListBulkImportJob— Ruft eine paginierte Liste mit Zusammenfassungen aller Massenimportaufträge ab.

Erstellen Sie einen Massenimportauftrag ()AWS CLI

Verwenden Sie den CreateBulkImportJobAPI-Vorgang, um Daten von Amazon S3 zu zu übertragen AWS IoT SiteWise. Verwenden Sie die CreateBulkImportJobAPI, um Daten auf kostengünstige Weise in kleinen Batches aufzunehmen. Im folgenden Beispiel wird verwende AWS CLI.

> **Important**
>
> Bevor Sie einen Massenimportauftrag erstellen, müssen Sie AWS IoT SiteWise Warm Tier oder AWS IoT SiteWise Cold Tier aktivieren. Weitere Informationen finden Sie unter Speichereinstellungen konfigurieren.
> Der Massenimport dient zum Speichern historischer Daten in AWS IoT SiteWise. Es werden keine Berechnungen oder Benachrichtigungen auf der AWS IoT SiteWise warmen oder AWS IoT SiteWise kalten Stufe gestartet.

Führen Sie den folgenden Befehl aus. Ersetzen Sie *file-name* durch den Namen der Datei, die die Konfiguration des Massenimportauftrags enthält.

```
aws iotsitewise create-bulk-import-job --cli-input-json file://file-name.json
```

Example Konfiguration des Massenimport-Jobs

Im Folgenden finden Sie Beispiele für Konfigurationseinstellungen:

- Ersetzen Sie *adaptive-ingestion-flag* durch `true` oder `false`.
  - Wenn diese Option auf gesetzt ist`false`, nimmt der Massenimportjob historische Daten in AWS IoT SiteWise auf.
  - Wenn diese Option auf gesetzt ist`true`, führt der Massenimportjob Folgendes aus:
    - Nimmt neue Daten auf in AWS IoT SiteWise.
    - Berechnet Metriken und Transformationen und unterstützt Benachrichtigungen für Daten mit einem Zeitstempel, der innerhalb von sieben Tagen liegt.

- Ersetzen Sie *delete-files-after-import-flag* durch`true`, um die Daten aus dem S3-Daten-Bucket zu löschen, nachdem sie in einen Warm-Tier-Speicher aufgenommen AWS IoT SiteWise wurden.
- Ersetzen Sie *error-bucket* durch den Namen des Amazon S3 S3-Buckets, an den Fehler im Zusammenhang mit diesem Massenimportauftrag gesendet werden.
- *error-bucket-prefix*Ersetzen Sie es durch das Präfix des Amazon S3 S3-Buckets, an den Fehler im Zusammenhang mit diesem Massenimportauftrag gesendet werden.

  Amazon S3 verwendet das Präfix als Ordnernamen, um Daten im Bucket zu organisieren. Jedes Amazon S3 S3-Objekt hat einen Schlüssel, der seine eindeutige Kennung im Bucket ist. Jedes Objekt in einem Bucket besitzt genau einen Schlüssel. Das Präfix muss mit einem Schrägstrich enden (/). Weitere Informationen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon Simple Storage Service-Benutzerhandbuch.
- Ersetzen Sie *data-bucket* durch den Namen des Amazon S3 S3-Buckets, aus dem Daten importiert werden.
- *data-bucket-key*Ersetzen Sie es durch den Schlüssel des Amazon S3 S3-Objekts, das Ihre Daten enthält. Jedes Objekt hat einen Schlüssel, der eine eindeutige Kennung ist. Jedes Objekt hat genau einen Schlüssel.
- *data-bucket-version-id*Ersetzen Sie es durch die Versions-ID, um eine bestimmte Version des Amazon S3 S3-Objekts zu identifizieren, das Ihre Daten enthält. Dieser Parameter ist optional.
- Ersetzen Sie *column-name* durch den in der .csv-Datei angegebenen Spaltennamen.
- Ersetzen Sie *job-name* durch einen eindeutigen Namen, der den Massenimportauftrag identifiziert.
- *job-role-arn*Ersetzen Sie durch die IAM-Rolle, die das Lesen von Amazon S3 S3-Daten ermöglicht AWS IoT SiteWise .

> **Note**
>
> Stellen Sie sicher, dass Ihre Rolle über die im folgenden Beispiel gezeigten Berechtigungen verfügt. Ersetzen Sie *data-bucket* durch den Namen des Amazon S3 S3-Buckets, der Ihre Daten enthält. Ersetzen Sie außerdem *error-bucket* durch den Namen des Amazon S3 S3-Buckets, an den Fehler im Zusammenhang mit diesem Massenimportauftrag gesendet werden.
>
> ```
> {
> ```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::data-bucket",
                "arn:aws:s3:::data-bucket/*",
            ],
            "Effect": "Allow"
        },
      {
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::error-bucket",
                "arn:aws:s3:::error-bucket/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

```
{
   "adaptiveIngestion": adaptive-ingestion-flag,
   "deleteFilesAfterImport": delete-files-after-import-flag,
   "errorReportLocation": {
      "bucket": "error-bucket",
      "prefix": "error-bucket-prefix"
   },
   "files": [
      {
         "bucket": "data-bucket",
         "key": "data-bucket-key",
         "versionId": "data-bucket-version-id"
      }
```

```
   ],
   "jobConfiguration": {
      "fileFormat": {
         "csv": {
            "columnNames": [ "column-name" ]
         }
      }
   },
   "jobName": "job-name",
   "jobRoleArn": "job-role-arn"
}
```

Example response

```
{
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5",
   "jobStatus":"PENDING",
   "jobName":"myBulkImportJob"
}
```

Beschreiben Sie einen Massenimportauftrag ()AWS CLI

Verwenden Sie den DescribeBulkImportJobAPI-Vorgang, um Informationen über einen Massenimportauftrag abzurufen. Das folgende Beispiel verwendet AWS CLI.

Ersetzen Sie *Job-ID* durch die ID des Massenimportauftrags, den Sie abrufen möchten.

```
aws iotsitewise describe-bulk-import-job --job-id job-ID
```

Example response

```
{
   "files":[
      {
         "bucket":"test-bucket",
         "key":"100Tags12Hours.csv"
      },
      {
         "bucket":"test-bucket",
         "key":"BulkImportData1MB.csv"
      },
```

```
      {
         "bucket":"test-bucket",
         "key":"UnmodeledBulkImportData1MB.csv"
      }
   ],
   "errorReportLocation":{
      "prefix":"errors/",
      "bucket":"test-error-bucket"
   },
   "jobConfiguration":{
      "fileFormat":{
         "csv":{
            "columnNames":[
               "ALIAS",
               "DATA_TYPE",
               "TIMESTAMP_SECONDS",
               "TIMESTAMP_NANO_OFFSET",
               "QUALITY",
               "VALUE"
            ]
         }
      }
   },
   "jobCreationDate":1645745176.498,
   "jobStatus":"COMPLETED",
   "jobName":"myBulkImportJob",
   "jobLastUpdateDate":1645745279.968,
   "jobRoleArn":"arn:aws:iam::123456789012:role/DemoRole",
   "jobId":"f8c031d0-01d1-4b94-90b1-afe8bb93b7e5"
}
```

Auflisten von Massenimportaufträgen ()AWS CLI

Verwenden Sie den ListBulkImportJobsAPI-Vorgang, um eine paginierte Liste mit Zusammenfassungen aller Massenimportaufträge abzurufen. Das folgende Beispiel verwendet. AWS CLI

```
aws iotsitewise list-bulk-import-jobs --filter COMPLETED
```

Example response

```
{
```

```
   "jobSummaries":[
      {
         "id":"bdbbfa52-d775-4952-b816-13ba1c7cb9da",
         "name":"myBulkImportJob",
         "status":"COMPLETED"
      },
      {
         "id":"15ffc641-dbd8-40c6-9983-5cb3b0bc3e6b",
         "name":"myBulkImportJob2",
         "status":"RUNNING"
      }
   ]
}
```

Verwenden von SiteWise Edge-Gateways

Ein AWS IoT SiteWise Edge-Gateway dient als Vermittler zwischen Ihren Industrieanlagen und. AWS IoT SiteWise Das SiteWise Edge-Gateway läuft darauf und unterstützt AWS IoT Greengrass V2 die Datenerfassung und -verarbeitung vor Ort. Sie können AWS OpsHub for verwenden AWS IoT SiteWise , um Ihre SiteWise Edge-Gateways zu verwalten und den Betrieb vor Ort zu überwachen.

Mithilfe von Monitor-Portalen auf Ihren lokalen Geräten können Sie Daten lokal in Ihrer Einrichtung SiteWise überwachen. Weitere Informationen finden Sie unter Aktivierung Ihres Portals am Edge.

Themen

SiteWise Anforderungen an das Edge-Gateway

AWS IoT SiteWise Edge-Gateways werden AWS IoT Greengrass V2 als eine Reihe von AWS IoT Greengrass Komponenten ausgeführt, die die Datenerfassung, -verarbeitung und -veröffentlichung vor Ort unterstützen. Um ein SiteWise Edge-Gateway zu konfigurieren, das auf läuft AWS IoT

Greengrass V2, müssen Sie ein Gateway in der erstellen AWS Cloud und die SiteWise Edge-Gateway-Software ausführen, um Ihr lokales Gerät einzurichten.

Voraussetzungen

Lokale Geräte müssen die folgenden Anforderungen erfüllen, um die SiteWise Edge-Gateway-Software installieren und ausführen zu können.

- Unterstützt die AWS IoT Greengrass V2 Core-Softwareversion v2.3.0 oder neuer. Weitere Informationen finden Sie unter Anforderungen im AWS IoT Greengrass Version 2 Entwicklerhandbuch.
- Eine der folgenden unterstützten Plattformen:
  - Betriebssystem: Ubuntu 20.04 oder höher

    Architektur: x86_64 (AMD64) oder ARMv8 (Aarch64)
  - Betriebssystem: Red Hat Enterprise Linux (RHEL) 8

    Architektur: x86_64 (AMD64) oder ARMv8 (Aarch64)
  - Betriebssystem: Amazon Linux 2

    Architektur: x86_64 (AMD64) oder ARMv8 (Aarch64)
  - Betriebssystem: Debian 11

    Architektur: x86_64 (AMD64) oder ARMv8 (Aarch64)
  - Betriebssystem: Windows Server 2019 und später

    Architektur: x86_64 (AMD64)

  > **Note**
  >
  > ARM-Plattformen unterstützen SiteWise Edge-Gateways nur mit Data Collection Pack. Das Data Processing Pack wird nicht unterstützt.

- Mindestens 4 GB RAM.
- Für die SiteWise Edge-Gateway-Software stehen mindestens 10 GB Festplattenspeicher zur Verfügung.
- Wenn Sie planen, Daten am Edge mit zu verarbeiten AWS IoT SiteWise, muss Ihr lokales Gerät außerdem die folgenden Anforderungen erfüllen:

  - Hat einen x86-64-Bit-Quad-Core-Prozessor.
  - Hat mindestens 16 GB RAM.
  - Hat mindestens 32 GB RAM, wenn Sie Windows verwenden.
  - Hatte mindestens 256 GB freien Festplattenspeicher.
- Die Mindestanforderungen an Festplattenspeicher und Rechenkapazität hängen von einer Vielzahl von Faktoren ab, die für Ihre Implementierung und Ihren Anwendungsfall spezifisch sind.
  - Der für das Caching von Daten zur zeitweiligen Internetkonnektivität benötigte Festplattenspeicher ist von folgenden Faktoren abhängig:
    - Zahl der hochgeladenen Daten-Streams
    - Datenpunkte pro Daten-Stream pro Sekunde
    - Größe jedes Datenpunkts
    - Kommunikationsgeschwindigkeiten
    - Erwartete Netzwerkausfallzeit
  - Die zum Abfragen und Hochladen von Daten benötigte Rechenkapazität ist von folgenden Faktoren abhängig:
    - Zahl der hochgeladenen Daten-Streams
    - Datenpunkte pro Daten-Stream pro Sekunde
- Konfigurieren Sie Ihr lokales Gerät für den Zugriff auf den folgenden S3-Bucket:`iot-sitewise-gateway-<region>-748875242063`.
- Konfigurieren Sie Ihr lokales Gerät, um sicherzustellen, dass auf die folgenden Ports zugegriffen werden kann:
  - Das lokale Gerät muss eingehenden Netzwerkverkehr auf Port 443 zulassen.
  - Das lokale Gerät muss ausgehenden Verkehr an den Ports 443 und 8883 zulassen.

    Eine vollständige Liste der erforderlichen ausgehenden Dienstendpunkte finden Sie unter Erforderliche Dienstendpunkte für Edge-Gateways. AWS IoT SiteWise
  - Die folgenden Ports sind für die Verwendung durch reserviert AWS IoT SiteWise: 80, 443, 3001, 4569, 4572, 8000, 8081, 8082, 8084, 8085, 8445, 8086, 9000, 9500, 11080 und 50010. Die Verwendung eines reservierten Ports für den Datenverkehr kann zu einem Verbindungsabbruch führen.

> **Note**
>
> Die AWS IoT Greengrass V2 Stream Manager-Komponente hat ihre eigenen Anforderungen. Weitere Informationen finden Sie unter Konfiguration im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

- Java Runtime Environment (JRE) Version 11 oder höher. Java muss in der `PATH` Umgebungsvariablen auf dem Gerät verfügbar sein. Um Java zur Entwicklung benutzerdefinierter Komponenten zu verwenden, müssen Sie ein Java Development Kit (JDK) installieren. Wir empfehlen die Verwendung von Amazon Corretto oder OpenJDK.

Sie benötigen die folgenden Berechtigungen, um Edge-Gateways verwenden zu können: SiteWise

> **Note**
>
> Wenn Sie die AWS IoT SiteWise Konsole verwenden, um Ihr SiteWise Edge-Gateway zu erstellen, werden diese Berechtigungen für Sie hinzugefügt.

- Die IAM-Rolle für Ihr SiteWise Edge-Gateway muss es Ihnen ermöglichen, ein SiteWise Edge-Gateway auf einem AWS IoT Greengrass V2 Gerät zu verwenden, um Asset-Modelldaten und Asset-Daten zu verarbeiten.

  Die Rolle ermöglicht es dem folgenden Dienst, die Rolle zu übernehmen:`credentials.iot.amazonaws.com`.

  Details zu Berechtigungen

  Die Rolle muss über die folgenden Berechtigungen verfügen:

  - `iotsitewise`— Ermöglicht Prinzipalen das Abrufen von Asset-Modelldaten und Asset-Daten am Edge.
  - `iot`— Ermöglicht Ihren AWS IoT Greengrass V2 Geräten die Interaktion mit AWS IoT.
  - `logs`— Ermöglicht Ihren AWS IoT Greengrass V2 Geräten, Protokolle an Amazon CloudWatch Logs zu senden.
  - `s3`— Ermöglicht Ihren AWS IoT Greengrass V2 Geräten, benutzerdefinierte Komponentenartefakte von Amazon S3 herunterzuladen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:BatchPutAssetPropertyValue",
                "iotsitewise:List*",
                "iotsitewise:Describe*",
                "iotsitewise:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeCertificate",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "iot:Connect",
                "iot:Publish",
                "iot:Subscribe",
                "iot:Receive",
                "iot:DescribeEndpoint"
            ],
            "Resource": "*"
        }
    ]
}
```

Ein SiteWise Edge-Gateway erstellen

Sie können die AWS IoT SiteWise Konsole verwenden, um ein SiteWise Edge-Gateway zu erstellen. In diesem Verfahren wird beschrieben, wie Sie ein selbst gehostetes SiteWise Edge-Gateway erstellen, das Sie auf Ihrer eigenen Hardware installieren. Informationen zum Erstellen eines

SiteWise Edge-Gateways, das auf Siemens Industrial Edge läuft, finden Sie unterAusführen von SiteWise Edge auf Industrie Edge.

Erstellen Sie ein SiteWise Edge-Gateway

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Edge-Gateways aus.
3. Wählen Sie Create gateway (Gateway erstellen).
4. Wählen Sie als Bereitstellungstyp die Option Selbst gehostetes Gateway aus.
5. Geben Sie einen Namen für Ihr SiteWise Edge-Gateway ein oder verwenden Sie den von AWS IoT SiteWise generierten Namen.
6. Wählen Sie unter Greengrass-Gerätebetriebssystem das Betriebssystem des Geräts aus, auf dem Sie dieses SiteWise Edge-Gateway installieren möchten.

   > **Note**
   >
   > Das Data Processing Pack ist nur auf x86-Plattformen verfügbar.

7. (Optional) Um Daten am Edge zu verarbeiten und zu organisieren, wählen Sie unter Edge-Funktionen die Option Data Processing Pack aus.

   > **Note**
   >
   > Informationen dazu, wie Sie Benutzergruppen in Ihrem Unternehmensverzeichnis Zugriff auf dieses SiteWise Edge-Gateway gewähren, finden Sie unter Edge-Fähigkeit einrichten

8. (Optional) Gehen Sie unter „Erweiterte Konfiguration“ wie folgt vor:

   - Wählen Sie für das Greengrass-Core-Gerät eine der folgenden Optionen:
     - Standard-Setup — verwendet AWS automatisch die Standardeinstellungen, um ein Greengrass-Core-Gerät in AWS IoT Greengrass V2 zu erstellen.
       1. Geben Sie einen Namen für das Greengrass-Core-Gerät ein oder verwenden Sie den von AWS IoT SiteWise generierten Namen.
     - Erweiterte Einrichtung — Wählen Sie diese Option, wenn Sie ein vorhandenes Greengrass-Core-Gerät verwenden oder eines manuell erstellen möchten.

1. Wählen Sie ein Greengrass-Core-Gerät oder wählen Sie Create Greengrass Core-Gerät, um eines in der AWS IoT Greengrass V2 Konsole zu erstellen. Weitere Informationen finden Sie im AWS IoT Greengrass Version 2 Entwicklerhandbuch unter Einrichten von AWS IoT Greengrass V2 Kerngeräten.

9. Wählen Sie Create gateway (Gateway erstellen).
10. Wählen Sie im Dialogfeld „ SiteWise Edge-Gateway-Installationsprogramm generieren“ die Option Generieren und herunterladen aus. AWS IoT SiteWise generiert automatisch ein Installationsprogramm, mit dem Sie Ihr lokales Gerät konfigurieren können.

> **Important**
>
> Stellen Sie sicher, dass Sie die Installationsdatei an einem sicheren Ort speichern. Sie werden die Datei später verwenden.

Nachdem Sie das SiteWise Edge-Gateway erstellt haben, fügen Sie Datenquellen hinzu, konfigurieren Sie die Publisher-Komponente und sorgen Sie dafür, dass Ihr SiteWise Edge-Gateway Daten empfängt und an die AWS Cloud sendet.

Installieren der SiteWise Edge-Gateway-Software auf Ihrem lokalen Gerät

Sobald Sie ein SiteWise Edge-Gateway erstellt haben, müssen Sie die SiteWise Edge-Gateway-Software auf Ihrem lokalen Gerät installieren. SiteWise Die Edge-Gateway-Software kann auf lokalen Geräten installiert werden, auf denen Linux- oder Windows-Serverbetriebssysteme installiert sind.

> **Important**
>
> Stellen Sie sicher, dass Ihr lokales Gerät eine Verbindung zum Internet herstellt.

Linux

Das folgende Verfahren verwendet SSH, um eine Verbindung zu Ihrem lokalen Gerät herzustellen. Alternativ können Sie ein USB-Flash-Laufwerk oder andere Tools verwenden, um die Installationsdatei auf Ihr lokales Gerät zu übertragen. Wenn Sie SSH nicht verwenden

möchten, fahren Sie mit Schritt 2: Installieren der SiteWise Edge-Gateway-Software weiter unten fort.

SSH-Voraussetzungen

Bevor Sie über SSH eine Verbindung zu Ihrem Gerät herstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

- Rufen Sie die IP-Adresse Ihres Geräts ab.
- Rufen Sie den Benutzernamen ab, um eine Verbindung zu Ihrem Gerät herzustellen.
- Installieren Sie nach Bedarf einen SSH-Client auf Ihrem lokalen Computer.

  Auf Ihrem lokalen Computer ist möglicherweise standardmäßig ein SSH-Client installiert. Sie können dies überprüfen, indem Sie ssh in die Befehlszeile eingeben. Wenn Ihr Computer den Befehl nicht erkennt, können Sie einen SSH-Client installieren.

  - Linux und macOS – Laden Sie OpenSSH herunter und installieren Sie es. Weitere Informationen finden Sie unter https://www.openssh.com.

Schritt 1: Kopieren des Installationsprogramms auf Ihr SiteWise Edge-Gateway-Gerät

In den folgenden Anweisungen wird erläutert, wie Sie über einen SSH-Client eine Verbindung zu Ihrem lokalen Gerät herstellen.

1. Um eine Verbindung zu Ihrem Gerät herzustellen, führen Sie den folgenden Befehl in einem Terminalfenster auf Ihrem Computer aus und ersetzen Sie *Benutzername* und *IP* durch einen Benutzernamen mit erhöhten Rechten und einer IP-Adresse.

   ```
   ssh username@IP
   ```

2. Um die von AWS IoT SiteWise generierte Installationsdatei auf Ihr SiteWise Edge-Gateway-Gerät zu übertragen, führen Sie den folgenden Befehl aus.

   > **Note**
   >
   > - Ersetzen Sie durch *path-to-saved-installer* den Pfad auf Ihrem Computer, den Sie zum Speichern der Installationsdatei verwendet haben, und den Namen der Installationsdatei.
   > - Ersetzen Sie *IP-address* durch die IP-Adresse Ihres lokalen Geräts.

- Ersetzen Sie durch *directory-to-receive-installer* den Pfad auf Ihrem lokalen Gerät, den Sie zum Empfangen der Installationsdatei verwenden.

```
scp path-to-saved-installer.sh user-name@IP-address:directory-to-receive-
installer
```

Schritt 2: Installieren der SiteWise Edge-Gateway-Software

Führen Sie in den folgenden Verfahren die Befehle in einem Terminalfenster auf Ihrem SiteWise Edge-Gateway-Gerät aus.

1. Erteilen Sie der Installationsdatei die Ausführungsberechtigung.

```
chmod +x path-to-installer.sh
```

2. Führen Sie das Installationsprogramm aus.

```
sudo ./path-to-installer.sh
```

Windows server

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, um die SiteWise Edge-Gateway-Software installieren zu können:

- Windows Server 2019 oder höher installiert
- Administratorrechte
- PowerShell -Version 5.1 oder höher installiert
- SiteWise Das Edge-Gateway-Installationsprogramm wurde auf den Windows Server heruntergeladen, wo es bereitgestellt wird

Schritt 1: PowerShell Als Administrator ausführen

1. Melden Sie sich auf dem Windows-Server, auf dem Sie das SiteWise Edge-Gateway installieren möchten, als Administrator an.

2. Geben Sie PowerShell in die Windows-Suchleiste ein.
3. Öffnen Sie in den Suchergebnissen das Kontextmenü (rechte Maustaste) in der Windows-PowerShell App. Wählen Sie Als Administrator ausführen aus.

Schritt 2: Installieren der SiteWise Edge-Gateway-Software

Führen Sie die folgenden Befehle in einem Terminalfenster auf Ihrem SiteWise Edge Gateway-Gerät aus.

1. Entsperren Sie das SiteWise Edge-Gateway-Installationsprogramm.

```
unblock-file path-to-installer.ps1
```

2. Führen Sie das Installationsprogramm aus.

```
./path-to-installer.ps1
```

> **Note**
>
> Wenn die Skriptausführung auf dem System deaktiviert ist, ändern Sie die Skriptausführungsrichtlinie in `RemoteSigned`.
>
> ```
> Set-ExecutionPolicy RemoteSigned
> ```

Aktivierung der Edge-Datenverarbeitung

Sie können AWS IoT SiteWise Edge verwenden, um Gerätedaten lokal zu sammeln, zu speichern, zu organisieren und zu überwachen. Sie können SiteWise Edge verwenden, um Ihre Industriedaten zu modellieren, und SiteWise Monitor verwenden, um Dashboards zu erstellen, mit denen Ihr Betriebspersonal Daten lokal visualisieren kann. Sie können Ihre Daten lokal verarbeiten und an die AWS Cloud senden oder sie mithilfe der AWS IoT SiteWise API vor Ort verarbeiten.

Mit AWS IoT SiteWise Edge können Sie Rohdaten lokal verarbeiten und festlegen, dass nur aggregierte Daten an die gesendet werden, um Ihre Bandbreitennutzung und Ihre Cloud-Speicherkosten AWS Cloud zu optimieren.

> **Note**
>
> - AWS IoT SiteWise speichert Ihre Edge-Daten bis zu 30 Tage auf Ihren SiteWise Edge-Gateways. Die Aufbewahrungsdauer Ihrer Daten hängt vom verfügbaren Speicherplatz Ihres Geräts ab.
> - Wenn Ihr SiteWise Edge-Gateway 30 Tage lang nicht mit dem AWS Cloud verbunden war, wird das Data Processing Pack automatisch deaktiviert.

Edge-Fähigkeit einrichten

AWS IoT SiteWise stellt die folgenden Pakete bereit, anhand SiteWise derer Ihr Edge-Gateway bestimmen kann, wie Ihre Daten erfasst und verarbeitet werden sollen. Wählen Sie Pakete aus, um Edge-Funktionen für Ihr SiteWise Edge-Gateway zu aktivieren.

- Das Datenerfassungspaket ermöglicht es Ihrem SiteWise Edge-Gateway, Daten von mehreren OPC-UA-Servern zu sammeln und die Daten dann vom Edge zum zu exportieren. AWS Cloud Es wird aktiv, sobald Sie Ihrem SiteWise Edge-Gateway Datenquellen hinzugefügt haben.
- Mit dem Data Processing Pack kann Ihr SiteWise Edge-Gateway Ihre Gerätedaten am Edge verarbeiten. Sie können beispielsweise Anlagenmodelle verwenden, um Metriken und Transformationen zu berechnen. Weitere Informationen zu Anlagenmodellen und Vermögenswerten finden Sie unterModellieren von industriellen Komponenten.

> **Note**
>
> - Das Data Processing Pack ist nur auf x86-Plattformen verfügbar.
> - Das Data Processing Pack unterstützt keine Netzwerk-Proxys.

Um Edge-Funktionen zu konfigurieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Edge-Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, für das Sie Edge-Funktionen aktivieren möchten.
4. Wählen Sie im Abschnitt Edge-Funktionen die Option Bearbeiten

5. Wählen Sie im Abschnitt Edge-Funktionen die Option Datenverarbeitungspaket aktivieren aus (es fallen zusätzliche Gebühren an).
6. (Optional) Im Abschnitt Edge-LDAP-Verbindung können Sie Benutzergruppen in Ihrem Unternehmensverzeichnis Zugriff auf dieses SiteWise Edge-Gateway gewähren. Die Benutzergruppen können die LDAP-Anmeldeinformationen (Lightweight Directory Access Protocol) verwenden, um auf das SiteWise Edge-Gateway zuzugreifen. Anschließend können sie die AWS OpsHub für AWS IoT SiteWise Anwendungen, AWS IoT SiteWise API-Operationen oder andere Tools verwenden, um das SiteWise Edge-Gateway zu verwalten. Weitere Informationen finden Sie unter Verwalten von SiteWise Edge-Gateways.

   > **Note**
   >
   > Sie können auch die Linux- oder Windows-Anmeldeinformationen verwenden, um auf das SiteWise Edge-Gateway zuzugreifen. Weitere Informationen finden Sie unter Zugreifen auf Ihr SiteWise Edge-Gateway mit Linux-Betriebssystemanmeldeinformationen.

   a. Wählen Sie Aktiviert aus.
   b. Geben Sie unter Anbietername einen Namen für Ihren LDAP-Anbieter ein.
   c. Geben Sie für Hostname oder IP-Adresse den Hostnamen oder die IP-Adresse Ihres LDAP-Servers ein.
   d. Geben Sie für Port eine Portnummer ein.
   e. Geben Sie für Base Distinguished Name (DN) einen definierten Namen (DN) für die Basis ein.

      Die folgenden Attributtypen werden unterstützt: CommonName (CN), LocalityName (L), Name (ST), stateOrProvince OrganizationName (O), (OU), CountryName organizationalUnitName (C), StreetAddress (STREET), DomainComponent (DC) und userid (UID).
   f. Geben Sie für Admin-Gruppen-DN einen DN ein.
   g. Geben Sie für Benutzergruppen-DN einen DN ein.
7. Wählen Sie Speichern.

Nachdem Sie die Edge-Funktionen auf Ihrem SiteWise Edge-Gateway aktiviert haben, müssen Sie Ihr Asset-Modell für das Edge konfigurieren. Die Edge-Konfiguration Ihres Asset-Modells gibt an, wo Ihre Asset-Eigenschaften berechnet werden. Sie können alle Eigenschaften am Rand berechnen oder Sie können die Eigenschaften Ihres Asset-Modells separat konfigurieren. Zu den Eigenschaften des Anlagenmodells gehören Metriken, Transformationen und Messungen.

Weitere Informationen zu Asset-Eigenschaften finden Sie unterthe section called “Definieren von Dateneigenschaften”.

Nachdem Sie Ihr Asset-Modell erstellt haben, können Sie es für den Edge konfigurieren. Weitere Informationen zur Konfiguration Ihres Asset-Modells für den Edge finden Sie unterthe section called “Erstellen eines Komponentenmodells (Konsole)”.

> **Note**
>
> Asset-Modelle und Dashboards werden automatisch alle 10 Minuten zwischen dem AWS Cloud und Ihrem SiteWise Edge-Gateway synchronisiert. Sie können die Synchronisierung auch manuell über die lokale SiteWise Edge-Gateway-Anwendung durchführen.

Verarbeiten von Daten am Edge

Sie müssen Ihr Komponentenmodell für den Edge konfigurieren, bevor Ihr Ihre SiteWise Edge-Gateway-Daten am Edge verarbeiten kann. Ihre Edge-Konfiguration des Komponentenmodells gibt an, wo Ihre Komponenteneigenschaften berechnet werden. Sie können alle Eigenschaften am Edge berechnen und die Ergebnisse an die senden oder anpassen AWS Cloud, wo jede Komponenteneigenschaft separat berechnet werden soll. Weitere Informationen finden Sie unter Aktivierung der Edge-Datenverarbeitung.

Zu den Komponenteneigenschaften gehören Metriken, Transformationen und Messungen:

- Metriken sind die aggregierten Daten der Komponente über einen bestimmten Zeitraum. Sie können neue Metriken berechnen, indem Sie vorhandene Metrikdaten verwenden. sendet Ihre Metriken AWS IoT SiteWise standardmäßig zur langfristigen Speicherung an die AWS Cloud. AWS IoT SiteWise berechnet Metriken in der AWS Cloud. Sie können Ihr Komponentenmodell so konfigurieren, dass es Ihre Metriken am Edge berechnet. AWS IoT SiteWise sendet verarbeitete Ergebnisse an die AWS Cloud.
- Transformationen sind mathematische Ausdrücke, die die Datenpunkte einer Komponenteneigenschaft aus einer Form in eine andere Form abbilden. Transformationen können

Metriken als Eingabedaten verwenden und müssen am selben Ort wie ihre Eingaben berechnet und gespeichert werden. Wenn Sie eine Metrikeingabe für die Berechnung am Edge konfigurieren, berechnet AWS IoT SiteWise auch die zugehörige Transformation am Edge.

- Messungen sind als Rohdaten formatiert, die Ihr Gerät standardmäßig sammelt und an die AWS Cloud sendet. Sie können Ihr Komponentenmodell so konfigurieren, dass diese Daten auf Ihrem lokalen Gerät gespeichert werden.

Weitere Informationen zu Komponenteneigenschaften finden Sie unter the section called “Definieren von Dateneigenschaften”.

Nachdem Sie Ihr Komponentenmodell erstellt haben, können Sie es dann für den Edge konfigurieren. Weitere Informationen zur Konfiguration Ihres Komponentenmodells für die Kante finden Sie unter the section called “Erstellen eines Komponentenmodells (Konsole)”.

> **Note**
>
> Komponentenmodelle und Dashboards werden alle 10 Minuten automatisch zwischen der AWS Cloud und Ihrem SiteWise Edge-Gateway synchronisiert. Sie können auch manuell über die synchronisierenVerwalten von SiteWise Edge-Gateways.

Sie können die AWS IoT SiteWise REST-APIs und die AWS Command Line Interface (AWS CLI) verwenden, um Ihr SiteWise Edge-Gateway nach Daten am Edge abzufragen. Bevor Sie Ihr SiteWise Edge-Gateway nach Daten am Edge abfragen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Ihre Anmeldeinformationen müssen für die REST-APIs festgelegt werden. Weitere Informationen zum Festlegen von Anmeldeinformationen finden Sie unter the section called “Verwalten von SiteWise Edge-Gateways”.
- Der SDK-Endpunkt muss auf die IP-Adresse Ihres SiteWise Edge-Gateways verweisen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem SDK. Weitere Informationen finden Sie unter Angeben von benutzerdefinierten Endpunkten im AWS SDK for Java 2.x Entwicklerhandbuch für .
- Ihr SiteWise Edge-Gateway-Zertifikat muss registriert sein. Weitere Informationen zur Registrierung Ihres SiteWise Edge-Gateway-Zertifikats finden Sie in der Dokumentation für Ihr SDK. Weitere Informationen finden Sie unter Registrieren von Zertifikatpaketen in Node.js im AWS SDK for Java 2.x Entwicklerhandbuch für .

Weitere Informationen zum Abfragen von Daten mit AWS IoT SiteWisefinden Sie unter Daten abfragen von AWS IoT SiteWise.

Konfiguration der AWS IoT SiteWise Publisher-Komponente

Nachdem Sie ein AWS IoT SiteWise Edge-Gateway erstellt und die Software installiert haben, richten Sie die Publisher-Komponente so ein, dass Ihr SiteWise Edge-Gateway Daten in die AWS Cloud exportieren kann. Weitere Informationen finden Sie unter AWS IoT SiteWise Publisher im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

Console

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Edge-Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, für das Sie den Publisher konfigurieren möchten.
4. Wählen Sie im Abschnitt Publisher-Konfiguration die Option Bearbeiten
5. Wählen Sie für die Reihenfolge der Veröffentlichung eine der folgenden Optionen aus:

   - Älteste Daten zuerst veröffentlichen — Das SiteWise Edge-Gateway veröffentlicht die ältesten Daten standardmäßig zuerst in der Cloud.
   - Neueste Daten zuerst veröffentlichen — Das SiteWise Edge-Gateway veröffentlicht die neuesten Daten zuerst in der Cloud.
6. (Optional) Wenn Sie nicht möchten, dass das SiteWise Edge-Gateway Ihre Daten komprimiert, deaktivieren Sie die Option Komprimierung beim Hochladen von Daten aktivieren.
7. (Optional) Wenn Sie keine alten Daten veröffentlichen möchten, wählen Sie „Abgelaufene Daten ausschließen“ und gehen Sie wie folgt vor:

   - Geben Sie für den Stichtag einen Wert ein und wählen Sie eine Einheit aus. Die Sperrfrist muss zwischen fünf Minuten und sieben Tagen liegen. Wenn die Sperrfrist beispielsweise drei Tage beträgt, werden Daten, die älter als drei Tage sind, nicht in der Cloud veröffentlicht.
8. (Optional) Um benutzerdefinierte Einstellungen für den Umgang mit Daten auf Ihrem lokalen Gerät festzulegen, wählen Sie Lokale Speichereinstellungen und gehen Sie wie folgt vor:

a. Geben Sie für den Aufbewahrungszeitraum eine Zahl ein und wählen Sie eine Einheit aus. Der Aufbewahrungszeitraum muss zwischen einer Minute und 30 Tagen liegen und mindestens dem Rotationszeitraum entsprechen. Wenn die Aufbewahrungsfrist beispielsweise 14 Tage beträgt, löscht das SiteWise Edge-Gateway alle Daten am Edge, die älter als die angegebene Sperrfrist sind, nachdem sie 14 Tage lang gespeichert wurden.

b. Geben Sie für den Rotationszeitraum eine Zahl ein und wählen Sie eine Einheit aus. Der Rotationszeitraum muss länger als eine Minute und gleich oder kürzer als der Aufbewahrungszeitraum sein. Angenommen, der Rotationszeitraum beträgt zwei Tage. Das SiteWise Edge-Gateway sammelt Daten, die älter als die Sperrfrist sind, und speichert sie in einer einzigen Datei. Das SiteWise Edge-Gateway überträgt alle zwei Tage einen Datenstapel in das folgende lokale Verzeichnis:. `/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`

c. Geben Sie für Speicherkapazität einen Wert ein, der größer oder gleich 1 ist. Wenn die Speicherkapazität 2 GB beträgt, beginnt das SiteWise Edge-Gateway mit dem Löschen von Daten, wenn mehr als 2 GB an Daten lokal gespeichert sind.

9. Wählen Sie Speichern.

AWS CLI

Sie können die UpdateGatewayCapabilityConfigurationAPI verwenden, um den Herausgeber zu konfigurieren. Stellen Sie den Parameter `capabilityNamespace` auf `iotsitewise:publisher:2` ein.

Der Herausgeber stellt die folgenden Konfigurationsparameter bereit, die Sie anpassen können:

`SiteWisePublisherConfiguration`

`publishingOrder`

Die Reihenfolge, in der Daten in der Cloud veröffentlicht werden. Der Wert dieses Parameters kann einer der folgenden sein:

- `TIME_ORDER`(Älteste Daten zuerst veröffentlichen) — Die frühesten Daten werden standardmäßig zuerst in der Cloud veröffentlicht.
- `RECENT_DATA`(Neueste Daten zuerst veröffentlichen) — Die neuesten Daten werden zuerst in der Cloud veröffentlicht.

`dropPolicy`

(Optional) Eine Richtlinie, die steuert, welche Daten in der Cloud veröffentlicht werden.

`cutoffAge`

Daten, die vor dem Stichtag liegen, werden nicht in der Cloud veröffentlicht. Das Mindestalter muss zwischen fünf Minuten und sieben Tagen liegen.

Sie können, und verwenden `m`h, `d` wenn Sie ein Mindestalter angeben. Hinweis, `m` der Minuten, `h` Stunden und Tage `d` darstellt.

`exportPolicy`

(Optional) Eine Richtlinie, die die Datenspeicherung am Netzwerkrand verwaltet. Diese Richtlinie gilt für Daten, die vor dem Stichtag liegen.

`retentionPeriod`

Ihr SiteWise Edge-Gateway löscht alle Daten am Edge, die vor dem Sperrzeitraum liegen, aus dem lokalen Speicher, nachdem sie für den angegebenen Aufbewahrungszeitraum gespeichert wurden. Die Aufbewahrungsdauer muss zwischen einer Minute und 30 Tagen liegen und mindestens dem Rotationszeitraum entsprechen.

Sie können`m`, und verwenden`h`, `d` wenn Sie einen Aufbewahrungszeitraum angeben. Hinweis, `m` der Minuten, `h` Stunden und Tage `d` darstellt.

`rotationPeriod`

Das Zeitintervall, über das Daten, die vor dem Stichtag liegen, gebündelt und in einer einzigen Datei gespeichert werden sollen. Das SiteWise Edge-Gateway überträgt am Ende jeder Rotationsperiode einen Datenstapel in das folgende lokale Verzeichnis:`/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/exports`. Der Rotationszeitraum muss länger als eine Minute und gleich oder kürzer als der Aufbewahrungszeitraum sein.

Sie können`m`, und verwenden`h`, `d` wenn Sie einen Rotationszeitraum angeben. Hinweis, `m` der Minuten, `h` Stunden und Tage `d` darstellt.

`exportSizeLimitGB`

Die maximal zulässige Größe der lokal gespeicherten Daten in GB. Wenn dieses Kontingent überschritten wird, beginnt das SiteWise Edge-Gateway mit dem

Löschen der frühesten Daten, bis die Größe der lokal gespeicherten Daten dem Kontingent entspricht oder darunter liegt. Der Wert dieses Parameters muss größer oder gleich 1 sein.

Example Publisher-Konfiguration:

Der Herausgeber-Namespace: `iotsitewise:publisher:2`

```
{
"SiteWisePublisherConfiguration": {
    "publishingOrder": "TIME_ORDER",
    "dropPolicy": {
        "cutoffAge": "7d",
        "exportPolicy": {
            "retentionPeriod": "7d",
            "rotationPeriod": "6h",
            "exportLocation": "/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/
exports",
            "exportSizeLimitGB": 10
        }
    }
}
}
```

Konfigurieren von Datenquellen

Nachdem Sie ein AWS IoT SiteWise Edge-Gateway eingerichtet haben, können Sie Datenquellen so konfigurieren, dass Ihr SiteWise Edge-Gateway Daten von lokalen Industrieanlagen aufnehmen kann. AWS IoT SiteWise Jede Quelle steht für einen lokalen Server, z. B. einen OPC-UA-Server, mit dem Ihr SiteWise Edge-Gateway eine Verbindung herstellt und industrielle Datenströme abruft. Weitere Informationen zum Einrichten eines SiteWise Edge-Gateways finden Sie unter. Konfiguration eines AWS IoT Greengrass V1 SiteWise Edge-Gateways

> **Note**
>
> AWS IoT SiteWise startet Ihr SiteWise Edge-Gateway jedes Mal neu, wenn Sie eine Quelle hinzufügen oder bearbeiten. Ihr SiteWise Edge-Gateway nimmt während des Neustarts keine Daten auf. Die Zeit für den Neustart Ihres SiteWise Edge-Gateways hängt von der Anzahl der Tags in den Quellen Ihres SiteWise Edge-Gateways ab. Die Neustartzeit kann zwischen

einigen Sekunden (für ein SiteWise Edge-Gateway mit wenigen Tags) und mehreren Minuten (für ein SiteWise Edge-Gateway mit vielen Tags) liegen.

Nachdem Sie Quellen erstellt haben, können Sie Ihre Datenströme mit Asset-Eigenschaften verknüpfen. Weitere Informationen zum Erstellen und Verwenden von Assets finden Sie unter Modellieren von industriellen Komponenten undZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Sie können CloudWatch Messwerte anzeigen, um zu überprüfen, ob eine Datenquelle verbunden ist AWS IoT SiteWise. Weitere Informationen finden Sie unter AWS IoT Greengrass Version 2 Gateway-Metriken.

AWS IoT SiteWise Unterstützt derzeit die folgenden Datenquellenprotokolle:

- OPC-UA — Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung.

> **Note**
>
> SiteWise Edge-Gateways, auf denen AWS IoT Greengrass V2 derzeit läuft, unterstützen Modbus TCP- und Ethernet-IP-Quellen nicht.

Themen

Konfigurieren Sie eine OPC-UA-Quelle

Sie können die AWS IoT SiteWise Konsole oder eine SiteWise Edge-Gateway-Funktion verwenden, um eine OPC-UA-Quelle zu definieren und zu Ihrem SiteWise Edge-Gateway hinzuzufügen, die einen lokalen OPC-UA-Server darstellt.

Themen

- Konfigurieren Sie eine OPC-UA-Quelle (Konsole)
- Konfiguration einer OPC-UA-Quelle (CLI)
- Ermöglicht es Ihren OPC-UA-Quellservern, dem SiteWise Edge-Gateway zu vertrauen
- Filtern Sie Datenaufnahmebereiche mit OPC-UA
- Verwenden von OPC-UA-Knotenfiltern

Konfigurieren Sie eine OPC-UA-Quelle (Konsole)

Um eine OPC-UA-Quelle mit der Konsole zu konfigurieren AWS IoT SiteWise

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, um eine OPC-UA-Quelle hinzuzufügen.
4. Wählen Sie Datenquelle hinzufügen aus.
5. Geben Sie einen Namen für die Quelle ein.
6. Geben Sie den Local endpoint (Lokaler Endpunkt) des Datenquellenservers ein. Der Endpunkt kann die IP-Adresse oder der Hostname sein. Sie können dem lokalen Endpunkt auch eine Portnummer hinzufügen. Ihr lokaler Endpunkt könnte beispielsweise so aussehen: **`opc.tcp://203.0.113.0:49320`**

   > **Note**
   >
   > Wenn Ihr SiteWise Edge-Gateway über ein `Deployment type` neues Siemens Industrial Edge-Gerät verfügt und Sie Daten aus der Edge OPC UA Server-Anwendung aufnehmen möchten, die auf demselben Siemens Industrial Edge-Gerät wie die AWS IoT SiteWise Edge-Anwendung ausgeführt wird, geben Sie Folgendes ein. **`opc.tcp://ie-opcua:48010`**

7. (Optional) Fügen Sie unter Knoten-ID zur Auswahl Knotenfilter hinzu, um einzuschränken, welche Datenströme in den aufgenommen werden. AWS Cloud Standardmäßig verwenden SiteWise Edge-Gateways den Stammknoten eines Servers, um alle Datenströme aufzunehmen. Sie können Knotenfilter verwenden, um die Startzeit und die CPU-Auslastung Ihres SiteWise Edge-Gateways zu reduzieren, indem Sie nur Pfade zu Daten einbeziehen, die Sie modellieren. AWS IoT SiteWise Standardmäßig laden SiteWise Edge-Gateways alle OPC-UA-Pfade hoch, außer denen, die mit beginnen. `/Server/` Um OPC-UA-Knotenfilter zu definieren, können Sie

Knotenpfade und die Platzhalterzeichen * und ** verwenden. Weitere Informationen finden Sie unter Verwenden von OPC-UA-Knotenfiltern.

8. Wählen Sie unter Ziele das Ziel für die Quelldaten aus:

   - AWS IoT SiteWise Echtzeit — Wählen Sie diese Option, um Daten direkt an den AWS IoT SiteWise Speicher zu senden. Erfassen und überwachen Sie Daten in Echtzeit und verarbeiten Sie Daten am Netzwerkrand.
   - AWS IoT SiteWise Mit Amazon S3 gepuffert — Daten im Parquet-Format an Amazon S3 senden und dann in den AWS IoT SiteWise Speicher importieren. Wählen Sie diese Option, um Daten stapelweise aufzunehmen und historische Daten kostengünstig zu speichern. Sie können Ihren bevorzugten Amazon S3-Bucket-Standort und die Häufigkeit, mit der Daten auf Amazon S3 hochgeladen werden sollen, konfigurieren. Sie können auch wählen, was mit den Daten nach der Aufnahme geschehen soll. AWS IoT SiteWise Sie können wählen, ob die Daten SiteWise sowohl in Amazon S3 als auch in Amazon S3 verfügbar sein sollen, oder Sie können wählen, ob sie automatisch aus Amazon S3 gelöscht werden sollen.
     - Der Amazon S3 S3-Bucket ist ein Staging- und Puffermechanismus und unterstützt Dateien im Parquet-Format.
     - Wenn Sie das Kontrollkästchen Daten in AWS IoT SiteWise Speicher importieren aktivieren, werden Daten zuerst in Amazon S3 und dann in den AWS IoT SiteWise Speicher hochgeladen.
       - Wenn Sie das Kontrollkästchen Daten aus Amazon S3 löschen aktivieren, werden Daten aus Amazon S3 gelöscht, nachdem sie in den SiteWise Speicher importiert wurden.
       - Wenn Sie das Kontrollkästchen Daten aus Amazon S3 löschen deaktivieren, werden Daten sowohl in Amazon S3 als auch im SiteWise Speicher gespeichert.
     - Wenn Sie das Kontrollkästchen Daten in AWS IoT SiteWise Speicher importieren deaktivieren, werden Daten nur in Amazon S3 gespeichert. Sie werden nicht in den SiteWise Speicher importiert.

     Einzelheiten Verwaltung des Datenspeichers zu den verschiedenen Speicheroptionen finden Sie AWS IoT SiteWise unter. Weitere Informationen zu den Preisoptionen finden Sie unter AWS IoT SiteWise Preise.
   - AWS IoT Greengrass Stream-Manager — Verwenden Sie den AWS IoT Greengrass Stream-Manager, um Daten an die folgenden AWS Cloud Ziele zu senden: Kanäle in AWS IoT Analytics, Streams in Amazon Kinesis Data Streams, Asset-Eigenschaften in AWS IoT SiteWise oder Objekte in Amazon Simple Storage Service (Amazon S3). Weitere

Informationen finden Sie im AWS IoT Greengrass Version 2 Entwicklerhandbuch unter Datenstreams auf dem AWS IoT Greengrass Core verwalten.

Geben Sie einen Namen für den AWS IoT Greengrass Stream ein.

Bei der Konfiguration einer Datenquelle wird die Knoten-ID zur Auswahl verwendet, um das Ziel des Datenflusses zu bestimmen.

- Wenn dieselben Daten mit Amazon S3 sowohl AWS IoT SiteWise in Echtzeit als auch inAWS IoT SiteWise Buffered veröffentlicht werden, müssen Sie zwei Datenquellen hinzufügen, die an beiden Zielen veröffentlichen.
- Um die Daten so aufzuteilen, dass ein Teil davon AWS IoT SiteWise in Echtzeit und der andere Teil mithilfe von Amazon S3 in AWS IoT SiteWise Buffered veröffentlicht wird, müssen Sie nach den folgenden Datenaliasen filtern:

```
/Alias01/Data1
/Alias02/Data1
/Alias03/Data1
/Alias03/Data2
```

Beispielsweise können Sie mithilfe von Amazon S3 eine Datenquelle hinzufügen, die auf den **`/**/Data1`** Node-Filter verweist AWS IoT SiteWise , und eine weitere Datenquelle, die auf **`/**/Data2`**AWS IoT SiteWise Buffered verweist

9. Im Bereich Erweiterte Konfiguration können Sie wie folgt vorgehen:

   a. Wählen Sie einen Nachrichtensicherheitsmodus für Verbindungen und Daten, die zwischen Ihrem Quellserver und Ihrem SiteWise Edge-Gateway übertragen werden. Dieses Feld ist die Kombination aus der OPC-UA-Sicherheitsrichtlinie und dem Nachrichtensicherheitsmodus. Wählen Sie dieselbe Sicherheitsrichtlinie und denselben Nachrichtensicherheitsmodus, die Sie für Ihren OPC-UA-Server angegeben haben.

   b. Wenn Ihre Quelle eine Authentifizierung erfordert, wählen Sie ein AWS Secrets Manager Geheimnis aus der Authentifizierungskonfigurationsliste aus. Das SiteWise Edge-Gateway verwendet die Authentifizierungsanmeldeinformationen in diesem Geheimnis, wenn es eine Verbindung zu dieser Datenquelle herstellt. Sie müssen Geheimnisse an die AWS IoT Greengrass Komponente Ihres SiteWise Edge-Gateways anhängen, um sie für die Datenquellenauthentifizierung verwenden zu können. Weitere Informationen finden Sie unter the section called “Konfiguration der Datenquellenauthentifizierung”.

> **Tip**
>
> Ihr Datenserver verfügt möglicherweise über die Option Allow anonymous login (Anonyme Anmeldung zulassen). Wenn diese Option Yes (Ja) zeigt, ist für Ihre Quelle keine Authentifizierung erforderlich.

c. (Optional) Geben Sie ein Datenstream-Präfix ein. Das SiteWise Edge-Gateway fügt dieses Präfix allen Datenströmen aus dieser Quelle hinzu. Verwenden Sie ein Datenstrom-Präfix, um zwischen Datenströmen mit demselben Namen aus verschiedenen Quellen zu unterscheiden. Jeder Datenstrom sollte einen eindeutigen Namen in Ihrem Konto haben.

d. (Optional) Wählen Sie für Eigenschaftsgruppen die Option Neue Gruppe hinzufügen aus.

   i. Geben Sie einen Namen für die Eigenschaftsgruppe ein.

   ii. Für Eigenschaften:

      1. Fügen Sie für Knotenpfade OPC-UA-Knotenfilter hinzu, um einzuschränken, in welche OPC-UA-Pfade hochgeladen werden. AWS IoT SiteWise Das Format ähnelt der Knoten-ID für die Auswahl.

   iii. Gehen Sie für Gruppeneinstellungen wie folgt vor:

      1. Wählen Sie unter Datenqualitätseinstellung den Datenqualitätstyp aus, den AWS IoT SiteWise Collector aufnehmen soll.
      2. Konfigurieren Sie für die Einstellung für den Scanmodus die folgenden Standard-Abonnementeigenschaften:
         - Wählen Sie für den Scanmodus eine der folgenden Optionen: Weitere Informationen zum Scanmodus finden Sie unterthe section called “Filtern von Datenaufnahmebereichen mit OPC-UA”.
            - Um jeden Datenpunkt zu senden, wählen Sie Abonnieren und stellen Sie Folgendes ein:
               - Auslöser für Datenänderungen — Die Bedingung, die eine Warnung bei Datenänderungen auslöst.
               - Größe der Abonnement-Warteschlange — Die Tiefe der Warteschlange auf einem OPC-UA-Server für eine bestimmte Metrik, in der Benachrichtigungen für überwachte Elemente in die Warteschlange gestellt werden.

- Veröffentlichungsintervall für Abonnements — Das Intervall (in Millisekunden) des Veröffentlichungszyklus, das bei der Erstellung des Abonnements angegeben wurde.
- Snapshot-Intervall — Die Timeout-Einstellung für die Snapshot-Frequenz, um sicherzustellen, dass AWS IoT SiteWise Edge einen stetigen Datenstrom aufnimmt.
- Scanrate — Die Geschwindigkeit, mit der das SiteWise Edge-Gateway Ihre Register lesen soll. AWS IoT SiteWise berechnet automatisch die minimal zulässige Scanrate für Ihr SiteWise Edge-Gateway.

- Um Datenpunkte in einem bestimmten Intervall zu senden, wählen Sie Poll und geben Sie eine Scanrate ein.

3. Wenn Sie den Scanmodus „Abonnieren“ wählen, konfigurieren Sie einen Deadband-Typ und die entsprechenden Einstellungen für Ihre Quelle. Dadurch wird gesteuert, welche Daten Ihre Quelle an Ihre AWS IoT SiteWise sendet und welche Daten sie verwirft. Weitere Informationen zur Deadband-Einstellung finden Sie unter. the section called “Filtern von Datenaufnahmebereichen mit OPC-UA”

10. Wählen Sie Speichern.

Konfiguration einer OPC-UA-Quelle (CLI)

Sie können OPC-UA-Datenquellen für ein SiteWise Edge-Gateway mithilfe der definieren. AWS CLI Erstellen Sie dazu eine JSON-Datei mit der OPC-UA-Fähigkeitskonfiguration und aktualisieren Sie mit dem update-gateway-capability-configurationBefehl die Edge-Gateway-Konfiguration. SiteWise Sie müssen alle OPC-UA-Quellen in einer einzigen Funktionskonfiguration definieren.

Diese Funktion hat den folgenden Namespace.

- `iotsitewise:opcuacollector:2`

Erforderliche Syntax

```
{
  "sources": [
    {
      "name": "string",
      "endpoint": {
        "certificateTrust": {
```

```
          "type": "TrustAny" | "X509",
          "certificateBody": "string",
          "certificateChain": "string",
        },
        "endpointUri": "string",
        "securityPolicy": "NONE" | "BASIC128_RSA15" | "BASIC256" | "BASIC256_SHA256" |
 "AES128_SHA256_RSAOAEP" | "AES256_SHA256_RSAPSS",
        "messageSecurityMode": "NONE" | "SIGN" | "SIGN_AND_ENCRYPT",
        "identityProvider": {
          "type": "Anonymous" | "Username",
          "usernameSecretArn": "string"
        },
        "nodeFilterRules": [
          {
            "action": "INCLUDE",
            "definition": {
              "type": "OpcUaRootPath",
              "rootPath": "string"
            }
          }
        ]
      },
      "measurementDataStreamPrefix": "string"
     "destination": {
        "type": "StreamManager",
        "streamName": "string",
        "streamBufferSize": integer
      },
      "propertyGroups": [
        {
          "name": "string",
          "nodeFilterRuleDefinitions": [
            {
              "type": "OpcUaRootPath",
              "rootPath": "string"
            }
          ],
          "deadband": {
            "type": "PERCENT" | "ABSOLUTE",
            "value": double,
            "eguMin": double,
            "eguMax": double,
            "timeoutMilliseconds": integer
          },
```

```
          "scanMode": {
            "type": "EXCEPTION" | "POLL",
            "rate": integer
          },
          "dataQuality": {
            "allowGoodQuality": true | false,
            "allowBadQuality": true | false,
            "allowUncertainQuality": true | false
          },
          "subscription": {
            "dataChangeTrigger": "STATUS" | "STATUS_VALUE" | "STATUS_VALUE_TIMESTAMP",
            "queueSize": integer,
            "publishingIntervalMilliseconds": integer,
            "snapshotFrequencyMilliseconds": integer
          }
        }
      ]
    }
  ]
}
```

Anforderungstext

Quellen

Eine Liste der OPC-UA-Quelldefinitionsstrukturen, die jeweils die folgenden Informationen enthalten:

Name

Ein eindeutiger und aussagekräftiger Name für die Quelle.

Endpunkt

Eine Endpunktstruktur, die die folgenden Informationen enthält:

CertificateTrust

Eine Zertifikatvertrauensrichtlinienstruktur, die die folgenden Informationen enthält:

Typ

Der Zertifikatvertrauensmodus für die Quelle. Wählen Sie eine der folgenden Optionen aus:

- **`TrustAny`**— Das SiteWise Edge-Gateway vertraut jedem Zertifikat, wenn es eine Verbindung zur OPC-UA-Quelle herstellt.
- `X509`— Das SiteWise Edge-Gateway vertraut einem X.509-Zertifikat, wenn es eine Verbindung zur OPC-UA-Quelle herstellt. Wenn Sie diese Option wählen, müssen Sie `certificateBody` in `certificateTrust` definieren. Sie können auch `certificateChain` in `certificateTrust` definieren.

Stelle des Zertifikats

(Optional) Der Hauptteil eines X.509-Zertifikats.

Dieses Feld ist erforderlich, wenn Sie `X509` für `type` in `certificateTrust` auswählen.

certificateChain

(Optional) Die Vertrauenskette für ein X.509-Zertifikat.

Dieses Feld wird nur verwendet, wenn Sie `X509` für `type` in `certificateTrust` auswählen.

Endpunkt-URI

Der lokale Endpunkt der OPC-UA-Quelle. Der lokale Endpunkt könnte z. B. wie `opc.tcp://203.0.113.0:49320` aussehen.

Sicherheitsrichtlinie

Die Sicherheitsrichtlinie, die verwendet werden soll, damit Sie Nachrichten schützen können, die aus der OPC-UA-Quelle gelesen werden. Wählen Sie eine der folgenden Optionen aus:

- `NONE`— Das SiteWise Edge-Gateway schützt keine Nachrichten von der OPC-UA-Quelle. Wir empfehlen Ihnen, eine andere Sicherheitsrichtlinie zu wählen. Wenn Sie diese Option wählen, müssen Sie auch `NONE` für `messageSecurityMode` auswählen.
- `BASIC256_SHA256`— Die `Basic256Sha256` Sicherheitsrichtlinie.
- `AES128_SHA256_RSAOAEP`— Die `Aes128_Sha256_RsaOaep` Sicherheitspolitik.
- `AES256_SHA256_RSAPSS`— Die `Aes256_Sha256_RsaPss` Sicherheitspolitik.
- `BASIC128_RSA15`— (Veraltet) Die `Basic128Rsa15` Sicherheitsrichtlinie ist in der OPC-UA-Spezifikation veraltet, da sie nicht mehr als sicher gilt. Wir empfehlen Ihnen, eine andere Sicherheitsrichtlinie zu wählen. Weitere Informationen finden Sie unter Basic128Rsa15.

- `BASIC256`— (Veraltet) Die `Basic256` Sicherheitsrichtlinie ist in der OPC-UA-Spezifikation veraltet, da sie nicht mehr als sicher gilt. Wir empfehlen Ihnen, eine andere Sicherheitsrichtlinie zu wählen. Weitere Informationen finden Sie unter Basic256.

> **Important**
>
> Wenn Sie eine andere Sicherheitsrichtlinie als wählen`NONE`, müssen Sie `SIGN` oder `SIGN_AND_ENCRYPT` für wählen. `messageSecurityMode` Sie müssen Ihren Quellserver auch so konfigurieren, dass er dem SiteWise Edge-Gateway vertraut. Weitere Informationen finden Sie unter Ermöglicht es Ihren OPC-UA-Quellservern, dem SiteWise Edge-Gateway zu vertrauen.

Nachricht SecurityMode

Der Nachrichtensicherheitsmodus, der zum Sichern von Verbindungen zur OPC-UA-Quelle verwendet wird. Wählen Sie eine der folgenden Optionen aus:

- `NONE`— Das SiteWise Edge-Gateway sichert keine Verbindungen zur OPC-UA-Quelle. Wir empfehlen, dass Sie einen anderen Nachrichtensicherheitsmodus wählen. Wenn Sie diese Option wählen, müssen Sie auch `NONE` für `securityPolicy` auswählen.
- `SIGN`— Daten, die zwischen dem SiteWise Edge-Gateway und der OPC-UA-Quelle übertragen werden, sind signiert, aber nicht verschlüsselt.
- `SIGN_AND_ENCRYPT`— Daten, die zwischen dem Gateway und der OPC-UA-Quelle übertragen werden, sind signiert und verschlüsselt.

> **Important**
>
> Wenn Sie einen anderen Nachrichtensicherheitsmodus als wählen`NONE`, müssen Sie einen `securityPolicy` anderen als wählen. `NONE` Sie müssen Ihren Quellserver auch so konfigurieren, dass er dem SiteWise Edge-Gateway vertraut. Weitere Informationen finden Sie unter Ermöglicht es Ihren OPC-UA-Quellservern, dem SiteWise Edge-Gateway zu vertrauen.

Identitätsanbieter

Eine Identitätsanbieterstruktur, die die folgenden Informationen enthält:

Typ

Der Typ der Authentifizierungsanmeldeinformationen, die von der Quelle erfordert werden. Wählen Sie eine der folgenden Optionen aus:

- `Anonymous`— Die Quelle benötigt keine Authentifizierung, um eine Verbindung herzustellen.
- `Username`— Die Quelle benötigt einen Benutzernamen und ein Passwort, um eine Verbindung herzustellen. Wenn Sie diese Option wählen, müssen Sie `usernameSecretArn` in `identityProvider` definieren.

Nutzername SecretArn

(Optional) Der ARN eines AWS Secrets Manager Geheimnisses. Das SiteWise Edge-Gateway verwendet die Authentifizierungsanmeldeinformationen in diesem geheimen Schlüssel, wenn es eine Verbindung zu dieser Quelle herstellt. Sie müssen Geheimnisse an den SiteWise IoT-Connector Ihres SiteWise Edge-Gateways anhängen, um sie für die Quellauthentifizierung zu verwenden. Weitere Informationen finden Sie unter Konfiguration der Datenquellenauthentifizierung.

Dieses Feld ist erforderlich, wenn Sie `Username` für `type` in `identityProvider` auswählen.

Knoten FilterRules

Eine Liste von Regelstrukturen für Knotenfilter, die die OPC-UA-Datenstream-Pfade definieren, die an die AWS Cloud gesendet werden sollen. Sie können Knotenfilter verwenden, um die Startzeit und die CPU-Auslastung Ihres SiteWise Edge-Gateways zu reduzieren, indem Sie nur Pfade zu Daten einbeziehen, die Sie modellieren. AWS IoT SiteWise Standardmäßig laden SiteWise Edge-Gateways alle OPC-UA-Pfade hoch, außer denen, die mit beginnen. `/Server/` Um OPC-UA-Knotenfilter zu definieren, können Sie Knotenpfade und die Platzhalterzeichen * und ** verwenden. Weitere Informationen finden Sie unter Verwenden von OPC-UA-Knotenfiltern.

Jede Struktur in der Liste muss folgende Informationen enthalten:

Aktion

Die Aktion für diese Knotenfilterregel. Sie können die folgenden Optionen auswählen:

- `INCLUDE`— Das SiteWise Edge-Gateway enthält nur Datenströme, die dieser Regel entsprechen.

Definition

Eine Knotenfilterregelstruktur, die die folgenden Informationen enthält:

Typ

Der Typ des Knotenfilterpfads für diese Regel. Sie können die folgenden Optionen auswählen:

- `OpcUaRootPath`— Das SiteWise Edge-Gateway bewertet diesen Knotenfilterpfad anhand des Stammverzeichnisses der OPC-UA-Pfadhierarchie.

RootPath

Der Knotenfilterpfad, der anhand des Stammes der OPC-UA-Pfadhierarchie ausgewertet werden soll. Dieser Pfad muss beginnen mit. `/`

DataStreamPräfix für die Messung

Eine Zeichenfolge, die allen Datenströmen aus der Quelle vorangestellt wird. Das SiteWise Edge-Gateway fügt dieses Präfix allen Datenströmen aus dieser Quelle hinzu. Verwenden Sie ein Datenstrom-Präfix, um zwischen Datenströmen mit demselben Namen aus verschiedenen Quellen zu unterscheiden. Jeder Datenstrom sollte einen eindeutigen Namen in Ihrem Konto haben.

Eigenschaftengruppen

(Optional) Die Liste der Eigenschaftsgruppen, die das Protokoll definieren `deadband` und vom Protokoll `scanMode` angefordert werden.

Name

Der Name der Eigenschaftsgruppe. Dies sollte ein eindeutiger Bezeichner sein.

Deadband

Die `deadband` Struktur, die die folgenden Informationen enthält:

Typ

Die unterstützten Typen von Deadband. Zulässige Werte sind `ABSOLUTE` und`PERCENT`.

Wert

Der Wert des Totbandes. Wenn `type` ja`ABSOLUTE`, ist dieser Wert ein Double ohne Einheit. Wenn `type` ja`PERCENT`, ist dieser Wert ein Doppelter zwischen `1` und`100`.

eGumin

(Optional) Die minimale technische Einheit bei Verwendung eines `PERCENT` Deadbands. Sie legen dies fest, wenn auf dem OPC-UA-Server keine technischen Einheiten konfiguriert sind.

EGUmax

(Optional) Die maximale technische Einheit bei Verwendung eines `PERCENT` Deadbands. Sie legen dies fest, wenn auf dem OPC-UA-Server keine technischen Einheiten konfiguriert sind.

Timeout (Millisekunden)

Die Dauer in Millisekunden vor dem Timeout. Das Minimum ist. `100`

Scan-Modus

Die `scanMode` Struktur, die die folgenden Informationen enthält:

Typ

Die unterstützten Typen von`scanMode`. Zulässige Werte sind `POLL` und`EXCEPTION`.

bewerten

Das Abtastintervall für den Scanmodus.

FilterRuleKnoten-Definitionen

(Optional) Eine Liste von Knotenpfaden, die in die Eigenschaftsgruppe aufgenommen werden sollen. Eigenschaftsgruppen dürfen sich nicht überschneiden. Wenn Sie keinen Wert für dieses Feld angeben, enthält die Gruppe alle Pfade unter dem Stamm, und Sie können keine zusätzlichen Eigenschaftsgruppen erstellen. Die `nodeFilterRuleDefinitions`-Struktur enthält folgende Informationen:

Typ

`OpcUaRootPath`ist der einzige unterstützte Typ. Dies gibt an, dass der Wert von `rootPath` ein Pfad relativ zum Stammverzeichnis des OPC-UA-Browsingbereichs ist.

rootPath

Eine durch Kommas getrennte Liste, die die Pfade (relativ zum Stamm) angibt, die in die Eigenschaftsgruppe aufgenommen werden sollen.

Beispiele für die Konfiguration von Funktionen

Das folgende Beispiel definiert eine OPC-UA SiteWise Edge-Gateway-Funktionskonfiguration anhand einer Payload, die in einer JSON-Datei gespeichert ist.

```
aws iotsitewise update-gateway-capability-configuration \
--capability-namespace "iotsitewise:opcuacollector:2" \
--capability-configuration file://opc-ua-configuration.json
```

Example : OPC-UA-Quellkonfiguration

Die folgende `opc-ua-configuration.json` Datei definiert eine grundlegende, unsichere OPC-UA-Quellkonfiguration.

```
{
    "sources": [
        {
            "name": "Wind Farm #1",
            "endpoint": {
                "certificateTrust": {
                    "type": "TrustAny"
                },
                "endpointUri": "opc.tcp://203.0.113.0:49320",
                "securityPolicy": "NONE",
                "messageSecurityMode": "NONE",
                "identityProvider": {
                    "type": "Anonymous"
                },
                "nodeFilterRules": []
            },
            "measurementDataStreamPrefix": ""
        }
    ]
}
```

Example : OPC-UA-Quellkonfiguration mit definierten Eigenschaftsgruppen

Die folgende `opc-ua-configuration.json` Datei definiert eine grundlegende, unsichere OPC-UA-Quellkonfiguration mit definierten Eigenschaftsgruppen.

```
{
    "sources": [
```

```
        {
            "name": "source1",
            "endpoint": {
                "certificateTrust": {
                    "type": "TrustAny"
                },
                "endpointUri": "opc.tcp://10.0.0.9:49320",
                "securityPolicy": "NONE",
                "messageSecurityMode": "NONE",
                "identityProvider": {
                    "type": "Anonymous"
                },
                "nodeFilterRules": [
                    {
                        "action": "INCLUDE",
                        "definition": {
                            "type": "OpcUaRootPath",
                            "rootPath": "/Utilities/Tank"
                        }
                    }
                ]
            },
            "measurementDataStreamPrefix": "propertyGroups",
            "propertyGroups": [
                 {
                     "name": "Deadband_Abs_5",
                     "nodeFilterRuleDefinitions": [
                         {
                             "type": "OpcUaRootPath",
                             "rootPath": "/Utilities/Tank/Temperature/TT-001"
                         },
                         {
                             "type": "OpcUaRootPath",
                             "rootPath": "/Utilities/Tank/Temperature/TT-002"
                         }
                     ],
                     "deadband": {
                         "type":"ABSOLUTE",
                         "value": 5.0,
                         "timeoutMilliseconds": 120000
                     }
                 },
                 {
                     "name": "Polling_10s",
```

```
                    "nodeFilterRuleDefinitions": [
                        {
                            "type": "OpcUaRootPath",
                            "rootPath": "/Utilities/Tank/Pressure/PT-001"
                        }
                    ],
                    "scanMode": {
                        "type": "POLL",
                        "rate": 10000
                    }
                },
                {
                    "name": "Percent_Deadband_Timeout_90s",
                    "nodeFilterRuleDefinitions": [
                        {
                            "type": "OpcUaRootPath",
                            "rootPath": "/Utilities/Tank/Flow/FT-*"
                        }
                    ],
                    "deadband": {
                        "type":"PERCENT",
                        "value": 5.0,
                        "eguMin": -100,
                        "eguMax": 100,
                        "timeoutMilliseconds": 90000
                    }
                }
            ]
        }
    ]
}
```

Example : OPC-UA-Quellkonfiguration mit Eigenschaften

Das folgende JSON-Beispiel für `opc-ua-configuration.json` definiert eine OPC-UA-Quellkonfiguration mit den folgenden Eigenschaften:

- Vertraut jedem Zertifikat.
- Verwendet die `BASIC256` Sicherheitsrichtlinie, um Nachrichten zu sichern.
- Verwendet den `SIGN_AND_ENCRYPT`-Modus zum Sichern von Verbindungen.
- Verwendet Authentifizierungsdaten, die in einem Secrets Manager Manager-Secret gespeichert sind.

- Filtert Datenströme außer denjenigen heraus, deren Pfad mit `/WindFarm/2/WindTurbine/` beginnt.
- Fügt `/Washington` am Anfang jedes Datenstrompfades hinzu, um zwischen diesem „Windpark #2" und einem „Windpark #2" in einem anderen Bereich zu unterscheiden.

```
{
    "sources": [
        {
            "name": "Wind Farm #2",
            "endpoint": {
                "certificateTrust": {
                    "type": "TrustAny"
                },
                "endpointUri": "opc.tcp://203.0.113.1:49320",
                "securityPolicy": "BASIC256",
                "messageSecurityMode": "SIGN_AND_ENCRYPT",
                "identityProvider": {
                    "type": "Username",
                    "usernameSecretArn":
 "arn:aws:secretsmanager:region:123456789012:secret:greengrass-windfarm2-auth-1ABCDE"
                },
                "nodeFilterRules": [
                  {
                      "action": "INCLUDE",
                      "definition": {
                          "type": "OpcUaRootPath",
                          "rootPath": "/WindFarm/2/WindTurbine/"
                    }
                  }
                ]
            },
            "measurementDataStreamPrefix": "/Washington"
        }
    ]
}
```

Example : OPC-UA-Quellkonfiguration mit Zertifikatsvertrauen

Das folgende JSON-Beispiel für `opc-ua-configuration.json` definiert eine OPC-UA-Quellkonfiguration mit den folgenden Eigenschaften:

- Vertraut einem bestimmten X.509-Zertifikat.
- Verwendet die BASIC256 Sicherheitsrichtlinie, um Nachrichten zu sichern.
- Verwendet den SIGN_AND_ENCRYPT-Modus zum Sichern von Verbindungen.

```
{
    "sources": [
        {
            "name": "Wind Farm #3",
            "endpoint": {
                "certificateTrust": {
                    "type": "X509",
                    "certificateBody": "-----BEGIN CERTIFICATE-----
          MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
          -----END CERTIFICATE-----",
                    "certificateChain": "-----BEGIN CERTIFICATE-----
          MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
```

```
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
          -----END CERTIFICATE-----"
               },
               "endpointUri": "opc.tcp://203.0.113.2:49320",
               "securityPolicy": "BASIC256",
               "messageSecurityMode": "SIGN_AND_ENCRYPT",
               "identityProvider": {
                   "type": "Anonymous"
               },
               "nodeFilterRules": []
             },
            "measurementDataStreamPrefix": ""

        }
    ]
}
```

Ermöglicht es Ihren OPC-UA-Quellservern, dem SiteWise Edge-Gateway zu vertrauen

Wenn Sie bei der Konfiguration Ihrer OPC-UA-Quelle eine `messageSecurityMode` andere Option als Keine wählen, müssen Sie Ihre Quellserver so einrichten, dass sie dem Edge-Gateway vertrauen. AWS IoT SiteWise Das SiteWise Edge-Gateway generiert ein Zertifikat, das Ihr Quellserver möglicherweise benötigt. Der Prozess ist je nach Ihren Quellservern unterschiedlich. Weitere Informationen finden Sie in der Dokumentation zu Ihren Servern.

Das folgende Verfahren beschreibt die grundlegenden Schritte.

Um einem OPC-UA-Server zu ermöglichen, dem Edge-Gateway zu vertrauen SiteWise

1. Öffnen Sie die Schnittstelle zur Konfiguration Ihres OPC-UA-Servers.
2. Geben Sie den Benutzernamen und das Passwort des OPC-UA-Serveradministrators ein.
3. Suchen Sie auf der Benutzeroberfläche nach Trusted Clients (Vertrauenswürdige Clients), und wählen Sie dann AWS IoT SiteWise Gateway Client aus.
4. Wählen Sie Trust (Vertrauensstellung) aus.

Exportieren des OPC-UA-Clientzertifikats

Einige OPC-UA-Server benötigen Zugriff auf die OPC-UA-Client-Zertifikatsdatei, um dem Edge-Gateway zu vertrauen. SiteWise Wenn dies auf Ihre OPC-UA-Server zutrifft, können Sie das

OPC-UA-Client-Zertifikat mit dem folgenden Verfahren vom Edge-Gateway exportieren. SiteWise Anschließend können Sie das Zertifikat auf Ihren OPC-UA-Server importieren.

So exportieren Sie die OPC-UA-Clientzertifikatdatei für eine Quelle

1. Führen Sie den folgenden Befehl aus, um in das Verzeichnis zu wechseln, das die Zertifikatdatei enthält. *Ersetzen Sie sitewise-work durch den lokalen Speicherpfad für aws.iot. SiteWiseEdgeCollectorÖffnen Sie den* Greengrass-Arbeitsordner und ersetzen Sie *source-name durch den Namen* der Datenquelle.

   Standardmäßig ist der Greengrass-Arbeitsordner /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua unter Linux und *C: /greengrass/v2/work/aws.iot. SiteWiseEdgeCollectorOpcua* unter Windows.

   ```
   cd /sitewise-work/source-name/opcua-certificate-store
   ```

2. Das OPC-UA-Client-Zertifikat des SiteWise Edge-Gateways für diese Quelle befindet sich in der Datei. `aws-iot-opcua-client.pfx`

   Führen Sie den folgenden Befehl aus, um das Zertifikat in eine `.pem`-Datei namens `aws-iot-opcua-client-certificate.pem` zu exportieren.

   ```
   keytool -exportcert -v -alias aws-iot-opcua-client -keystore aws-iot-opcua-client.pfx -storepass amazon -storetype PKCS12 -rfc > aws-iot-opcua-client-certificate.pem
   ```

3. Übertragen Sie die Zertifikatsdatei,`aws-iot-opcua-client-certificate.pem`, vom SiteWise Edge-Gateway auf den OPC-UA-Server.

   Dazu können Sie gängige Software wie das `scp` Programm verwenden, um die Datei mit dem SSH-Protokoll zu übertragen. Weitere Informationen finden Sie unter Sichere Kopie auf Wikipedia.

   > **Note**
   >
   > Wenn Ihr SiteWise Edge-Gateway auf Amazon Elastic Compute Cloud (Amazon EC2) läuft und Sie sich zum ersten Mal damit verbinden, müssen Sie die Voraussetzungen für die Verbindung konfigurieren. Weitere Informationen finden Sie unter Connect to your Linux Instance im Amazon EC2 EC2-Benutzerhandbuch.

4. Importieren Sie die Zertifikatsdatei,`aws-iot-opcua-client-certificate.pem`, auf den OPC-UA-Server, um dem Edge-Gateway zu vertrauen. SiteWise Die Schritte sind von den von Ihnen verwendeten Quellservern abhängig. Weitere Informationen finden Sie in der Dokumentation für den Server.

Filtern Sie Datenaufnahmebereiche mit OPC-UA

Sie können steuern, wie Sie Daten mit einer OPC-UA-Quelle aufnehmen, indem Sie den Scanmodus und Deadband-Bereiche verwenden. Mit diesen Funktionen können Sie steuern, welche Art von Daten aufgenommen werden sollen und wie und wann Ihr Server und das SiteWise Edge-Gateway diese Informationen austauschen.

Erfassen oder filtern Sie Daten auf der Grundlage der Qualität

Sie können Ihre Datenqualitätseinstellungen so konfigurieren, dass Sie steuern, welche Daten aus der OPC-UA-Quelle gesammelt werden. Die Datenquelle enthält die Qualitätsbewertung als Metadaten, wenn sie gesendet wird. Sie können eine oder alle der folgenden Optionen auswählen:

- `Good`
- `Bad`
- `Uncertain`

Steuern Sie die Häufigkeit der Datenerfassung im Scanmodus

Sie können Ihren OPC-UA-Scanmodus so konfigurieren, dass er steuert, wie Sie Daten aus Ihrer OPC-UA-Quelle sammeln. Sie können den Abonnement- oder Abfragemodus wählen.

- Abonnementmodus — Die OPC-UA-Quelle sammelt Daten, um sie mit der durch Ihre SiteWise Scanrate definierten Frequenz an Ihr Edge-Gateway zu senden. Der Server sendet nur Daten, wenn sich der Wert geändert hat. Dies ist also die maximale Frequenz, mit der Ihr SiteWise Edge-Gateway Daten empfängt.
- Abfragemodus — Ihr SiteWise Edge-Gateway fragt die OPC-UA-Quelle mit einer festgelegten Frequenz ab, die durch Ihre Scanrate definiert wird. Der Server sendet Daten unabhängig davon, ob sich der Wert geändert hat, sodass Ihr SiteWise Edge-Gateway immer Daten in diesem Intervall empfängt.

> **Note**
>
> Die Option für den Abfragemodus überschreibt Ihre Deadband-Einstellungen für diese Quelle.

Filtern Sie die OPC-UA-Datenaufnahme anhand von Totbandbereichen

Sie können ein Deadband auf Ihre OPC-UA-Quelleigenschaftsgruppen anwenden, um bestimmte Daten herauszufiltern und zu verwerfen, anstatt sie an die Cloud zu senden. AWS Ein Deadband gibt ein Zeitfenster an, in dem zu erwartende Schwankungen der eingehenden Datenwerte aus Ihrer OPC-UA-Quelle zu erwarten sind. Wenn die Werte in dieses Fenster fallen, sendet Ihr OPC-UA-Server sie nicht an die Cloud. AWS Sie können die Deadband-Filterung verwenden, um die Datenmenge zu reduzieren, die Sie verarbeiten und an die Cloud senden. AWS Informationen zum Einrichten von OPC-UA-Quellen für Ihr SiteWise Edge-Gateway finden Sie unter. the section called “Konfigurieren von Datenquellen”

> **Note**
>
> Ihr Server löscht alle Daten, die in das durch Ihr Deadband angegebene Fenster fallen. Sie können diese verworfenen Daten nicht wiederherstellen.

Arten von Deadbands

Sie können zwei Arten von Deadbands für Ihre OPC-UA-Servereigenschaftsgruppe angeben. Mit diesen können Sie wählen, wie viele Daten an die AWS Cloud gesendet und wie viele verworfen werden.

- Prozentsatz — Sie geben ein Zeitfenster an, in dem ein Prozentsatz der zu erwartenden Fluktuation des Messwerts verwendet wird. Der Server berechnet anhand dieses Prozentsatzes das genaue Fenster und sendet Daten an die AWS Cloud, wenn der Wert außerhalb des Fensters liegt. Wenn Sie beispielsweise einen Totbandwert von 2% für einen Sensor mit einem Bereich von -100 Grad Fahrenheit bis +100 Grad Fahrenheit angeben, wird der Server angewiesen, Daten an die AWS Cloud zu senden, wenn sich der Wert um 4 Grad Fahrenheit oder mehr ändert.

> **Note**
>
> Sie können optional einen minimalen und einen maximalen Totbandwert für dieses Fenster angeben, wenn Ihr Quellserver keine technischen Einheiten definiert. Wenn kein Bereich für technische Einheiten angegeben wird, verwendet der OPC-UA-Server standardmäßig den gesamten Bereich des Messdatentyps.

- Absolut — Sie geben ein Fenster mit exakten Einheiten an. Wenn Sie beispielsweise einen Totbandwert von 2 für einen Sensor angeben, wird der Server angewiesen, Daten an die AWS Cloud zu senden, wenn sich der Wert um mindestens 2 Einheiten ändert. Sie können absolutes Deadbanding für dynamische Umgebungen verwenden, in denen während des normalen Betriebs regelmäßig mit Schwankungen zu rechnen ist.

Deadband-Timeouts

Sie können optional eine Einstellung für das Deadband-Timeout konfigurieren. Nach diesem Timeout sendet der OPC-UA-Server den aktuellen Messwert, auch wenn dieser innerhalb der erwarteten Deadband-Fluktuation liegt. Sie können die Timeout-Einstellung verwenden, um sicherzustellen, dass jederzeit ein stetiger Datenstrom aufgenommen AWS IoT SiteWise wird, auch wenn die Werte das definierte Totzonenfenster nicht überschreiten.

Verwenden von OPC-UA-Knotenfiltern

Wenn Sie OPC-UA-Datenquellen für ein SiteWise Edge-Gateway definieren, können Sie Knotenfilter definieren. Mit Knotenfiltern können Sie einschränken, welche Datenstream-Pfade das SiteWise Edge-Gateway an die Cloud sendet. Sie können Knotenfilter verwenden, um die Startzeit und die CPU-Auslastung Ihres SiteWise Edge-Gateways zu reduzieren, indem Sie nur Pfade zu Daten einbeziehen, die Sie modellieren AWS IoT SiteWise. Standardmäßig laden SiteWise Edge-Gateways alle OPC-UA-Pfade hoch, außer denen, die mit beginnen. `/Server/` Sie können die Platzhalterzeichen * und ** in den Knotenfiltern verwenden, um mehrere Daten-Stream-Pfade mit einem Filter einzuschließen. Informationen zum Einrichten von OPC-UA-Quellen für Ihr SiteWise Edge-Gateway finden Sie unter. Konfigurieren von Datenquellen

> **Note**
>
> AWS IoT SiteWise startet Ihr SiteWise Edge-Gateway jedes Mal neu, wenn Sie eine Quelle hinzufügen oder bearbeiten. Ihr SiteWise Edge-Gateway nimmt während des Neustarts keine

Daten auf. Die Zeit für den Neustart Ihres SiteWise Edge-Gateways hängt von der Anzahl der Tags in den Quellen Ihres SiteWise Edge-Gateways ab. Die Neustartzeit kann zwischen einigen Sekunden (für ein SiteWise Edge-Gateway mit wenigen Tags) und mehreren Minuten (für ein SiteWise Edge-Gateway mit vielen Tags) liegen.

In der folgenden Tabelle sind die Platzhalter aufgeführt, mit denen Sie OPC-UA-Datenquellen filtern können.

Platzhalter für OPC-UA-Knotenfilter

Platzhalter	Beschreibung
*	Entspricht einer einzelnen Ebene in einem Daten-Stream-Pfad.
**	Entspricht mehreren Ebenen in einem Daten-Stream-Pfad.

Note

Wenn Sie eine Quelle mit einem umfassenden Filter konfigurieren und die Quelle später ändern, sodass ein restriktiverer Filter verwendet wird, AWS IoT SiteWise werden keine Daten mehr gespeichert, die nicht dem neuen Filter entsprechen.

Example Beispielszenario mit Knotenfiltern

Sehen Sie sich beispielsweise die folgenden hypothetischen Daten-Streams an:

- `/WA/Factory 1/Line 1/PLC1`
- `/WA/Factory 1/Line 1/PLC2`
- `/WA/Factory 1/Line 2/Counter1`
- `/WA/Factory 1/Line 2/PLC1`
- `/OR/Factory 1/Line 1/PLC1`
- `/OR/Factory 1/Line 2/Counter2`

Mit den vorherigen Datenströmen können Sie Knotenfilter definieren, um zu beschränken, welche Daten aus Ihrer OPC-UA-Quelle enthalten sind.

- Um in diesem Beispiel alle Knoten auszuwählen, verwenden Sie `/` oder`/**/`. Mit den Platzhalterzeichen `**` können Sie mehrere Verzeichnisse oder Ordner einschließen.
- Um alle `PLC`-Daten-Streams auszuwählen, verwenden Sie `/*/*/*/PLC*` oder `/**/PLC*`.
- Um in diesem Beispiel alle Leistungsindikatoren auszuwählen, verwenden Sie `/**/Counter*` oder`/*/*/*/Counter*`.
- Wenn Sie alle Zähler aus `Line 2` auswählen möchten, verwenden Sie `/**/Line 2/Counter*`.

Konfiguration der Datenquellenauthentifizierung

Wenn Ihr OPC-UA-Server für die Verbindung Authentifizierungsdaten benötigt, können Sie diese verwenden, AWS Secrets Manager um ein Geheimnis zu erstellen und für Ihr SiteWise Edge-Gateway bereitzustellen. AWS Secrets Manager verschlüsselt Geheimnisse auf dem Gerät, um Ihren Benutzernamen und Ihr Passwort zu schützen, bis Sie sie verwenden müssen. Weitere Informationen zur AWS IoT Greengrass Secret Manager-Komponente finden Sie unter Secret Manager im AWS IoT Greengrass Version 2 Developer Guide.

Informationen zur Verwaltung des Zugriffs auf Secrets Manager Manager-Geheimnisse finden Sie unter:

- Wer hat die Rechte an Ihren AWS Secrets Manager Geheimnissen.
- Feststellen, ob eine Anfrage innerhalb eines Kontos zugelassen oder abgelehnt wird.

Schritt 1: Geheimnisse für die Quellauthentifizierung erstellen

Sie können AWS Secrets Manager es verwenden, um ein Authentifizierungsgeheimnis für Ihre Datenquelle zu erstellen. Definieren Sie im Secret Paare **`username`** und **`password`** Schlüssel-Wert-Paare, die Authentifizierungsdetails für Ihre Datenquelle enthalten.

Ein Secret erstellen (Konsole)

1. Navigieren Sie zur AWS Secrets Manager -Konsole.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Wählen Sie unter Geheimtyp die Option Andere Art von Geheimnissen aus.
4. Gehen Sie unter Schlüssel/Wert-Paare wie folgt vor:

1. Geben Sie in das erste Eingabefeld **`username`** und im zweiten Eingabefeld den Benutzernamen ein.
2. Wählen Sie Zeile hinzufügen.
3. Geben Sie im ersten Eingabefeld das Passwort ein **`password`** und im zweiten Eingabefeld geben Sie das Passwort ein.

5. Wählen Sie als Verschlüsselungsschlüssel aws/secretsmanager und dann Weiter aus.
6. Geben Sie auf der Seite Neues Geheimnis speichern einen geheimen Namen ein.
7. (Optional) Geben Sie eine Beschreibung ein, die Ihnen bei der Identifizierung dieses Geheimnisses hilft, und wählen Sie dann Weiter aus.
8. (Optional) Aktivieren Sie auf der Seite Neues Geheimnis speichern die Option Automatische Rotation. Weitere Informationen finden Sie im AWS Secrets Manager Benutzerhandbuch unter Rotation von Geheimnissen.
9. Geben Sie einen Rotationsplan an.
10. Wählen Sie eine Lambda-Funktion aus, die dieses Geheimnis rotieren kann, und klicken Sie dann auf Weiter.
11. Überprüfen Sie Ihre geheimen Konfigurationen und wählen Sie dann Store aus.

Um Ihr SiteWise Edge-Gateway für die Interaktion zu autorisieren AWS Secrets Manager, muss die IAM-Rolle für Ihr SiteWise Edge-Gateway die `secretsmanager:GetSecretValue` Aktion zulassen. Sie können das Greengrass-Core-Gerät verwenden, um nach der IAM-Richtlinie zu suchen. Weitere Informationen zur Aktualisierung einer IAM-Richtlinie finden Sie unter Bearbeiten von IAM-Richtlinien im Benutzerhandbuch.AWS Identity and Access Management

Example policy

Ersetzen Sie *`secret-arn`* durch den Amazon-Ressourcennamen (ARN) des Secrets, das Sie im vorherigen Schritt erstellt haben. Weitere Informationen zum Abrufen des ARN eines Secrets finden Sie unter Retrieve your secret from AWS Secrets Manager im AWS Secrets Manager Benutzerhandbuch.

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

```
            "secretsmanager:GetSecretValue"
        ],
        "Effect":"Allow",
        "Resource":[
            "secret-arn"
        ]
    }
]
}
```

Schritt 2: Stellen Sie Geheimnisse auf Ihrem SiteWise Edge-Gateway-Gerät bereit

Sie können die AWS IoT SiteWise Konsole verwenden, um Geheimnisse auf Ihrem SiteWise Edge-Gateway bereitzustellen.

So stellen Sie ein Geheimnis bereit (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Gateways aus.
3. Wählen Sie aus der Gateways-Liste das SiteWise Edge-Ziel-Gateway aus.
4. Wählen Sie im Abschnitt Gateway-Konfiguration den Link Greengrass Core-Gerät aus, um den mit dem SiteWise Edge-Gateway verknüpften AWS IoT Greengrass Core zu öffnen.
5. Wählen Sie im Navigationsbereich Deployments aus.
6. Wählen Sie die Zielbereitstellung und dann Revise aus.
7. Wählen Sie auf der Seite „Ziel angeben“ die Option Weiter aus.
8. Deaktivieren Sie auf der Seite Komponenten auswählen im Abschnitt Öffentliche Komponenten die Option Nur ausgewählte Komponenten anzeigen.
9. Suchen Sie nach aws.greengrass und wählen Sie es aus. SecretManagerKomponente und wählen Sie dann Weiter.
10. Wählen Sie aus der Liste Ausgewählte Komponenten die Datei aws.greengrass aus. SecretManagerKomponente und wählen Sie dann Komponente konfigurieren aus.
11. Fügen Sie im Feld Konfiguration zum Zusammenführen das folgende JSON-Objekt hinzu.

> **Note**
>
> Ersetzen Sie *secret-arn* durch den ARN des Secrets, das Sie im vorherigen Schritt erstellt haben. Weitere Informationen zum Abrufen des ARN eines Secrets finden Sie

unter Retrieve your secret from AWS Secrets Manager im AWS Secrets Manager Benutzerhandbuch.

```
{
"cloudSecrets":[
  {
     "arn":"secret-arn"
  }
]
}
```

12. Wählen Sie Bestätigen aus.
13. Wählen Sie Weiter aus.
14. Wählen Sie auf der Seite Erweiterte Einstellungen konfigurieren die Option Weiter aus.
15. Überprüfen Sie Ihre Bereitstellungskonfigurationen und wählen Sie dann Deploy aus.

Schritt 3: Fügen Sie Authentifizierungskonfigurationen hinzu

Sie können die AWS IoT SiteWise Konsole verwenden, um Ihrem SiteWise Edge-Gateway Authentifizierungskonfigurationen hinzuzufügen.

Um Authentifizierungskonfigurationen hinzuzufügen (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie aus der Gateways-Liste das SiteWise Edge-Ziel-Gateway aus.
3. Wählen Sie aus der Liste Datenquellen die Zieldatenquelle aus, und klicken Sie dann auf Bearbeiten.
4. Wählen Sie auf der Seite Datenquelle hinzufügen die Option Erweiterte Konfiguration aus.
5. Wählen Sie für die Authentifizierungskonfiguration den geheimen Schlüssel aus, den Sie im vorherigen Schritt bereitgestellt haben.
6. Klicken Sie auf Speichern.

Wählen Sie ein Ziel für Ihre Quellserverdaten

Daten werden mit Amazon S3 vom Edge AWS IoT SiteWise in Echtzeit oder in Batches exportiert. Sie können den Stream auch mithilfe eines AWS IoT Greengrass Streams an eine andere Komponente senden.

- AWS IoT SiteWise Echtzeit — Wählen Sie diese Option, um Daten direkt an den AWS IoT SiteWise Speicher zu senden. Erfassen und überwachen Sie Daten in Echtzeit und verarbeiten Sie Daten am Netzwerkrand.
- AWS IoT SiteWise Mit Amazon S3 gepuffert — Daten im Parquet-Format an Amazon S3 senden und dann in den AWS IoT SiteWise Speicher importieren. Wählen Sie diese Option, um Daten stapelweise aufzunehmen und historische Daten kostengünstig zu speichern. Sie können Ihren bevorzugten Amazon S3-Bucket-Standort und die Häufigkeit, mit der Daten auf Amazon S3 hochgeladen werden sollen, konfigurieren. Sie können auch wählen, was mit den Daten nach der Aufnahme geschehen soll. AWS IoT SiteWise Sie können wählen, ob die Daten SiteWise sowohl in Amazon S3 als auch in Amazon S3 verfügbar sein sollen, oder Sie können wählen, ob sie automatisch aus Amazon S3 gelöscht werden sollen.
  - Der Amazon S3 S3-Bucket ist ein Staging- und Puffermechanismus und unterstützt Dateien im Parquet-Format.
  - Wenn Sie das Kontrollkästchen Daten in AWS IoT SiteWise Speicher importieren aktivieren, werden Daten zuerst in Amazon S3 und dann in den AWS IoT SiteWise Speicher hochgeladen.
    - Wenn Sie das Kontrollkästchen Daten aus Amazon S3 löschen aktivieren, werden Daten aus Amazon S3 gelöscht, nachdem sie in den SiteWise Speicher importiert wurden.
    - Wenn Sie das Kontrollkästchen Daten aus Amazon S3 löschen deaktivieren, werden Daten sowohl in Amazon S3 als auch im SiteWise Speicher gespeichert.
  - Wenn Sie das Kontrollkästchen Daten in AWS IoT SiteWise Speicher importieren deaktivieren, werden Daten nur in Amazon S3 gespeichert. Sie werden nicht in den SiteWise Speicher importiert.

  Einzelheiten Verwaltung des Datenspeichers zu den verschiedenen Speicheroptionen finden Sie AWS IoT SiteWise unter. Weitere Informationen zu den Preisoptionen finden Sie unter AWS IoT SiteWise Preise.
- AWS IoT Greengrass Stream-Manager — Verwenden Sie den AWS IoT Greengrass Stream-Manager, um Daten an die folgenden AWS Cloud Ziele zu senden: Kanäle in AWS IoT Analytics, Streams in Amazon Kinesis Data Streams, Asset-Eigenschaften in AWS IoT SiteWise oder Objekte in Amazon Simple Storage Service (Amazon S3). Weitere Informationen finden Sie im AWS IoT

Greengrass Version 2 Entwicklerhandbuch unter Datenstreams auf dem AWS IoT Greengrass Core verwalten.

Das folgende Beispiel zeigt die erforderliche Nachrichtenstruktur des Datenstroms. Alle Felder sind erforderlich.

```
{
    "assetId": "string",
    "propertyAlias": "string",
    "propertyId": "string",
    "propertyValues": [
      {
         "quality": "string",
         "timestamp": {
            "offsetInNanos": number,
            "timeInSeconds": number
         },
         "value": {
            "booleanValue": boolean,
            "doubleValue": number,
            "integerValue": number,
            "stringValue": "string"
         }
      }
    ]
}
```

> **Note**
>
> Die Datenstromnachricht muss `propertyAlias` in ihrer Struktur entweder (`assetId`und`propertyId`) oder enthalten.

`assetId`

(Optional) Die ID des zu aktualisierenden Assets.

`propertyAlias`

(Optional) Der Alias, der die Eigenschaft identifiziert, z. B. ein OPC-UA-Serverdatenstream-Pfad. Beispielsweise:

```
/company/windfarm/3/turbine/7/temperature
```

Weitere Informationen finden Sie im AWS IoT SiteWise Benutzerhandbuch unter Zuordnung von industriellen Datenströmen zu Anlageneigenschaften.

`propertyId`

(Optional) Die ID der Anlageneigenschaft für diesen Eintrag.

`propertyValues`

(Erforderlich) Die Liste der hochzuladenden Eigenschaftswerte. Sie können bis zu 10 `propertyValues` Array-Elemente angeben.

`quality`

(Optional) Die Qualität des Immobilienwerts.

`timestamp`

(Erforderlich) Der Zeitstempel des Immobilienwerts.

`offsetInNanos`

(Optional) Der Nanosekunden-Offset von. `timeInSeconds`

`timeInSeconds`

(Erforderlich) Das Zeitstempeldatum in Sekunden im Unix-Epochenformat. Daten in Bruchteilen von Nanosekunden werden bereitgestellt von. `offsetInNanos`

`value`

(Erforderlich) Der Wert der Vermögenseigenschaft.

> **Note**
>
> In dem `value` Feld kann nur einer der folgenden Werte vorhanden sein.

`booleanValue`

(Optional) Objekteigenschaftsdaten vom Typ Boolean (`true`oder`false`).

`doubleValue`

(Optional) Anlageneigenschaftsdaten vom Typ Double (Fließkommazahl).

`integerValue`

(Optional) Daten zu Vermögenswerten vom Typ Ganzzahl (ganze Zahl).

`stringValue`

(Optional) Daten zu Vermögenswerten vom Typ Zeichenfolge (Zeichenfolge).

Hinzufügen von Partnerdatenquellen zu SiteWise Edge-Gateways

Wenn Sie ein AWS IoT SiteWise Edge-Gateway verwenden, können Sie eine Partnerdatenquelle mit Ihrem SiteWise Edge-Gateway verbinden und Daten vom Partner in Ihrem SiteWise Edge-Gateway und der AWS Cloud empfangen. Diese Partnerdatenquellen sind AWS IoT Greengrass Komponenten, die in Zusammenarbeit zwischen AWS und dem Partner entwickelt wurden. Wenn Sie eine Partnerdatenquelle hinzufügen, AWS IoT SiteWise erstellt diese Komponente und stellt sie auf Ihrem SiteWise Edge-Gateway bereit.

Gehen Sie wie folgt vor, um eine Partnerdatenquelle hinzuzufügen:

- Hinzufügen einer Partnerdatenquelle
- Gehen Sie zum Webportal des Partners und konfigurieren Sie die Partnerdatenquelle so, dass sie eine Verbindung zum SiteWise Edge-Gateway herstellt.

Themen

Sicherheit

Im Rahmen des -Modells der geteilten Verantwortung zwischen AWS, unseren Kunden und unseren Partnern wird im Folgenden beschrieben, wer für die verschiedenen Aspekte der Sicherheit verantwortlich ist:

Verantwortung des Kunden

- Überprüfung des Partners.

- Konfigurieren des Netzwerkzugriffs, der dem Partner gewährt wird.

AWS Verantwortung

- Isolierung des Partners von den Kunden-AWSCloud-Ressourcen, außer denen, die der Partner benötigt. In diesem Fall AWS IoT SiteWise Aufnahme.
- Beschränkung der Partnerlösung auf eine angemessene Nutzung der SiteWise Edge-Gateway-Computerressourcen (CPU, Arbeitsspeicher, Dateisystem).

Verantwortung des Partners

- Verwenden sicherer Standardwerte.
- Die Lösung im Laufe der Zeit durch Patches und andere geeignete Updates schützen.
- Vertraulichkeit von Kundendaten.

Hinzufügen einer Partnerdatenquelle

Um eine Partnerdatenquelle mit Ihrem SiteWise Edge-Gateway zu verbinden, fügen Sie sie als Datenquelle hinzu. Wenn Sie sie als Datenquelle hinzufügen, AWS IoT SiteWise stellt eine private AWS IoT Greengrass Komponente in Ihrem SiteWise Edge-Gateway bereit.

Voraussetzungen

Gehen Sie wie folgt vor, um eine Partnerdatenquelle hinzuzufügen:

- Erstellen Sie ein -Konto beim Partner.
- Binden Sie die Konten.

So erstellen Sie ein SiteWise Edge-Gateway mit einer Partnerdatenquelle

Wenn Sie ein neues SiteWise Edge-Gateway erstellen möchten, führen Sie die Schritte unter ausEin SiteWise Edge-Gateway erstellen. Nachdem Sie das SiteWise Edge-Gateway erstellt haben, führen Sie die Schritte unter ausSo fügen Sie eine Partnerdatenquelle zu einem vorhandenen SiteWise Edge-Gateway hinzu, um eine Partnerdatenquelle hinzuzufügen.

So fügen Sie eine Partnerdatenquelle zu einem vorhandenen SiteWise Edge-Gateway hinzu

1. Navigieren Sie zur AWS IoT SiteWise-Konsole.

2. Wählen Sie im Navigationsbereich Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, mit dem Sie die Partnerdatenquelle verbinden möchten.
4. Wählen Sie unter Datenquellen die Option Datenquelle hinzufügen aus.
5. Wählen Sie für Quelltyp den Partner aus, mit dem Sie Ihr SiteWise Edge-Gateway verbinden möchten.

   > **Note**
   >
   > Derzeit EasyEdge ist die einzige verfügbare Partnerdatenquelle. Wenn Sie zum ersten Mal eine EasyEdge Datenquelle hinzufügen, müssen Sie ein EasyEdge Konto erstellen.

6. Geben Sie einen Namen für die Quelle ein.
7. Um dem Partner Zugriff auf die Datenquelle zu gewähren, wählen Sie Autorisieren aus.
8. Um Ihre AWS IoT SiteWiseHerausgeberkomponente AWS IoT SiteWise aktualisieren zu lassen und, wenn das Datenverarbeitungspaket aktiviert ist, die AWS IoT SiteWise Prozessorkomponente zu aktualisieren, wählen Sie Komponenten aktualisieren aus.
9. Wählen Sie Speichern.

Einrichten von Docker auf Ihrem SiteWise Edge-Gateway

Um eine Partnerdatenquelle hinzuzufügen, muss Docker Engine 1.9.1 oder höher auf Ihrem lokalen Gerät installiert sein.

> **Note**
>
> Version 20.10 ist die neueste Version, für die verifiziert wurde, dass sie mit der SiteWise Edge-Gateway-Software funktioniert.

So überprüfen Sie, ob Docker installiert ist

Um zu überprüfen, ob Docker installiert ist, führen Sie den folgenden Befehl von einem Terminal aus, das mit Ihrem SiteWise Edge-Gateway verbunden ist:

```
docker info
```

Wenn der Befehl ein `docker is not recognized` Ergebnis zurückgibt oder eine ältere Version von Docker installiert ist, installieren Sie die Docker-Engine, bevor Sie fortfahren.

So richten Sie Docker ein

Der Systembenutzer, der eine Docker-Containerkomponente ausführt, muss über Root- oder Administratorberechtigungen verfügen, oder Sie müssen Docker so konfigurieren, dass es als Nicht-Root- oder Nicht-Administratorbenutzer ausgeführt wird.

Auf Linux-Geräten müssen Sie der `docker` Gruppe einen `ggc_user` Benutzer hinzufügen, um Docker-Befehle ohne aufzurufen`sudo`.

Um oder den Nicht-Root-Benutzer`ggc_user`, den Sie zum Ausführen von Docker-Containerkomponenten verwenden, zur `docker` Gruppe hinzuzufügen, führen Sie den folgenden Befehl aus:

```
sudo usermod -aG docker ggc_user
```

Weitere Informationen finden Sie unter Schritte nach der Linux-Installation für Docker Engine .

SiteWise Datenquellen von Edge-Gateway-Partnern

Verwenden Sie die folgenden Informationen, um eine Partnerdatenquelle zu konfigurieren.

EasyEdge

Portal:

https://studio.easyedge.io/

EasyEdge Dokumentation:

EasyEdge für AWS

EasyEdge Anforderungen — Informationen zu den EasyEdge Anforderungen, einschließlich der Endpunkte und Ports, die für die Konfiguration der Firewall erforderlich sind. Hinweis: Sie benötigen ein EasyEdge Konto, um auf diese Dokumentation zugreifen zu können.

Verwenden von Paketen

AWS IoT SiteWise Edge-Gateways verwenden unterschiedliche Pakete, um zu bestimmen, wie Ihre Daten erfasst und verarbeitet werden sollen.

Derzeit sind die folgenden Pakete verfügbar:

- Datenerfassungspaket — Verwenden Sie dieses Paket, um Ihre Industriedaten zu sammeln und an AWS Cloud-Ziele weiterzuleiten. Standardmäßig ist dieses Paket automatisch für Ihr SiteWise Edge-Gateway aktiviert.
- Datenverarbeitungspaket — Verwenden Sie dieses Paket, um die SiteWise Edge-Gateway-Kommunikation mit Edge-konfigurierten Anlagenmodellen und Anlagen zu aktivieren. Mithilfe der Edge-Konfiguration können Sie steuern, welche Anlagendaten vor Ort berechnet und verarbeitet werden sollen. Anschließend können Sie Ihre Daten an AWS IoT SiteWise oder andere AWS Dienste senden. Weitere Hinweise zum Datenverarbeitungspaket finden Sie unterthe section called “Aktivierung der Edge-Datenverarbeitung”.

Pakete aktualisieren

> **Important**
>
> Ein Upgrade von Data Processing Pack-Versionen von Versionen vor (und einschließlich) 2.0.x auf Version 2.1.x führt zum Datenverlust lokal gespeicherter Messungen.

SiteWise Edge-Gateways verwenden unterschiedliche Pakete, um zu bestimmen, wie Ihre Daten erfasst und verarbeitet werden sollen. Sie können die AWS IoT SiteWise Konsole verwenden, um Pakete zu aktualisieren.

Um Pakete zu aktualisieren (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Gateways aus.
3. Wählen Sie in der Gateways-Liste das SiteWise Edge-Gateway mit den Paketen aus, die Sie aktualisieren möchten.
4. Wählen Sie im Abschnitt Gateway-Konfiguration die Option Verfügbare Softwareupdates aus.

5. Gehen Sie auf der Seite Softwareversionen bearbeiten im Abschnitt Gateway-Komponentenupdates wie folgt vor:
   - Um den OPC-UA Collector zu aktualisieren, wählen Sie eine Version und dann Deploy.
   - Um den Publisher zu aktualisieren, wählen Sie eine Version und dann Deploy.
   - Um das Data Processing Pack zu aktualisieren, wählen Sie eine Version und dann Bereitstellen aus.
6. Wenn Sie mit der Bereitstellung neuer Versionen fertig sind, wählen Sie Fertig.

Falls Sie Probleme beim Upgrade der Packs haben, finden Sie weitere Informationen unterPakete können nicht für SiteWise Edge-Gateways bereitgestellt werden.

Verwalten von SiteWise Edge-Gateways

Sie können die AWS IoT SiteWise Konsole und API-Operationen verwenden, um AWS IoT SiteWise Edge-Gateways zu verwalten. Sie können auch die Anwendung AWS OpsHub für AWS IoT SiteWise for Windows verwenden, um einige Aspekte Ihres SiteWise Edge-Gateways von Ihrem lokalen Gerät aus zu verwalten.

Wir empfehlen dringend, dass Sie die AWS OpsHub für die AWS IoT SiteWise Anwendung verwenden, um die Festplattennutzung auf Ihrem lokalen Gerät zu überwachen. Sie können auch die `Gateway.UsedPercentageDiskSpace` Amazon- CloudWatch Metriken `Gateway.AvailableDiskSpace` und überwachen und Alarme erstellen, um benachrichtigt zu werden, wenn der Speicherplatz knapp wird. Weitere Informationen zu Amazon- CloudWatch Alarmen finden Sie unter Erstellen eines CloudWatch Alarms basierend auf einem statischen Schwellenwert.

Stellen Sie sicher, dass Ihr Gerät über genügend Speicherplatz für bevorstehende Daten verfügt. Wenn Ihnen der Speicherplatz auf Ihrem lokalen Gerät ausgeht, löscht der Service automatisch eine kleine Datenmenge mit den ältesten Zeitstempeln, um Platz für bevorstehende Daten zu schaffen.

Gehen Sie wie folgt vor, um zu überprüfen, ob der Service Ihre Daten gelöscht hat:

1. Melden Sie sich bei der AWS OpsHub für die AWS IoT SiteWise Anwendung an.
2. Wählen Sie Settings (Einstellungen) aus.
3. Geben Sie für Protokolle einen Zeitraum an und wählen Sie dann Herunterladen aus.

4. Entpacken Sie die Protokolldatei.
5. Wenn die Protokolldatei die folgende Meldung enthält, hat der Service Ihre Daten gelöscht: *Anzahl* der Bytes an Daten wurden gelöscht, um zu verhindern, dass der SiteWise Edge-Gateway-Speicher nicht über genügend Speicherplatz verfügt.

Verwalten Ihres SiteWise Edge-Gateways mit der AWS IoT SiteWise Konsole

Sie können die AWS IoT SiteWise Konsole verwenden, um alle SiteWise Edge-Gateways in Ihrem AWS Konto zu konfigurieren, zu aktualisieren und zu überwachen.

Sie können Ihre SiteWise Edge-Gateways anzeigen, indem Sie zur Seite Edge Gateways in der AWS IoT SiteWise Konsole navigieren. Um auf die Detailseite des Edge-Gateways für ein bestimmtes Gateway zuzugreifen, wählen Sie den Namen eines Edge-Gateways aus.

Auf der Registerkarte Übersicht der Seite mit den Edge-Gateway-Details können Sie Folgendes tun:

- Aktualisieren Sie im Abschnitt Datenquellen die Konfiguration der Datenquelle und konfigurieren Sie zusätzliche Datenquellen
- Wählen Sie CloudWatch Metriken öffnen, um die Anzahl der pro Datenquelle erfassten Datenpunkte in der CloudWatch Metrikkonsole anzuzeigen
- Fügen Sie Ihrem SiteWise Edge-Gateway im Abschnitt Edge-Funktionen Datenpakete hinzu, indem Sie auf Bearbeiten klicken
- Zeigen Sie im Abschnitt Gateway-Konfiguration den Verbindungsstatus Ihrer SiteWise Edge-Gateways an
- Zeigen Sie im Abschnitt Publisher-Konfiguration den Status der SiteWise Edge-Gateway-Synchronisierung und die Konfiguration der AWS IoT SiteWise Publisher-Komponente an

Auf der Registerkarte Updates der Detailseite des Edge-Gateways können Sie die aktuellen Komponenten- und Paketversionen sehen, die auf dem Edge-Gateway bereitgestellt werden. Hier stellen Sie auch neue Versionen bereit, wenn sie verfügbar sind.

Verwalten von SiteWise Edge-Gateways mit AWS OpsHub für AWS IoT SiteWise

Sie verwenden die AWS OpsHub für die AWS IoT SiteWise Anwendung, um Ihre SiteWise Edge-Gateways zu verwalten und zu überwachen. Diese Anwendung bietet die folgenden Überwachungs- und Verwaltungsoptionen:

- Unter Übersicht können Sie Folgendes tun:
  - Zeigen Sie SiteWise Edge-Gateway-Details an, mit denen Sie Einblicke in Ihre SiteWise Edge-Gateway-Gerätedaten erhalten, Probleme identifizieren und die Leistung des SiteWise Edge-Gateways verbessern können.
  - Zeigen Sie SiteWise Monitor-Portale an, die die Daten von lokalen Servern und Geräten am Edge überwachen. Weitere Informationen finden Sie unter Was ist AWS IoT SiteWise Monitor im AWS IoT SiteWise Monitor -Anwendungshandbuch.
- Unter Zustand gibt es ein Dashboard, das Daten aus Ihrem SiteWise Edge-Gateway anzeigt. Domainexperten wie Prozessingenieure können das Dashboard verwenden, um einen Überblick über das Verhalten des SiteWise Edge-Gateways zu erhalten.
- Zeigen Sie unter Assets die auf dem lokalen Gerät bereitgestellten Assets und den letzten für Asset-Eigenschaften erfassten oder berechneten Wert an.
- Unter Einstellungen können Sie Folgendes tun:
  - Wenn das Data Processing Pack installiert ist, zeigen Sie die Konfigurationsinformationen des SiteWise Edge-Gateways an und synchronisieren Sie Ressourcen mit der AWS Cloud.
  - Laden Sie die Authentifizierungsdateien herunter, mit denen Sie mithilfe anderer Tools auf das SiteWise Edge-Gateway zugreifen können.
  - Laden Sie Protokolle herunter, mit denen Sie Probleme mit dem SiteWise Edge-Gateway beheben können.
  - Zeigen Sie die AWS IoT SiteWise Komponenten an, die auf dem SiteWise Edge-Gateway bereitgestellt werden.

Important

Folgendes ist erforderlich, um AWS OpsHub für zu verwenden AWS IoT SiteWise:

- Ihr lokales Gerät und die AWS OpsHub für die AWS IoT SiteWise Anwendung müssen mit demselben Netzwerk verbunden sein.

- Das Datenverarbeitungspaket muss aktiviert sein.

So verwalten Sie SiteWise Edge-Gateways mit AWS OpsHub

1. Laden Sie die Anwendung AWS OpsHub für AWS IoT SiteWise for Windows herunter und installieren Sie sie.
2. Öffnen Sie die Anwendung .
3. Wenn Sie keine lokalen Anmeldeinformationen für Ihr Gateway eingerichtet haben, führen Sie die Schritte unter aus, Zugreifen auf Ihr SiteWise Edge-Gateway mit Anmeldeinformationen des lokalen Betriebssystems um sie einzurichten.
4. Sie können sich mit Ihren Linux- oder Lightweight Directory Access Protocol (LDAP)-Anmeldeinformationen bei Ihrem SiteWise Edge-Gateway anmelden. Führen Sie einen der folgenden Schritte aus, um sich bei Ihrem SiteWise Edge-Gateway anzumelden:

   Linux

   1. Geben Sie für Hostname oder IP-Adresse den Hostnamen oder die IP-Adresse Ihres lokalen Geräts ein.
   2. Wählen Sie für Authentifizierung Linux aus.
   3. Geben Sie unter Benutzername den Benutzernamen Ihres Linux-Betriebssystems ein.
   4. Geben Sie für Passwort das Passwort Ihres Linux-Betriebssystems ein.
   5. Klicken Sie auf Sign in.

   LDAP

   1. Geben Sie für Hostname oder IP-Adresse den Hostnamen oder die IP-Adresse Ihres lokalen Geräts ein.
   2. Wählen Sie für Authentifizierung die Option LDAP aus.
   3. Geben Sie für Benutzername den Benutzernamen Ihres LDAP ein.
   4. Geben Sie für Passwort das Passwort Ihres LDAP ein.
   5. Klicken Sie auf Sign in.

Zugreifen auf Ihr SiteWise Edge-Gateway mit Anmeldeinformationen des lokalen Betriebssystems

Neben dem Lightweight Directory Access Protocol (LDAP) können Sie die Linux- oder Windows-Anmeldeinformationen für den Zugriff auf Ihr SiteWise Edge-Gateway verwenden.

> **Important**
>
> Um mit Linux-Anmeldeinformationen auf Ihr SiteWise Edge-Gateway zuzugreifen, müssen Sie das Datenverarbeitungspaket für Ihr SiteWise Edge-Gateway aktivieren.

Zugreifen auf Ihr SiteWise Edge-Gateway mit Linux-Betriebssystemanmeldeinformationen

Bei den folgenden Schritten wird davon ausgegangen, dass Sie ein Gerät mit Ubuntu verwenden. Wenn Sie eine andere Linux-Distribution verwenden, lesen Sie die entsprechende Dokumentation für Ihr Gerät.

So erstellen Sie einen Linux-Benutzerpool

1. Führen Sie den folgenden Befehl aus, um eine Admin-Gruppe zu erstellen.

   ```
   sudo groupadd --system SWE_ADMIN_GROUP
   ```

   Benutzer in der `SWE_ADMIN_GROUP` Gruppe können Administratorzugriff für das SiteWise Edge-Gateway gewähren.
2. Führen Sie den folgenden Befehl aus, um eine Benutzergruppe zu erstellen.

   ```
   sudo groupadd --system SWE_USER_GROUP
   ```

   Benutzer in der `SWE_USER_GROUP` Gruppe können schreibgeschützten Zugriff für das SiteWise Edge-Gateway zulassen.
3. Führen Sie den folgenden Befehl aus, um der Administratorgruppe einen Benutzer hinzuzufügen. Ersetzen Sie *`user-name`* und *`password`* durch den Benutzernamen und das Passwort, die Sie hinzufügen möchten.

   ```
   sudo useradd -p $(openssl passwd -1 password) user-name
   ```

4. Um einen Benutzer entweder zu SWE_ADMIN_GROUP oder hinzuzufügenSWE_USER_GROUP, ersetzen Sie *user-name* durch den Benutzernamen, den Sie im vorherigen Schritt hinzugefügt haben.

   ```
   sudo usermod -a -G SWE_ADMIN_GROUP user-name
   ```

Sie können jetzt den Benutzernamen und das Passwort verwenden, um sich beim SiteWise Edge-Gateway auf der AWS OpsHub für die AWS IoT SiteWise Anwendung anzumelden.

Zugreifen auf Ihr SiteWise Edge-Gateway mit Windows-Anmeldeinformationen

Bei den folgenden Schritten wird davon ausgegangen, dass Sie ein Gerät mit Windows verwenden.

> **Important**
>
> Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Erstellen Sie eine starke Passwortrichtlinie mit mindestens 12 Zeichen und einer Kombination aus Groß-, Klein-, Zahlen und Symbolen. Legen Sie außerdem die Windows-Firewall-Regeln fest, um eingehenden Datenverkehr auf Port 443 zuzulassen und eingehenden Datenverkehr auf allen anderen Ports zu blockieren.

So erstellen Sie einen Windows Server-Benutzerpool

1. Führen Sie PowerShell als Administrator aus.

   a. Melden Sie sich auf dem Windows-Server, auf dem Sie SiteWise Edge Gateway installieren möchten, als Administrator an.

   b. Geben Sie PowerShell in die Windows-Suchleiste ein.

   c. Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf die Windows PowerShell-App. Wählen Sie Als Administrator ausführen aus.

2. Führen Sie den folgenden Befehl aus, um eine Admin-Gruppe zu erstellen.

   ```
   net localgroup SWE_ADMIN_GROUP /add
   ```

   Sie müssen ein Benutzer in der SWE_ADMIN_GROUP Gruppe sein, um Administratorzugriff für das SiteWise Edge-Gateway zu gewähren.

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

```
net localgroup SWE_USER_GROUP /add
```

   Sie müssen ein Benutzer in der -SWE_USER_GROUPGruppe sein, um den reinen Zugriff für das SiteWise Edge-Gateway zu erlauben.

4. Führen Sie den folgenden Befehl aus, um einen Benutzer hinzuzufügen. Ersetzen Sie *user-name* und *password* durch den Benutzernamen und das Passwort, das Sie erstellen möchten.

```
net user user-name password /add
```

5. Führen Sie den folgenden Befehl aus, um der Administratorgruppe einen Benutzer hinzuzufügen. Ersetzen Sie *user-name* durch den Benutzernamen, den Sie hinzufügen möchten.

```
net localgroup SWE_ADMIN_GROUP user-name /add
```

Sie können jetzt den Benutzernamen und das Passwort verwenden, um sich beim SiteWise Edge-Gateway auf der AWS OpsHub für die AWS IoT SiteWise Anwendung anzumelden.

Verwalten des SiteWise Edge-Gateway-Zertifikats

Sie können SiteWise Monitor und Drittanbieteranwendungen wie Grafana auf Ihren SiteWise Edge-Gateway-Geräten verwenden. Diese Anwendungen erfordern eine TLS-Verbindung zum -Service. SiteWise Edge-Gateways verwenden derzeit ein selbstsigniertes Zertifikat. Wenn Sie einen Browser verwenden, um die Anwendungen zu öffnen, z. B. ein SiteWise Monitor-Portal, erhalten Sie möglicherweise eine Warnung für nicht vertrauenswürdige Zertifikate.

Im Folgenden wird gezeigt, wie Sie das vertrauenswürdige Zertifikat von der AWS OpsHub für die AWS IoT SiteWise Anwendung herunterladen.

1. Melden Sie sich bei der Anwendung an.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie für Authentifizierung die Option Zertifikat herunterladen aus.

Im Folgenden wird davon ausgegangen, dass Sie Google Chrome oder verwenden FireFox. Wenn Sie einen anderen Browser verwenden, lesen Sie die entsprechende Dokumentation für Ihren

Browser. Führen Sie einen der folgenden Schritte aus, um das Zertifikat, das Sie im vorherigen Schritt heruntergeladen haben, zu einem Browser hinzuzufügen:

- Wenn Sie Google Chrome verwenden, folgen Sie den Anweisungen in der Dokumentation zur Google Chrome Enterprise Help.
- Wenn Sie Firefox verwenden, folgen Sie der Anleitung So laden Sie das Zertifikat in den Mozilla- oder Firefox-Browser in der Oracle-Dokumentation .

Ändern der Version von SiteWise Edge-Gateway-Komponentenpaketen

Sie können die AWS IoT SiteWise Konsole verwenden, um die Version von Komponentenpaketen auf Ihren SiteWise Edge-Gateways zu ändern.

So ändern Sie die Version eines SiteWise Edge-Gateway-Komponentenpakets

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, für das Sie die Paketversionen ändern möchten.
4. Wählen Sie unter Gateway-Konfiguration die Option Softwareversionen anzeigen aus.
5. Wählen Sie auf der Seite Softwareversionen bearbeiten für das Paket, von dem Sie die Version aktualisieren möchten, die Version aus, die Sie bereitstellen möchten, und wählen Sie Bereitstellen aus.
6. Wählen Sie Erledigt aus.

Ausführen von SiteWise Edge auf Industrie Edge

Sie können Daten von Ihrem Industrial Edge-Gerät in Ihr aufnehmen, AWS-Konto indem Sie ein SiteWise Edge-Gateway auf dem Gerät ausführen. Dazu erstellen Sie eine SiteWise Edge-Gateway-Ressource mit dem Bereitstellungsziel Industrial Edge-Gerät – neu, laden die Konfigurationsdatei herunter und laden sie über das IEM-Portal (Industrial Edge Management) in Ihre Bol-App hoch. Weitere Informationen zur Ausführung von AWS IoT SiteWise Edge auf Industrial Edge, einschließlich der Einrichtung der erforderlichen Ressourcen, finden Sie unter Was ist Industrial Edge? in der Bol-Dokumentation.

> **Note**
>
> Bol ist kein Anbieter oder Anbieter für AWS IoT SiteWise Edge. Der Industrial Edge Marketplace ist ein unabhängiger Marketplace.

Themen

Voraussetzungen

Zum Ausführen von AWS IoT SiteWise Edge auf Industrie Edge benötigen Sie Folgendes:

- Ein Konto für die Bol Digital Exchange Platform
- A Industrial Edge Hub (iehub)-Konto
- Eine Industrial Edge Management (IEM)-Instance
- Entweder ein Bol Industrial Edge Device (IED) oder ein Virtual Edge Device (IEvD)
- Zugriff auf das Bereitstellungsziel für Industrial Edge-Geräte. Um Zugriff zu erhalten, rufen Sie die -AWS IoT SiteWise Konsole auf und wählen Sie Zugriff anfordern aus.

Sicherheit

Im Rahmen des -Modells der geteilten Verantwortung zwischen AWS, unseren Kunden und unseren Partnern wird im Folgenden beschrieben, wer für die verschiedenen Aspekte der Sicherheit verantwortlich ist:

Verantwortung des Kunden

- Überprüfung des Partners.
- Konfigurieren des Netzwerkzugriffs, der dem Partner gewährt wird.

- Physische Sicherung des Geräts, auf dem AWS IoT SiteWise Edge ausgeführt wird.

AWS Verantwortung

- Isolierung des Partners von den Kunden- AWS Cloud-Ressourcen.

Verantwortung des Partners

- Verwenden sicherer Standardwerte.
- Die Lösung im Laufe der Zeit durch Patches und andere geeignete Updates schützen.
- Vertraulichkeit von Kundendaten.
- Überprüfung anderer Anwendungen, die auf dem Partner-Marketplace verfügbar sind.

Während der Vorschauphase dieses Features sind Kundendaten, die auf dem Partnergerät AWS IoT SiteWise zwischengespeichert werden, für den Partner und andere Anwendungen zugänglich, die über den Partner-Marketplace installiert werden.

Erstellen der Konfigurationsdatei

Sobald Sie über die richtigen Bol-Konten und IEM-Instances verfügen, können Sie ein SiteWise Edge-Gateway vom Bereitstellungstyp Industrial Edge-Gerät erstellen.

So erstellen Sie die Konfigurationsdatei

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Edge-Gateways aus.
3. Wählen Sie Create gateway (Gateway erstellen).
4. Wählen Sie für Bereitstellungstyp die Option Industrie Edge-Gerät – neu aus.
5. Geben Sie einen Namen für Ihr SiteWise Edge-Gateway ein oder verwenden Sie den von generierten Namen AWS IoT SiteWise.
6. (Optional) Gehen Sie unter Erweiterte Konfiguration wie folgt vor:
   - Geben Sie einen Namen für Ihr AWS IoT Core Objekt ein oder verwenden Sie den von generierten Namen AWS IoT SiteWise.
7. Wählen Sie Create gateway (Gateway erstellen).
8. Wählen Sie im Dialogfeld SiteWise Edge-Gateway-Konfigurationsdatei generieren die Option Generieren und herunterladen aus. generiert AWS IoT SiteWise automatisch eine Konfigurationsdatei, mit der Sie die AWS IoT SiteWise Edge-Anwendung konfigurieren.

> **Important**
>
> Stellen Sie sicher, dass Sie die Konfigurationsdatei an einem sicheren Ort speichern. Sie werden die Datei später verwenden.

Nachdem Sie das SiteWise Edge-Gateway erstellt haben, führen Sie die folgenden Schritte aus, um die Einrichtung Ihres SiteWise Edge-Gateways abzuschließen:

1. Hinzufügen von Datenquellen
2. Konfigurieren der Herausgeberkomponente

Sobald Sie die Konfigurationsdatei haben und das SiteWise Edge-Gateway konfiguriert ist, laden Sie die AWS IoT SiteWise Edge-Anwendung aus dem Industrial Edge Marketplace herunter und installieren Sie sie mithilfe des Bol Industrial Edge Management (IEM)-Portals. Greifen Sie dann über das Bol Industrial Edge Management (IEM)-Portal auf Ihr Industry Edge-Gerät zu und laden Sie die Konfigurationsdatei auf das Gerät hoch, auf dem Sie das SiteWise Edge-Gateway installieren möchten.

Fehlerbehebung

Um Probleme mit dem SiteWise Edge-Gateway auf Ihrem Industrial Edge-Gerät zu beheben, können Sie über die IEM-Portale (Industrial Edge Management) oder IED (Industrial Edge Device) auf die Protokolle für die Anwendung zugreifen. Weitere Informationen finden Sie unter Herunterladen von Protokollen in der Bol-Dokumentation.

Ich sehe 'SESSION_TAKEN_OVER' oder 'com.aws.greengrass.mqttclient.MqttClient: Die Nachricht konnte nicht über Spooler veröffentlicht werden und wird es erneut versuchen.' in den Protokollen

Wenn Sie eine Warnung mit `SESSION_TAKEN_OVER` oder einen Fehler sehen, der `com.aws.greengrass.mqttclient.MqttClient: Failed to publish the message via Spooler and will retry.` in Ihren Protokollen unter enthalten ist`/greengrass/v2/logs/greengrass.log`, versuchen Sie möglicherweise, dieselbe Konfigurationsdatei für mehrere SiteWise Edge-Gateways auf mehreren Geräten zu verwenden. Jedes SiteWise Edge-Gateway benötigt eine eindeutige Konfigurationsdatei, um eine Verbindung zu Ihrem herzustellen AWS-Konto.

Ich sehe 'com.aws.greengrass.deployment.IotJobsHelper: Kein Bereitstellungsauftrag gefunden.' oder „Bereitstellungsergebnis wurde bereits gemeldet“. in den Protokollen

Wenn Sie `com.aws.greengrass.deployment.IotJobsHelper: No deployment job found.` oder `Deployment result already reported.` in Ihren Protokollen unter sehen`/greengrass/v2/logs/greengrass.log`, versuchen Sie möglicherweise, dieselbe Konfigurationsdatei wiederzuverwenden.

Es gibt mehrere Lösungen:

- Wenn Sie die Konfigurationsdatei wiederverwenden möchten, gehen Sie wie folgt vor:
  1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
  2. Wählen Sie im Navigationsbereich Gateways aus.
  3. Wählen Sie das SiteWise Edge-Gateway aus, das Sie wiederverwenden möchten.
  4. Wählen Sie die Registerkarte Updates aus.
  5. Wählen Sie eine andere Herausgeberversion und dann Bereitstellen aus.
- Führen Sie die Schritte unter ausErstellen der Konfigurationsdatei, um eine neue Konfigurationsdatei zu erstellen.

Ich sehe in den Protokollen „Konfigurationsdatei fehlt AWS_REGION“.

Wenn Sie `Config file missing AWS_REGION` in den Bol-Protokollen sehen, wurde das JSON der Konfigurationsdatei beschädigt. Sie müssen eine neue Konfigurationsdatei erstellen. Führen Sie die Schritte unter ausErstellen der Konfigurationsdatei, um eine neue Konfigurationsdatei zu erstellen.

Kontakt

- Wenn Sie Zugriff auf die Anwendung anfordern möchten, rufen Sie die -AWS IoT SiteWise Konsole auf und wählen Sie Zugriff anfordern aus.
- Wenn Sie Hilfe bei der Fehlerbehebung der Anwendung benötigen, rufen Sie die AWS IoT SiteWise Konsole auf, navigieren Sie zur Detailseite des SiteWise Edge-Gateways und wählen Sie Support erhalten aus.

Filtern von Assets auf einem SiteWise Edge-Gateway

Sie können die Edge-Filterung verwenden, um Ihre Ressourcen effizienter zu verwalten, indem Sie nur eine Teilmenge der Ressourcen zur Datenverarbeitung an ein bestimmtes SiteWise Edge-Gateway senden. Wenn Ihre Ressourcen in einer Baumstruktur oder einer übergeordneten und untergeordneten Struktur angeordnet sind, können Sie eine IAM-Richtlinie einrichten, die an die IAM-Rolle eines SiteWise Edge-Gateways angehängt ist, sodass nur der Stamm des Baums oder das übergeordnete Element und seine untergeordneten Elemente an ein bestimmtes Edge-Gateway gesendet werden können. SiteWise

> **Note**
>
> Wenn Sie vorhandene Elemente in einer Baumstruktur anordnen, gehen Sie nach dem Erstellen der Struktur zu jedem vorhandenen Asset, das Sie der Struktur hinzugefügt haben, und wählen Sie Bearbeiten und dann Speichern, um sicherzustellen, dass die neue Struktur AWS IoT SiteWise erkannt wird.

Kantenfilterung einrichten

Richten Sie die Edge-Filterung auf Ihrem SiteWise Edge-Gateway ein, indem Sie der IAM-Rolle des SiteWise Edge-Gateways die folgende IAM-Richtlinie hinzufügen und *< root-asset-id >* durch die ID des Root-Assets ersetzen, das Sie an das SiteWise Edge-Gateway senden möchten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssociatedAssets"
            ],
            "Resource": "arn:aws:iotsitewise:*:*:asset/*",
            "Condition": {
                "StringNotLike": {
                    "iotsitewise:assetHierarchyPath": "/<root-asset-id>*"
                }
            }
        }
```

```
    ]
}
```

Wenn sich auf Ihrem SiteWise Edge-Gateway derzeit Assets befinden, die Sie entfernen möchten, melden Sie sich bei Ihrem SiteWise Edge-Gateway an und führen Sie den folgenden Befehl aus, um die Synchronisierung des SiteWise Edge-Gateways zu erzwingen, AWS IoT SiteWise indem Sie den Cache löschen.

```
sudo rm /greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/sync-app/
sync_resource_bundles/edge.json
```

Verwenden von AWS IoT SiteWise APIs am Edge

Sie können eine Teilmenge der verfügbaren AWS IoT SiteWise APIs zusammen mit Edge-spezifischen APIs verwenden, um mit Komponentenmodellen und ihren Komponenten am Edge zu interagieren. Die Komponentenmodelle müssen so konfiguriert sein, dass sie am Edge ausgeführt werden. Weitere Informationen finden Sie unter Verarbeiten von Daten am Edge.

Verwenden Sie diese APIs, um Daten über Ihre Komponentenmodelle und Komponenten zu sammeln, Ihre bereitgestellten Portale und Dashboard-Metriken zu überwachen und Komponentendaten am Edge zu erhalten. Dies bietet einen zentralen Host in Ihrem Netzwerk für Interaktionen mit , AWS IoT SiteWise ohne dass ein Web-API-Aufruf erforderlich ist.

Topics

- Alle verfügbaren APIs zur Verwendung mit AWS IoT SiteWise Edge-Geräten
- Nur-Edge-APIs zur Verwendung mit AWS IoT SiteWise Edge-Geräten
- Tutorial: Abrufen einer Liste von Komponentenmodellen auf einem SiteWise Edge-Gateway

Alle verfügbaren APIs zur Verwendung mit AWS IoT SiteWise Edge-Geräten

Wenn Sie mit Geräten am Edge arbeiten, können Sie eine Vielzahl von APIs verwenden, um mit dem Gerät zu interagieren AWS IoT SiteWise und Aufgaben lokal auf dem Gerät abzuschließen.

Verfügbare AWS IoT SiteWise APIs

Die folgenden AWS IoT SiteWise APIs sind auf Edge-Geräten verfügbar:

- ListAssetModels
- DescribeAssetModel
- ListAssets
- DescribeAsset
- DescribeAssetProperty
- ListAssociatedAssets
- GetAssetPropertyAggregates
- GetAssetPropertyValue
- GetAssetPropertyValueHistory
- ListDashboards
- ListPortals
- ListProjectAssets
- ListProjects
- DescribeDashboard
- DescribePortal
- DescribeProject

Verfügbare reine Edge-APIs

Die folgenden APIs werden lokal auf Geräten am Edge verwendet:

- Authentifizieren – Verwenden Sie diese API, um die temporären SigV4-Anmeldeinformationen abzurufen, die Sie für API-Aufrufe verwenden.

Nur-Edge-APIs zur Verwendung mit AWS IoT SiteWise Edge-Geräten

Zusätzlich zu den AWS IoT SiteWise APIs, die auf dem Edge verfügbar sind, gibt es auch Edge-spezifische APIs. Diese Edge-spezifischen APIs werden unten beschrieben.

Authentifizieren

Ruft die Anmeldeinformationen vom SiteWise Edge-Gateway ab. Sie müssen lokale Benutzer hinzufügen oder über LDAP oder einen Linux-Benutzerpool eine Verbindung zu Ihrem System

herstellen. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter LDAP -oder Linux-Benutzerpool.

Erforderliche Syntax

```
POST /authenticate HTTP/1.1
Content-type: application/json
{
  "username": "string",
  "password": "string",
  "authMechanism": "string"
}
```

URI-Anforderungsparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

username

Der Benutzername, der zur Validierung des Anforderungsaufrufs verwendet wird.

Typ: Zeichenfolge

Erforderlich: Ja

password

Das Passwort des Benutzers, der Anmeldeinformationen anfordert.

Typ: Zeichenfolge

Erforderlich: Ja

authMechanism

Die Authentifizierungsmethode zur Validierung dieses Benutzers im Host.

Typ: Zeichenfolge

Zulässige Werte: `ldap`, `linux`, `winnt`

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json
{
  "accessKeyId": "string",
  "secretAccessKey": "string",
  "sessionToken": "string",
  "region": "edge"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden im JSON-Format zurückgegeben.

accessKeyId

Die Zugriffsschlüssel-ID, die die temporären Sicherheitsanmeldeinformationen identifiziert.

Längenbeschränkungen: Mindestlänge von 16. Maximale Länge beträgt 128 Zeichen.

Pattern: `[\w]*`

secretAccessKey

Der geheime Zugriffsschlüssel, der zum Signieren von Anforderungen verwendet werden kann.

Typ: Zeichenfolge

sessionToken

Das Token, das Benutzer an die Service-API übergeben müssen, um die temporären Anmeldeinformationen zu verwenden.

Typ: Zeichenfolge

Region

Die Region, die Sie für API-Aufrufe verwenden möchten.

Typ: CONSTANT – `edge`

Fehler

IllegalArgumentException

Die Anforderung wurde abgelehnt, da das bereitgestellte Textdokument falsch formatiert war. Die Fehlermeldung beschreibt den spezifischen Fehler.

HTTP Status Code: 400

AccessDeniedException

Der Benutzer verfügt nicht über gültige Anmeldeinformationen, die auf dem aktuellen Identitätsanbieter basieren. Die Fehlermeldung beschreibt den Authentifizierungsmechanismus.

HTTP Status Code: 403

TooManyRequestsException

Die Anforderung hat ihr Limit an Authentifizierungsversuchen erreicht. Die Fehlermeldung enthält die Wartezeit, bis neue Authentifizierungsversuche durchgeführt werden.

HTTP-Statuscode: 429

Tutorial: Abrufen einer Liste von Komponentenmodellen auf einem SiteWise Edge-Gateway

Sie können eine Teilmenge der verfügbaren AWS IoT SiteWise APIs zusammen mit Edge-spezifischen APIs verwenden, um mit Komponentenmodellen und ihren Komponenten am Edge zu interagieren. Dieses Tutorial führt Sie durch das Abrufen temporärer Anmeldeinformationen für ein AWS IoT SiteWise Edge-Gateway und das Abrufen einer Liste der Komponentenmodelle auf dem SiteWise Edge-Gateway.

Voraussetzungen

In den Schritten dieses Tutorials können Sie eine Vielzahl von Tools verwenden. Um diese Tools zu verwenden, stellen Sie sicher, dass Sie die entsprechenden Voraussetzungen installiert haben.

Zum Durcharbeiten dieses Tutorials ist Folgendes erforderlich:

- Ein bereitgestelltes und ausgeführtes SiteWise Anforderungen an das Edge-Gateway
- Zugriff auf Ihr SiteWise Edge-Gateway im selben Netzwerk über Port 443.

- OpenSSL installiert
- (AWS OpsHub für AWS IoT SiteWise) Die AWS OpsHub für die AWS IoT SiteWise Anwendung
- (curl) curl installiert
- (Python) urllib3 installiert
- (Python) Python3 installiert
- (Python) Boto3 installiert
- (Python) BotoCore installiert

Schritt 1: Abrufen eines vom SiteWise Edge-Gateway-Service signierten Zertifikats

Um eine TLS-Verbindung zu den im SiteWise Edge-Gateway verfügbaren APIs herzustellen, benötigen Sie ein vertrauenswürdiges Zertifikat. Sie können dieses Zertifikat mit einer OpenSSL oder AWS OpsHub für generierenAWS IoT SiteWise.

OpenSSL

> **Note**
>
> Sie müssen OpenSSL installiert haben, um diesen Befehl auszuführen.

Öffnen Sie ein Terminal und führen Sie den folgenden Befehl aus, um ein signiertes Zertifikat vom SiteWise Edge-Gateway abzurufen. Ersetzen Sie durch `<sitewise_gateway_ip>` die IP des SiteWise Edge-Gateways.

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | openssl
 x509 -outform PEM > GatewayCert.pem
```

AWS OpsHub for AWS IoT SiteWise

Sie können AWS OpsHub für verwendenAWS IoT SiteWise. Weitere Informationen finden Sie unter Verwalten von SiteWise Edge-Gateways.

Der absolute Pfad zum heruntergeladenen SiteWise Edge-Gateway-Zertifikat wird in diesem Tutorial verwendet. Führen Sie den folgenden Befehl aus, um den vollständigen Pfad Ihres Zertifikats zu exportieren und durch `<absolute_path_to_certificate>` den Pfad zum Zertifikat zu ersetzen:

```
export PATH_TO_CERTIFICATE='<absolute_path_to_certificate>'
```

Schritt 2: Abrufen Ihres SiteWise Edge-Gateway-Hostnamens

> **Note**
>
> Sie müssen OpenSSL installiert haben, um diesen Befehl auszuführen.

Um das Tutorial abzuschließen, benötigen Sie den Hostnamen Ihres SiteWise Edge-Gateways. Um den Hostnamen Ihres SiteWise Edge-Gateways abzurufen, führen Sie Folgendes aus und ersetzen Sie durch `<sitewise_gateway_ip>` die IP des SiteWise Edge-Gateways:

```
openssl s_client -connect <sitewise_gateway_ip>:443 </dev/null 2>/dev/null | grep -Po
 'CN = \K.*'| head -1
```

Führen Sie den folgenden Befehl aus, um den Hostnamen zur späteren Verwendung zu exportieren. Ersetzen Sie dabei durch `<your_edge_gateway_hostname>` den Hostnamen Ihres SiteWise Edge-Gateways:

```
export GATEWAY_HOSTNAME='<your_edge_gateway_hostname>'
```

Schritt 3: Abrufen temporärer Anmeldeinformationen für Ihr SiteWise Edge-Gateway

Nachdem Sie nun das signierte Zertifikat und den Hostnamen Ihres SiteWise Edge-Gateways haben, müssen Sie temporäre Anmeldeinformationen abrufen, damit Sie APIs auf dem Gateway ausführen können. Sie können diese Anmeldeinformationen über AWS OpsHub für AWS IoT SiteWise oder direkt über das SiteWise Edge-Gateway mithilfe von APIs abrufen.

> **Important**
>
> Anmeldeinformationen laufen alle 4 Stunden ab. Daher sollten Sie die Anmeldeinformationen kurz vor der Verwendung der APIs auf Ihrem SiteWise Edge-Gateway abrufen. Zwischenspeichern Sie Anmeldeinformationen nicht länger als 4 Stunden.

Abrufen temporärer Anmeldeinformationen mit AWS OpsHub für AWS IoT SiteWise

> **Note**
>
> Sie müssen die AWS OpsHub für die AWS IoT SiteWise Anwendung installiert haben.

Gehen Sie wie folgt vor, um AWS OpsHub für die AWS IoT SiteWise Anwendung zum Abrufen Ihrer temporären Anmeldeinformationen zu verwenden:

1. Melden Sie sich bei der Anwendung an.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie für Authentifizierung die Option Anmeldeinformationen kopieren aus.
4. Erweitern Sie die Option, die zu Ihrer Umgebung passt, und wählen Sie Kopieren aus.
5. Speichern Sie die Anmeldeinformationen zur späteren Verwendung.

Abrufen temporärer Anmeldeinformationen mithilfe der SiteWise Edge-Gateway-API

Um die temporären Anmeldeinformationen mit der SiteWise Edge-Gateway-API abzurufen, können Sie ein Python-Skript oder curl verwenden. Zuerst benötigen Sie einen Benutzernamen und ein Passwort für Ihr SiteWise Edge-Gateway. Die SiteWise Edge-Gateways verwenden SigV4-Authentifizierung und -Autorisierung. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter LDAP -oder Linux-Benutzerpool. Diese Anmeldeinformationen werden in den folgenden Schritten verwendet, um die lokalen Anmeldeinformationen auf Ihrem SiteWise Edge-Gateway abzurufen, die für die Verwendung der AWS IoT SiteWise APIs benötigt werden.

Python

> **Note**
>
> Sie müssen urllib3 und Python3 installiert haben.

So rufen Sie die Anmeldeinformationen mit Python ab

1. Erstellen Sie eine Datei namens get_credentials.py und kopieren Sie den folgenden Code in diese Datei.

```
'''
The following demonstrates how to get the credentials from the SiteWise Edge
 gateway. You will need to add local users or connect your system to LDAP/AD
https://docs.aws.amazon.com/iot-sitewise/latest/userguide/manage-gateways-
ggv2.html#create-user-pool

Example usage:
    python3 get_credentials.py -e https://<gateway_hostname> -c
 <path_to_certificate> -u '<gateway_username>' -p '<gateway_password>' -m
 '<method>'
'''
import urllib3
import json
import urllib.parse
import sys
import os
import getopt

"""
This function retrieves the AWS IoT SiteWise Edge gateway credentials.
"""
def get_credentials(endpoint,certificatePath, user, password, method):
    http = urllib3.PoolManager(cert_reqs='CERT_REQUIRED', ca_certs=
 certificatePath)
    encoded_body = json.dumps({
        "username": user,
        "password": password,
        "authMechanism": method,
    })

    url =  urllib.parse.urljoin(endpoint, "/authenticate")

    response = http.request('POST', url,
        headers={'Content-Type': 'application/json'},
        body=encoded_body)

    if response.status != 200:
        raise Exception(f'Failed to authenticate! Response status
 {response.status}')

    auth_data = json.loads(response.data.decode('utf-8'))

    accessKeyId = auth_data["accessKeyId"]
```

```
    secretAccessKey = auth_data["secretAccessKey"]
    sessionToken = auth_data["sessionToken"]
    region = "edge"

    return accessKeyId, secretAccessKey, sessionToken, region

def print_help():
    print('Usage:')
    print(f'{os.path.basename(__file__)} -e <endpoint> -c <path/to/certificate>
 -u <user> -p <password> -m <method> -a <alias>')
    print('')
    print('-e, --endpoint   edge gateway endpoint. Usually the Edge gateway
 hostname.')
    print('-c, --cert_path path to downloaded gateway certificate')
    print('-u, --user       Edge user')
    print('-p, --password   Edge password')
    print('-m, --method     (Optional) Authentication method (linux, winnt,
 ldap), default is linux')
    sys.exit()


def parse_args(argv):
    endpoint = ""
    certificatePath = None
    user = None
    password = None
    method = "linux"

    try:
        opts, args = getopt.getopt(argv, "he:c:u:p:m:",
 ["endpoint=","cert_path=", "user=", "password=", "method="])
    except getopt.GetoptError:
        print_help()

    for opt, arg in opts:
        if opt == '-h':
            print_help()
        elif opt in ("-e", "--endpoint"):
            endpoint = arg
        elif opt in ("-u", "--user"):
            user = arg
        elif opt in ("-p", "--password"):
            password = arg
        elif opt in ("-m", "--method"):
```

```
            method = arg.lower()
        elif opt in ("-c", "--cert_path"):
            certificatePath = arg

    if method not in ['ldap', 'linux', 'winnt']:
        print("not valid method parameter, required are ldap, linux, winnt")
        print_help()

    if (user == None or password == None):
        print("To authenticate against edge user, password have to be passed
 together, and the region has to be set to 'edge'")
        print_help()

    if(endpoint == ""):
        print("You must provide a valid and reachable gateway hostname")
        print_help()

    return endpoint,certificatePath, user, password, method


def main(argv):
    # get the command line args
    endpoint, certificatePath, user, password, method = parse_args(argv)

    accessKeyId, secretAccessKey, sessionToken, region=get_credentials(endpoint,
 certificatePath, user, password, method)

    print("Copy and paste the following credentials into the shell, they are
 valid for 4 hours:")
    print(f"export AWS_ACCESS_KEY_ID={accessKeyId}")
    print(f"export AWS_SECRET_ACCESS_KEY={secretAccessKey}")
    print(f"export AWS_SESSION_TOKEN={sessionToken}")
    print(f"export AWS_REGION={region}")
    print()




if __name__ == "__main__":
   main(sys.argv[1:])
```

2. Führen Sie get_credentials.py vom Terminal aus, indem Sie <gateway_username> und <gateway_password> durch die von Ihnen erstellten Anmeldeinformationen ersetzen.

```
python3 get_credentials.py -e https://$GATEWAY_HOSTNAME -c $PATH_TO_CERTIFICATE
 -u '<gateway_username>' -p '<gateway_password>' -m 'linux'
```

curl

> **Note**
>
> Sie müssen curl installiert haben.

So rufen Sie die Anmeldeinformationen mit curl ab

1. Führen Sie den folgenden Befehl vom Terminal aus aus, indem Sie <gateway_username> und <gateway_password> durch die von Ihnen erstellten Anmeldeinformationen ersetzen.

   ```
   curl --cacert $PATH_TO_CERTIFICATE --location \
   -X POST https://$GATEWAY_HOSTNAME:443/authenticate \
   --header 'Content-Type: application/json' \
   --data-raw '{
       "username": "<gateway_username>",
       "password": "<gateway_password>",
       "authMechanism": "linux"
   }'
   ```

   Die Antwort sollte wie folgt aussehen:

   ```
   {
       "username": "sweuser",
       "accessKeyId": "<accessKeyId>",
       "secretAccessKey": "<secretAccessKey>",
       "sessionToken": "<sessionToken>",
       "sessionExpiryTime": "2022-11-17T04:51:40.927095Z",
       "authMechanism": "linux",
       "role": "edge-user"
   }
   ```

2. Führen Sie im Terminal den folgenden Befehl aus:

   ```
   export AWS_ACCESS_KEY_ID=<accessKeyId>
   ```

```
export AWS_SECRET_ACCESS_KEY=<secretAccessKey>
export AWS_SESSION_TOKEN=<sessionToken>
export AWS_REGION=edge
```

Schritt 4: Abrufen einer Liste der Komponentenmodelle auf dem SiteWise Edge-Gateway

Nachdem Sie nun über ein signiertes Zertifikat, Ihren SiteWise Edge-Gateway-Hostnamen und temporäre Anmeldeinformationen für Ihr SiteWise Edge-Gateway verfügen, können Sie die `ListAssetModels`-API verwenden, um eine Liste der Komponentenmodelle auf Ihrem SiteWise Edge-Gateway abzurufen.

Python

> **Note**
>
> Python3, Boto3 und müssen BotoCore installiert sein.

So rufen Sie die Liste der Komponentenmodelle mit Python ab

1. Erstellen Sie eine Datei namens list_asset_model.py und kopieren Sie den folgenden Code in diese Datei.

```
import json
import boto3
import botocore
import os

# create the client using the credentials
client = boto3.client("iotsitewise",
    endpoint_url= "https://"+ os.getenv("GATEWAY_HOSTNAME"),
    region_name=os.getenv("AWS_REGION"),
    aws_access_key_id=os.getenv("AWS_ACCESS_KEY_ID"),
    aws_secret_access_key=os.getenv("AWS_SECRET_ACCESS_KEY"),
    aws_session_token=os.getenv("AWS_SESSION_TOKEN"),
    verify=os.getenv("PATH_TO_CERTIFICATE"),
    config=botocore.config.Config(inject_host_prefix=False))

# call the api using local credentials
```

```
response = client.list_asset_models()
print(response)
```

2. Führen Sie list_asset_model.py vom Terminal aus.

```
python3 list_asset_model.py
```

curl

> **Note**
>
> Sie müssen curl installiert haben.

So rufen Sie die Liste der Komponentenmodelle mit curl ab

Führen Sie den folgenden Befehl vom Terminal aus.

```
curl \
  --request GET https://$GATEWAY_HOSTNAME:443/asset-models \
  --cacert $PATH_TO_CERTIFICATE \
  --aws-sigv4 "aws:amz:edge:iotsitewise" \
  --user "$AWS_ACCESS_KEY_ID:$AWS_SECRET_ACCESS_KEY" \
  -H "x-amz-security-token:$AWS_SESSION_TOKEN"
```

Die Antwort sollte wie folgt aussehen:

```
{
    "assetModelSummaries": [
        {
            "arn": "arn:aws:iotsitewise:{region}:{account-id}:asset-model/{asset-
model-id}",
            "creationDate": 1.669245291E9,
            "description": "This is a small example asset model",
            "id": "{asset-model-id}",
            "lastUpdateDate": 1.669249038E9,
            "name": "Some Metrics Model",
            "status": {
                "error": null,
                "state": "ACTIVE"
```

```
            }
        },
        .
        .
        .
    ],
    "nextToken": null
}
```

SiteWise Edge-Gateways Backup und wiederherstellen

In diesem Thema wird beschrieben, wie Sie SiteWise Edge-Gateways wiederherstellen und Ihre Metrikdaten sichern. Wenn Sie Probleme mit einem defekten SiteWise Edge-Gateway auf demselben Computer haben und das Problem beheben müssen, lesen Sie bitte die AWS IoT SiteWise Dokumentation Fehlerbehebung bei SiteWise Edge-Gateway-Problemen.

> **Note**
>
> Die in diesem Thema behandelten Anleitungen gelten für SiteWise Edge-Gateways, die auf AWS IoT Greengrass V2 Version 2.1.0 oder höher installiert sind.

Tägliche Backups von metrischen Daten

Das Erstellen eines Backups ist wichtig, wenn Sie die Daten auf einen neuen Computer übertragen oder wiederherstellen möchten. Durch die Sicherung Ihrer Daten wird das Risiko eines Verlusts von Betriebsdaten während eines Übertragungs- oder Wiederherstellungsvorgangs erheblich reduziert.

Der Influxdb-Ordnerpfad lautet wie folgt:

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeProcessor/influxdb
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeProcessor\influxdb
```

Wir empfehlen, dass Sie den gesamten Ordner mit allem, was sich darunter befindet, sichern.

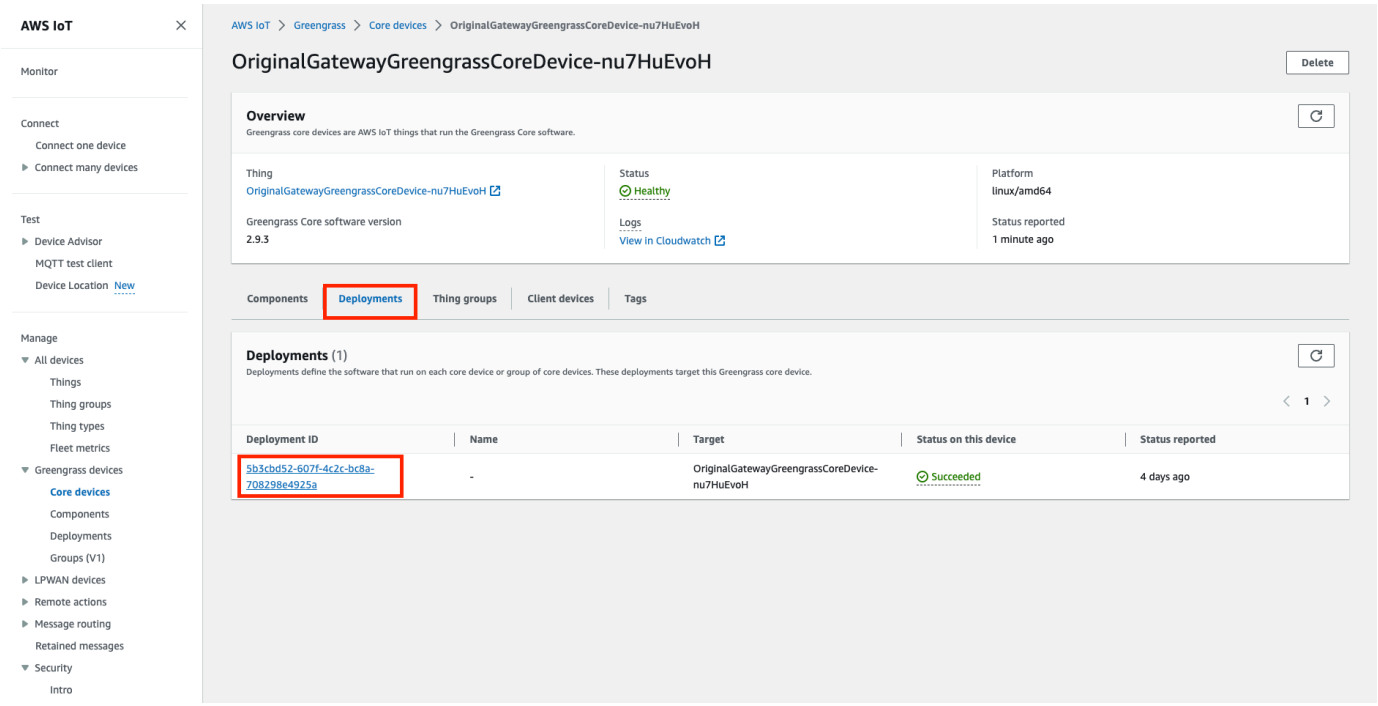
Wir empfehlen Ihnen, Ihre Messdaten regelmäßig vom 1.0 SiteWise Edge entweder auf einer externen Festplatte oder in der AWS Cloud zu sichern.

Stellen Sie ein SiteWise Edge-Gateway wieder her

Gehen Sie wie folgt vor, um ein SiteWise Edge-Gateway wiederherzustellen:

1. Verwenden Sie das Installationsskript, das beim Erstellen des SiteWise Edge-Gateways heruntergeladen wurde, um das SiteWise Edge-Gateway auf der neuen Maschine wiederherzustellen. Lesen Sie das Verfahren zur Installation der SiteWise Edge-Gateway-Software auf Ihrem lokalen Gerät, um das SiteWise Edge-Gateway einzurichten.

   Wenn Sie das Installationsskript verlieren oder nicht finden können, wenden Sie sich bitte an den AWS Kundensupport.
2. Melden Sie sich nach der Installation des SiteWise Edge-Gateways an der AWS IoT Greengrass Konsole an.
3. Um die Komponenten erneut bereitzustellen, navigieren Sie zu Verwalten und wählen Sie dann unter AWS IoT Greengrass Geräte die Option Core-Geräte aus.
4. Wählen Sie in der Tabelle mit den AWS IoT Greengrass Kerngeräten das Kerngerät aus, das Ihrem SiteWise Edge-Gateway entspricht.
5. Öffnen Sie auf der Geräteseite die Registerkarte Bereitstellungen und wählen Sie Ihre Bereitstellungs-ID aus. Dadurch wird die Seite Bereitstellungen mit Ihrer ausgewählten ID geöffnet.



6. Sobald Sie sich auf der Seite Bereitstellungen befinden, klicken Sie oben rechts auf die Schaltfläche Aktionen und wählen Sie die Option Überarbeiten aus, um eine neue Bereitstellung zu starten. Konfigurieren Sie die Bereitstellung. Wenn Sie die Bereitstellung unverändert lassen möchten, fahren Sie mit Überprüfen und Bereitstellen fort.
7. Warten Sie, bis der Bereitstellungsstatus lautet`Completed`.

> **Note**
>
> Außerdem dauert es einige Minuten, bis alle Komponenten auf dem SiteWise Edge vollständig eingerichtet und ausgeführt sind.

AWS IoT SiteWise Daten wiederherstellen

Gehen Sie wie folgt vor, um Daten auf einem neuen Computer wiederherzustellen.

1. Kopieren Sie den `influxdb` Ordner auf das neue Gerät.
2. Stoppen Sie die SiteWise EdgeProcessor Komponente, indem Sie den folgenden Befehl in Ihrem Terminal ausführen:

Linux

```
sudo /greengrass/v2/bin/greengrass-cli component stop -n
aws.iot.SiteWiseEdgeProcessor
```

Windows

```
C:\greengrass\v2\bin\greengrass-cli component stop -n
aws.iot.SiteWiseEdgeProcesso
```

3. Suchen Sie den Pfad, in dem Sie Ihre Daten gesichert haben, und führen Sie den folgenden Befehl aus:

   Linux

   ```
   sudo yes | sudo cp -rf <influxdb_backup_path> /greengrass/v2/work/
   aws.iot.SiteWiseEdgeProcessor/influxdb
   ```

   PowerShell

   ```
   Copy-Item -Recurse -Force <influxdb_backup_path>\* C:\greengrass
   \v2\work\aws.iot.SiteWiseEdgeProcessor\
   ```

   Windows

   ```
   robocopy <influxdb_backup_path> C:\greengrass\v2\work
   \aws.iot.SiteWiseEdgeProcessor\ /E
   ```

4. Starten Sie die SiteWiseEdgeProcessor Komponente neu:

   Linux

   ```
   sudo /greengrass/v2/bin/greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

   Windows

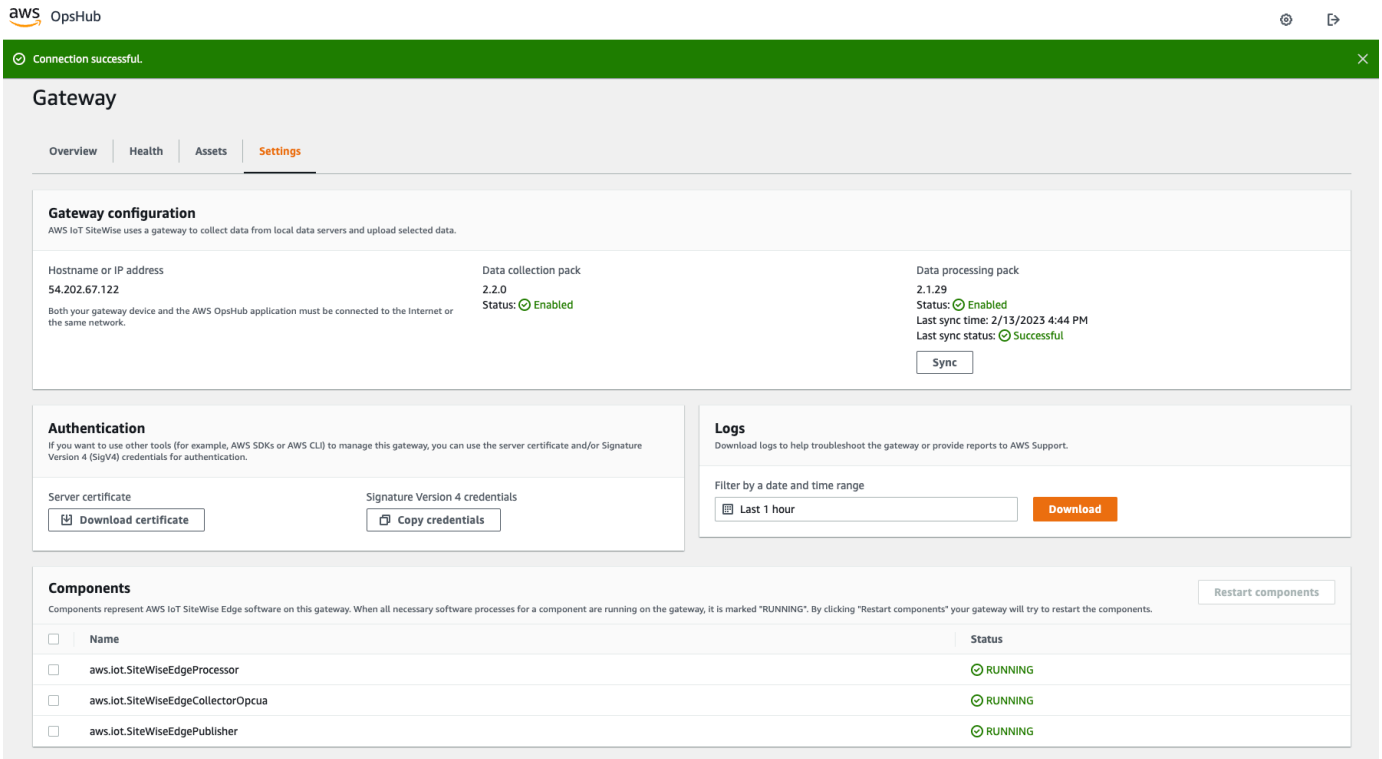
   ```
   C:\greengrass\v2\bin\greengrass-cli component restart -n
   aws.iot.SiteWiseEdgeProcessor
   ```

Bestätigen Sie erfolgreiche Backups und Wiederherstellungen

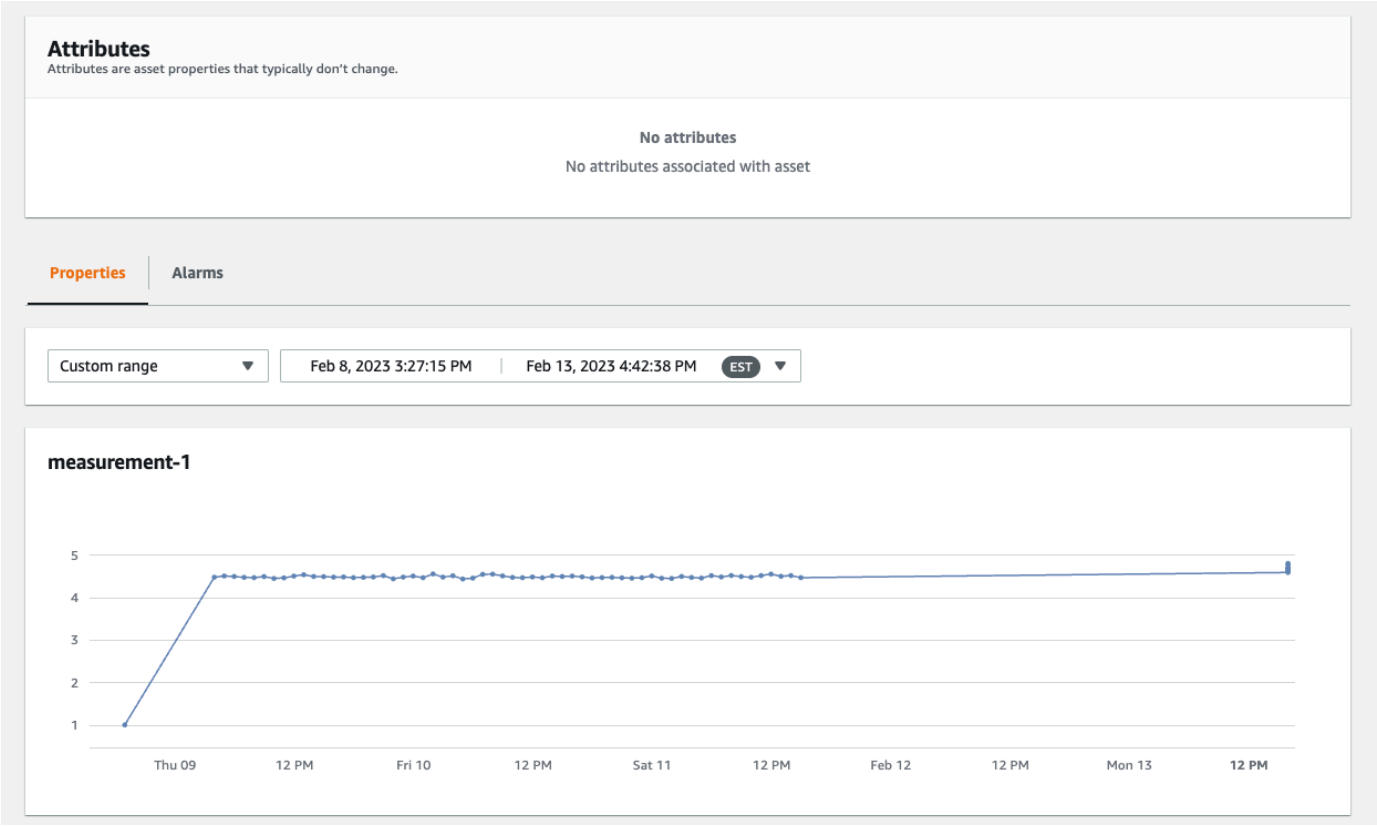
Verwenden Sie dieses Verfahren, um Ihre gesicherten Daten und Edge-Gateway-Wiederherstellungen zu validieren. SiteWise

> **Note**
>
> Dieses Verfahren setzt voraus, dass Sie für installiert haben. AWS OpsHub AWS IoT SiteWise Weitere Informationen finden Sie unter Verwalten von SiteWise Edge-Gateways mithilfe von AWS OpsHub . AWS IoT SiteWise

1. Öffnen AWS OpsHub für AWS IoT SiteWise.
2. Überprüfen Sie auf der Seite mit den SiteWise Edge-Gateway-Einstellungen den Status der einzelnen Komponenten, die in der Tabelle Komponenten aufgeführt sind. Stellen Sie sicher, dass die Statusfarbe grün ist und die Anzeige LÄUFT anzeigt.



3. Überprüfen Sie Ihre früheren Daten im Portal-Dashboard, um zu überprüfen, ob sowohl die alten als auch die neuen Daten ordnungsgemäß eingerichtet sind. Zwischen vergangenen und neuen Daten wird es zu Ausfallzeiten kommen. Sie sollten davon ausgehen, dass eine Dauer angezeigt wird, für die keine Datenpunkte erfasst werden.



Wenn Sie Probleme beim Sichern oder Wiederherstellen eines SiteWise Edge-Gateways haben, finden Sie weitere Informationen zur Problembehandlung bei einem AWS IoT SiteWise Edge-Gateway.

SiteWise Edge-Gateways einrichten ()AWS IoT Greengrass Version 1

> **Note**
>
> SiteWise Edge-Gateways, die auf laufen, AWS IoT Greengrass V1 sind nur verfügbar, wenn Sie vor dem 29. Juli 2021 mit der Nutzung dieser Funktion begonnen haben. Andernfalls richten Sie SiteWise Edge-Gateways ein, die auf ausgeführt werden. AWS IoT Greengrass V2

Sie können Industriedaten an AWS IoT SiteWise ein SiteWise Edge-Gateway senden, um Daten von Industrieanlagen hochzuladen. Das SiteWise Edge-Gateway dient als Vermittler zwischen AWS

IoT SiteWise und Ihren industriellen Datengeräten. AWS IoT SiteWise stellt AWS IoT Greengrass Komponenten bereit, die Sie auf jedem Gerät bereitstellen können, das AWS IoT Greengrass zur Einrichtung eines SiteWise Edge-Gateways verwendet werden kann. AWS IoT SiteWise unterstützt die Verknüpfung mit dem OPC-UA-Serverprotokoll.

Wenn Sie AWS IoT SiteWise Edge-Gateways haben, die auf laufen AWS IoT Greengrass V1, können Sie Ihre SiteWise Edge-Gateways auf aktualisieren. AWS IoT Greengrass V2 Weitere Informationen finden Sie unter Anweisungen für das Upgrade von SiteWise Edge-Gateways von auf. AWS IoT Greengrass V1 AWS IoT Greengrass V2

Themen

- Auswahl eines AWS IoT Greengrass V1 SiteWise Edge-Gateway-Geräts
- Konfiguration eines AWS IoT Greengrass V1 SiteWise Edge-Gateways
- Konfiguration von Datenquellen auf AWS IoT Greengrass V1 SiteWise Edge-Gateways

Auswahl eines AWS IoT Greengrass V1 SiteWise Edge-Gateway-Geräts

Wählen Sie ein lokales Gerät, das am besten zu Ihrem Industriebetrieb passt. Sie können ein SiteWise Edge-Gateway auf jedem Gerät konfigurieren, das ausgeführt werden kann AWS IoT Greengrass. Alle lokalen Geräte müssen die folgenden Anforderungen erfüllen:

- Unterstützt die AWS IoT Greengrass Core-Software v1.10.2 oder höher. Weitere Informationen finden Sie im AWS IoT Greengrass Version 1 Entwicklerhandbuch unter Unterstützte Plattformen und Anforderungen.
- Hat mindestens 4 GB RAM.
- Sie müssen über mindestens 10 GB an freiem Festplattenspeicherplatz verfügen.
- Support für Java 8 Virtual Machine (JVM).

Wenn Sie planen, Daten am Edge mit zu verarbeiten AWS IoT SiteWise, muss Ihr lokales Gerät außerdem die folgenden Anforderungen erfüllen:

- Hat einen x86-64-Bit-Quad-Core-Prozessor.
- Hat mindestens 16 GB RAM.
- Hat mindestens 32 GB RAM, wenn Sie Windows verwenden.
- Hatte mindestens 256 GB freien Festplattenspeicher.

Der für das Caching von Daten zur zeitweiligen Internetkonnektivität benötigte Festplattenspeicher ist von folgenden Faktoren abhängig:

- Zahl der hochgeladenen Daten-Streams
- Datenpunkte pro Daten-Stream pro Sekunde
- Größe jedes Datenpunkts
- Kommunikationsgeschwindigkeiten
- Erwartete Netzwerkausfallzeit

Die zum Abfragen und Hochladen von Daten benötigte Rechenkapazität ist von folgenden Faktoren abhängig:

- Zahl der hochgeladenen Daten-Streams
- Datenpunkte pro Daten-Stream pro Sekunde

Konfiguration eines AWS IoT Greengrass V1 SiteWise Edge-Gateways

Ein AWS IoT SiteWise Edge-Gateway dient als Vermittler zwischen Ihren Industrieanlagen und AWS IoT SiteWise. Sie können die SiteWise Edge-Gateway-Software auf jedem Gerät bereitstellen, das ausgeführt AWS IoT Greengrass werden kann. Weitere Informationen finden Sie unter Auswahl eines AWS IoT Greengrass V1 SiteWise Edge-Gateway-Geräts.

Sie können AWS IoT SiteWise die lokale Verarbeitung von Daten auf Ihren Edge-Geräten aktivieren, indem Sie das Datenverarbeitungspaket auf Ihrem SiteWise Edge-Gateway verwenden. Sie tun dies, wenn Sie Ihr SiteWise Edge-Gateway zu hinzufügen AWS IoT SiteWise. Weitere Informationen zur Verarbeitung von Daten am Edge finden Sie unterthe section called “Aktivierung der Edge-Datenverarbeitung”.

> **Note**
>
> Wir empfehlen, dass Sie die folgenden Schritte mit jemandem durchführen, der über IT-administrativen Zugriff auf Ihre lokalen und Unternehmensnetzwerke verfügt. Für diese Schritte ist möglicherweise eine Person erforderlich, die sich mit Ihren Industrieanlagen auskennt und befugt ist, Firewall-Einstellungen zu konfigurieren.

Themen

- Einrichtung der SiteWise Edge-Gateway-Umgebung
- Eine IAM-Richtlinie und -Rolle erstellen
- Eine AWS IoT Greengrass Gruppe konfigurieren
- Konfiguration des AWS IoT SiteWise Connectors
- Hinzufügen des SiteWise Edge-Gateways zu AWS IoT SiteWise

Einrichtung der SiteWise Edge-Gateway-Umgebung

In diesem Verfahren installieren AWS IoT Greengrass und konfigurieren Sie Ihr SiteWise Edge-Gateway zur Verwendung mit AWS IoT SiteWise.

> **Note**
>
> Dieser Abschnitt enthält Anweisungen zum Installieren von Paketen mit dem Befehl `apt`. Die Anweisungen gelten für Systeme mit Ubuntu oder ähnliche Systeme. Wenn Sie kein ähnliches System verwenden, lesen Sie die Dokumentation für Ihre Distribution und verwenden Sie das empfohlene Paketinstallationsprogramm.

So richten Sie das SiteWise Edge-Gateway ein

1. Ändern Sie gegebenenfalls die BIOS-Einstellungen des SiteWise Edge-Gateways wie folgt.
   a. Stellen Sie sicher, dass das SiteWise Edge-Gateway nach einem möglichen Stromausfall automatisch neu gestartet wird, falls zutreffend.
   b. Stellen Sie gegebenenfalls sicher, dass das SiteWise Edge-Gateway nicht in den Ruhezustand oder in den Standbymodus wechselt.
2. Stellen Sie sicher, dass das SiteWise Edge-Gateway eine Verbindung zum Internet herstellt.
3. (Optional) Um das SiteWise Edge-Gateway ohne Maus, Tastatur und Monitor zu verwenden, führen Sie die folgenden Schritte aus, um es `ssh` auf dem SiteWise Edge-Gateway einzurichten:
   a. Wenn Sie das SSH-Paket noch nicht installiert haben, führen Sie den folgenden Befehl aus.

      ```
      sudo apt install ssh
      ```

   b. Führen Sie den folgenden Befehl aus.

```
service ssh status
```

c. Um zu bestätigen, dass der SSH-Server ausgeführt wird, suchen Sie in der Ausgabe nach `Active: active (running)`.

d. Drücken Sie zum Beenden Q.

Führen Sie den folgenden Befehl aus, um mithilfe von SSH von einem anderen Computer aus eine Verbindung zum SiteWise Edge-Gateway herzustellen. Ersetzen Sie den *Benutzernamen* durch die Benutzeranmeldung und *IP* durch die IP-Adresse des SiteWise Edge-Gateways.

```
ssh username@IP
```

Sie können das `-p` *port-number*-Argument verwenden, um eine Verbindung mit einem anderen Port als Standardport 22 herzustellen.

4. Laden Sie die AWS IoT Greengrass Core-Software v1.10.2 oder höher herunter, installieren Sie sie und erstellen Sie eine AWS IoT Greengrass Gruppe für Ihr SiteWise Edge-Gateway. Befolgen Sie dazu die Anweisungen unter Erste Schritte mit AWS IoT Greengrass im AWS IoT Greengrass -Entwicklerhandbuch.

   Es wird empfohlen, das AWS IoT Greengrass -Geräte-Setup-Skript auszuführen, um schnell beginnen zu können. Wenn Sie sich die AWS IoT Greengrass Anforderungen und Prozesse genauer ansehen möchten, können Sie die Einrichtung AWS IoT Greengrass anhand der Schritte in Modul 1 und Modul 2 durchführen.

   > **Important**
   >
   > Sehen Sie sich die AWS Regionen an, in denen AWS IoT SiteWise dies unterstützt wird. Wenn Sie eine Region für auswählen AWS IoT Greengrass, stellen Sie sicher, dass die Region auch unterstützt AWS IoT SiteWise. Andernfalls können Sie Ihr SiteWise Edge-Gateway nicht mit verbinden AWS IoT SiteWise.

   Bevor Sie mit dem nächsten Schritt fortfahren, sollte die AWS IoT Greengrass Core-Software auf Ihrem SiteWise Edge-Gateway installiert sein.

5. Führen Sie die folgenden Befehle aus, um Java 8 zu installieren:

```
sudo apt update
      sudo apt install openjdk-8-jre
```

Die SiteWise Edge-Gateway-Software, die Sie später in diesem Handbuch installieren, verwendet eine Java 8-Runtime.

6. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob Java erfolgreich installiert wurde:

```
java -version
```

7. Die AWS IoT Greengrass Core-Software geht von einem `java8` Verzeichnis aus. Führen Sie den folgenden Befehl aus, um Ihre Java-Installation mit diesem Verzeichnis `java8` zu verknüpfen.

```
sudo ln -s /usr/bin/java /usr/bin/java8
```

8. Führen Sie den folgenden Befehl aus, um ein `/var/sitewise` Datenverzeichnis zu erstellen und die `ggc_user` Berechtigungen für dieses Verzeichnis zu vergeben. AWS IoT SiteWise speichert Daten in diesem Verzeichnis. Sie haben das `ggc_user` bei der Einrichtung zu einem AWS IoT Greengrass früheren Zeitpunkt dieses Verfahrens erstellt.

```
sudo mkdir /var/sitewise
      sudo chown ggc_user /var/sitewise
      sudo chmod 700 /var/sitewise
```

Das `/var/sitewise` ist das Standardverzeichnis, das AWS IoT SiteWise verwendet. Sie können den Verzeichnispfad anpassen (z. B. durch `/var/sitewise` ersetzen/`var/`*`custom`*`/`*`path`*`/`), dafür sind jedoch zusätzliche Schritte erforderlich, nachdem das SiteWise Edge-Gateway erstellt wurde. Weitere Informationen finden Sie in Schritt 6 in Konfiguration des AWS IoT SiteWise Connectors.

9. Bitten Sie Ihren IT-Administrator bei Bedarf, die folgenden Endpunkte und Ports zur Liste der zulässigen lokalen Netzwerke hinzuzufügen:

   - Ports: 443, 8443 und 8883.

> **Important**
>
> Sie können AWS IoT Greengrass Core so konfigurieren, dass nur Port 443 für die gesamte Netzwerkkommunikation verwendet wird. Weitere Informationen finden Sie unter Verbindungsherstellung auf Port 443 oder über einen Netzwerk-Proxy im Entwicklerhandbuch für AWS IoT Greengrass .

- Die IP-Adresse Ihres SiteWise Edge-Gateways (Port 443). Um die IP-Adresse zu erhalten, führen Sie den Befehl `ip address` oder `ifconfig` aus und notieren Sie sich den `inet`-Wert (beispielsweise `203.0.113.0`).
- Der AWS IoT SiteWise Datenendpunkt: `data.iotsitewise.`*`region`*`.amazonaws.com` (Port 443).
- Die folgenden AWS Endpunkte, die das SiteWise Edge-Gateway verwendet. Sie finden diese in der Datei */`greengrass-root`*`/config/config.json`. Ersetzen Sie *`greengrass-root`* durch den Stamm Ihrer AWS IoT Greengrass -Installation.
  - ggHost: `greengrass-ats.iot.`*`region`*`.amazonaws.com` (Ports 443, 8443 und 8883).
  - iotHost: *`prefix`*`-ats.iot.`*`region`*`.amazonaws.com` (Ports 443, 8443 und 8883).

  Weitere Informationen finden Sie unter AWS IoT Greengrass Endpunkte und -Kontingente.

10. Wenn die AWS IoT Greengrass Core-Software noch nicht ausgeführt wird, führen Sie den folgenden Befehl aus, um die AWS IoT Greengrass Core-Software zu starten. Ersetzen Sie *`greengrass-root`* durch das Stammverzeichnis Ihrer Installation. AWS IoT Greengrass Standard für *`greengrass-root`* ist `/greengrass`.

    ```
    cd /greengrass-root/ggc/core
          sudo ./greengrassd start
    ```

    Folgende Meldung sollte angezeigt werden: `Greengrass successfully started with PID:` *`some-PID-number`*

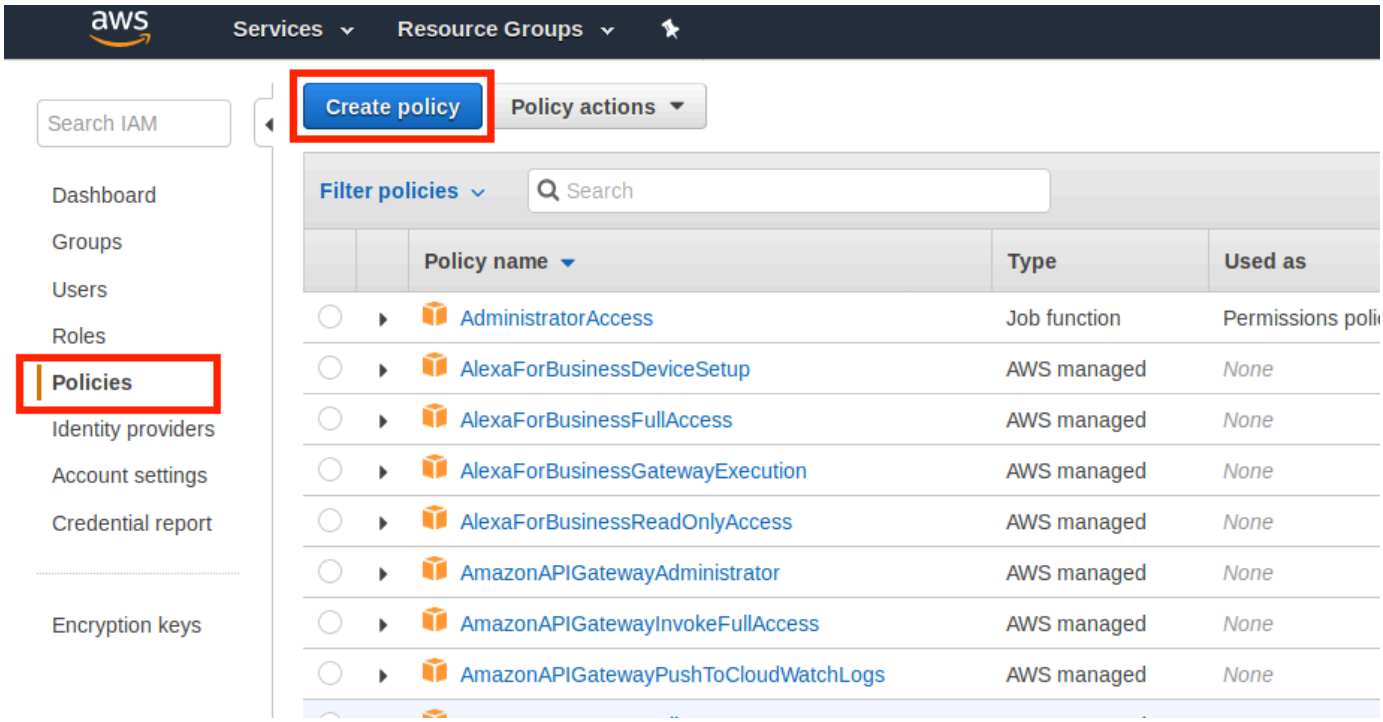
11. Konfigurieren Sie die AWS IoT Greengrass Core-Software so, dass sie automatisch gestartet wird, wenn Ihr SiteWise Edge-Gateway eingeschaltet wird. Schlagen Sie in der Dokumentation zum Betriebssystem Ihres SiteWise Edge-Gateways nach.

Eine IAM-Richtlinie und -Rolle erstellen

Sie müssen eine AWS Identity and Access Management (IAM-) Richtlinie und Rolle erstellen, damit das SiteWise Edge-Gateway in Ihrem Namen AWS IoT SiteWise darauf zugreifen kann.

Um eine IAM-Richtlinie und -Rolle zu erstellen

1. Navigieren Sie zur IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies (Richtlinien) und dann Create policy (Richtlinie erstellen).



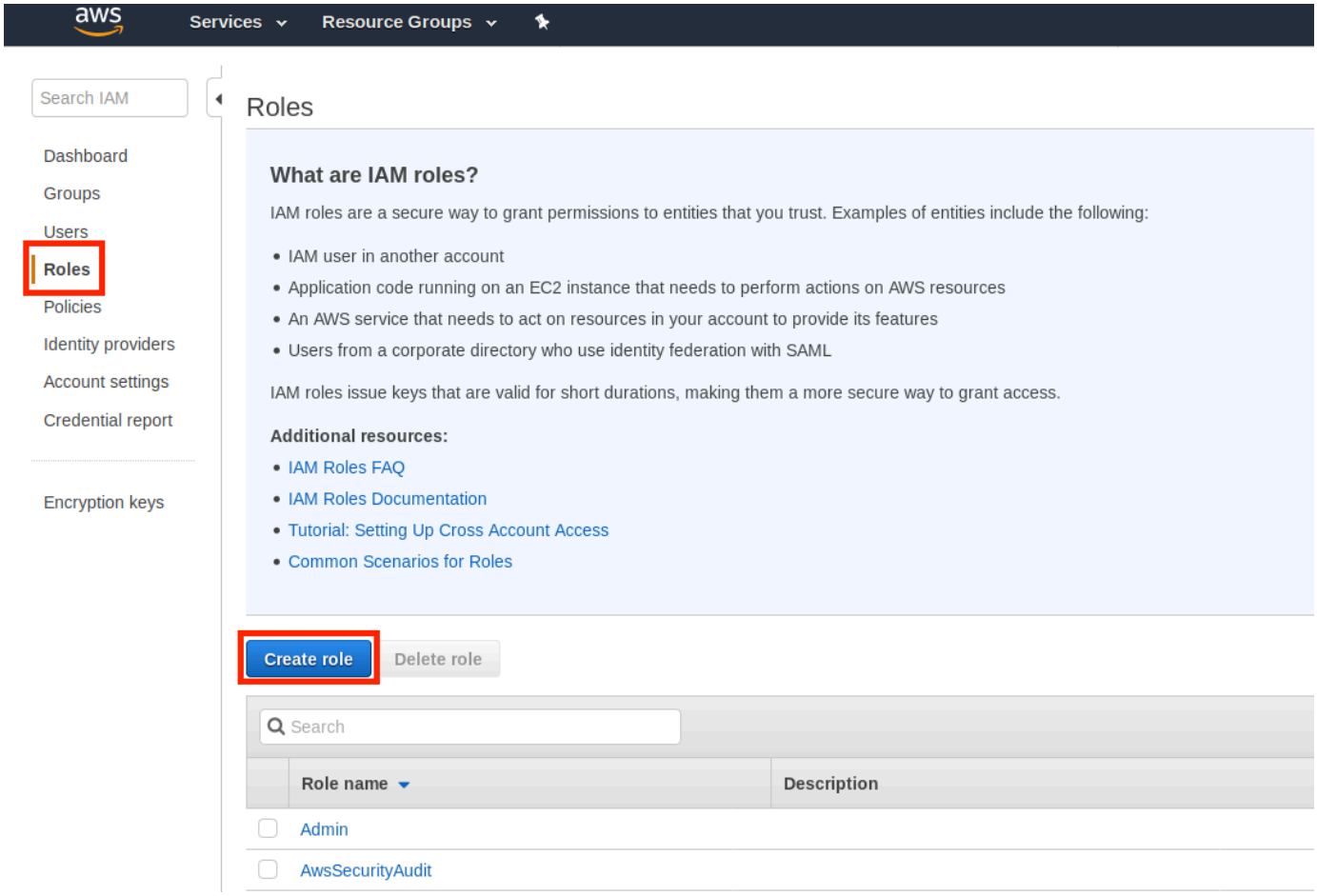
3. Löschen Sie auf der Registerkarte JSON den aktuellen Inhalt des Richtlinienfelds und fügen Sie folgende Richtlinie in das Feld ein.

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

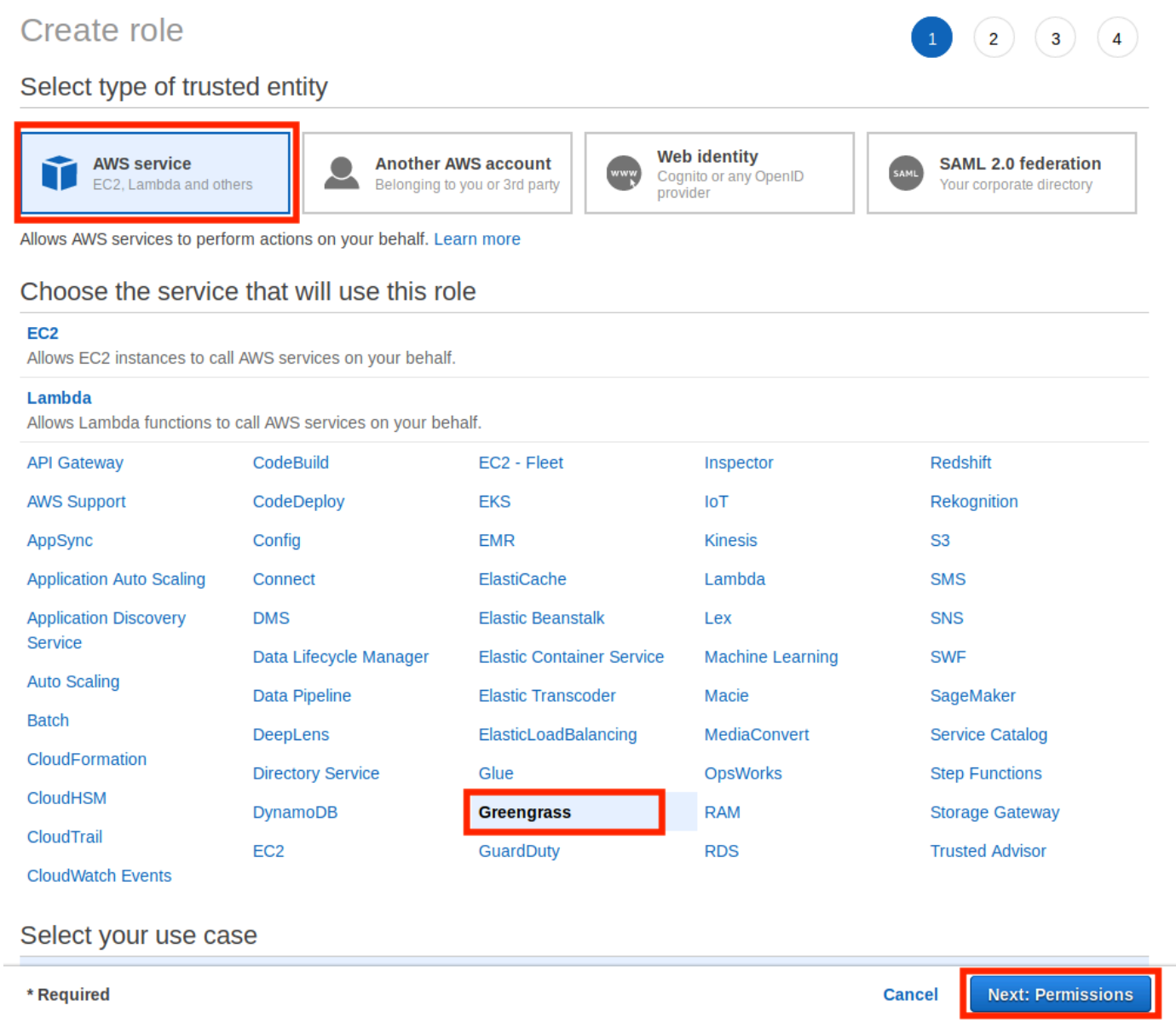
> **Note**
>
> Um die Sicherheit zu erhöhen, können Sie in der `Condition` Eigenschaft einen Pfad zur AWS IoT SiteWise Asset-Hierarchie angeben. Das folgende Beispiel ist eine Vertrauensrichtlinie, die einen Komponentenhierarchiepfad angibt.

```
{
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iotsitewise:BatchPutAssetPropertyValue",
            "Resource": "*",
            "Condition": {
              "StringLike": {
                "iotsitewise:assetHierarchyPath": [
                  "/root node asset ID",
                  "/root node asset ID/*"
                ]
              }
            }
          }
        ]
      }
```

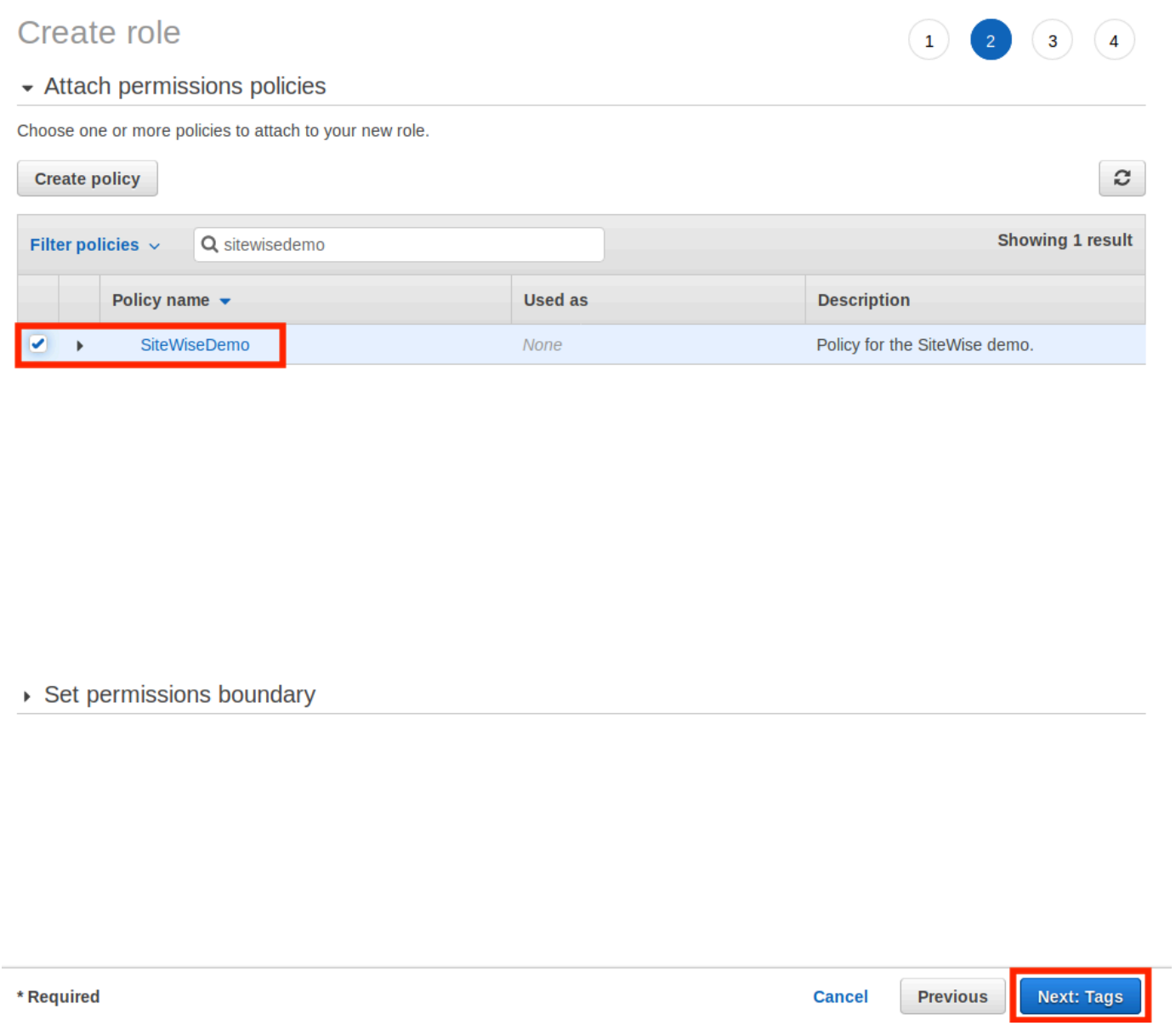
4. Wählen Sie Richtlinie prüfen.
5. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein und wählen Sie dann Create policy (Richtlinie erstellen) aus.
6. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).



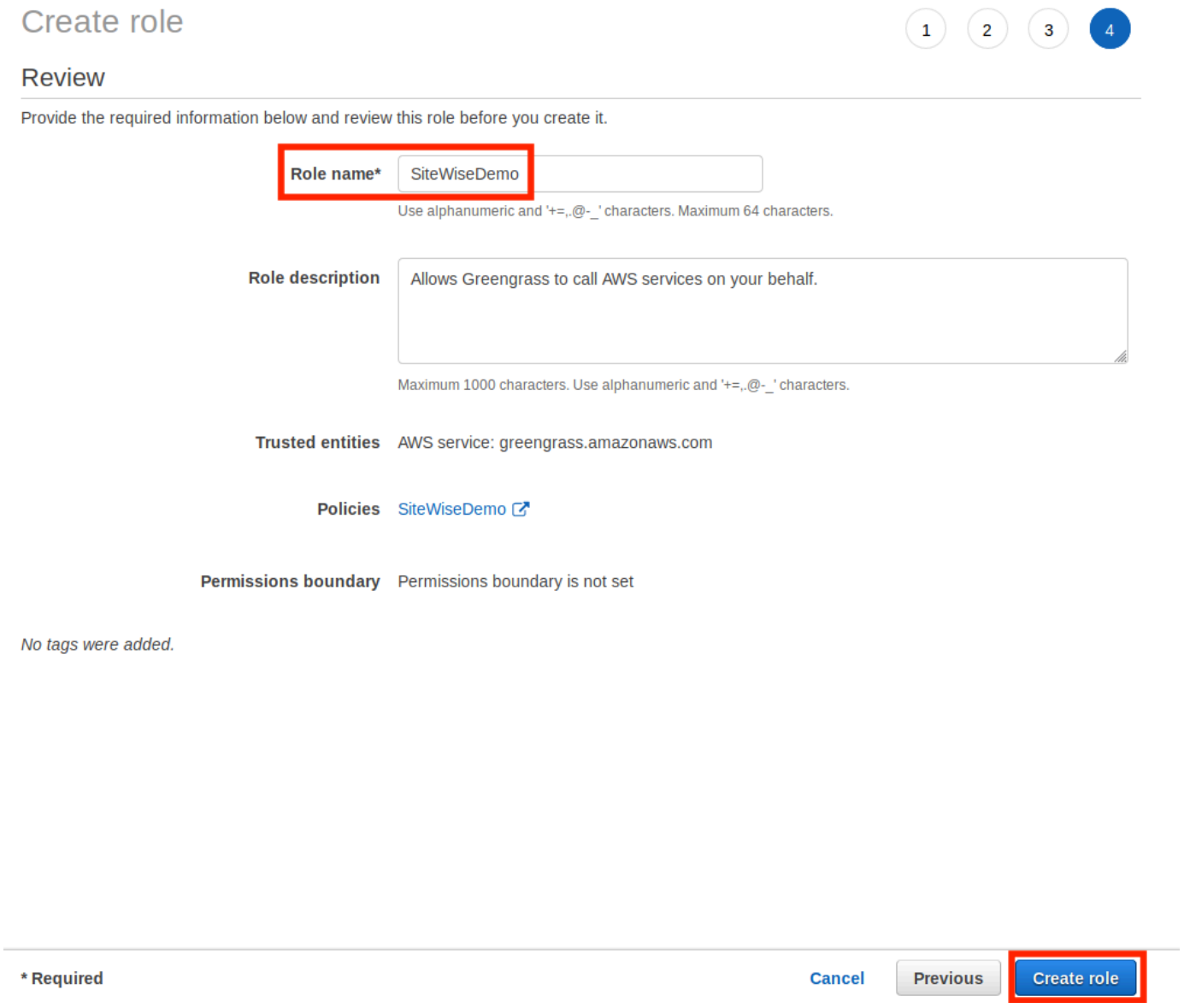
7. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus. Wählen Sie unter Choose the service that will use the role (Service auswählen, der die Rolle verwendet) als Services, der die Rolle verwendet, Greengrass aus und klicken Sie dann auf Next: Permissions (Weiter:Berechtigungen).



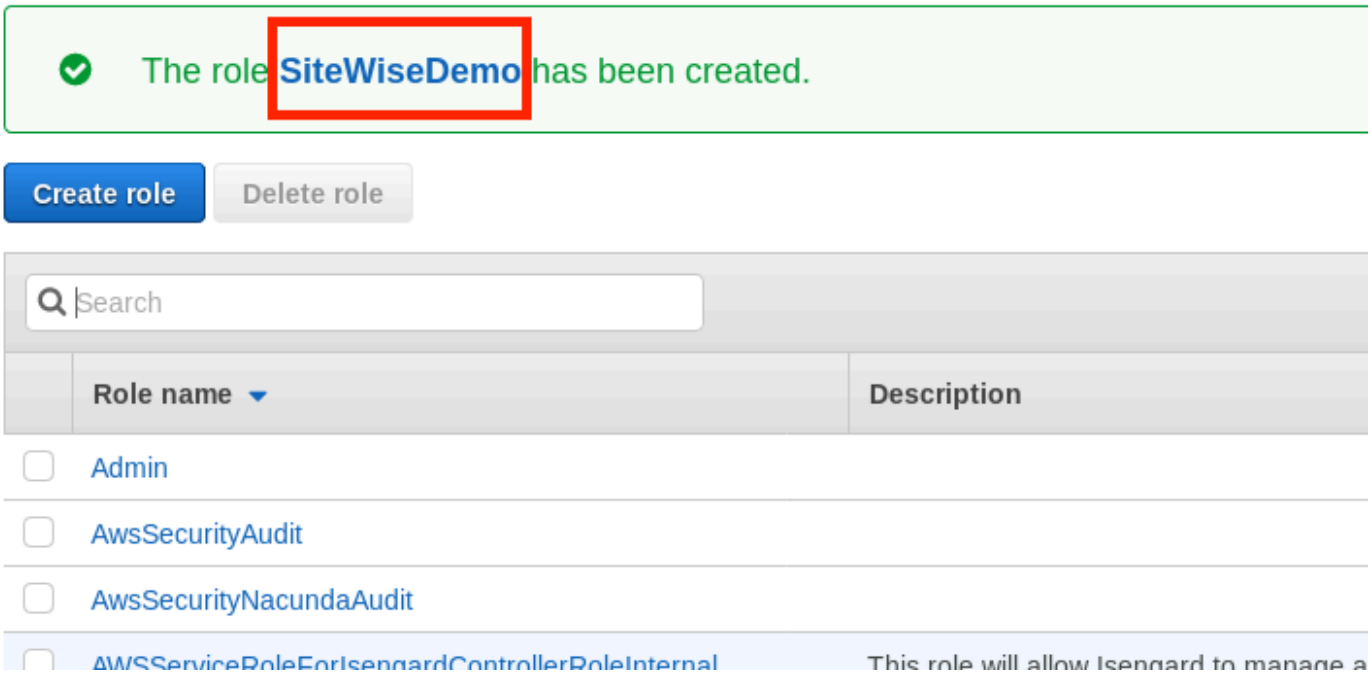
8. Suchen Sie nach der Richtlinie, die Sie erstellt haben, aktivieren Sie das Kontrollkästchen und wählen Sie dann Weiter: Tags aus.



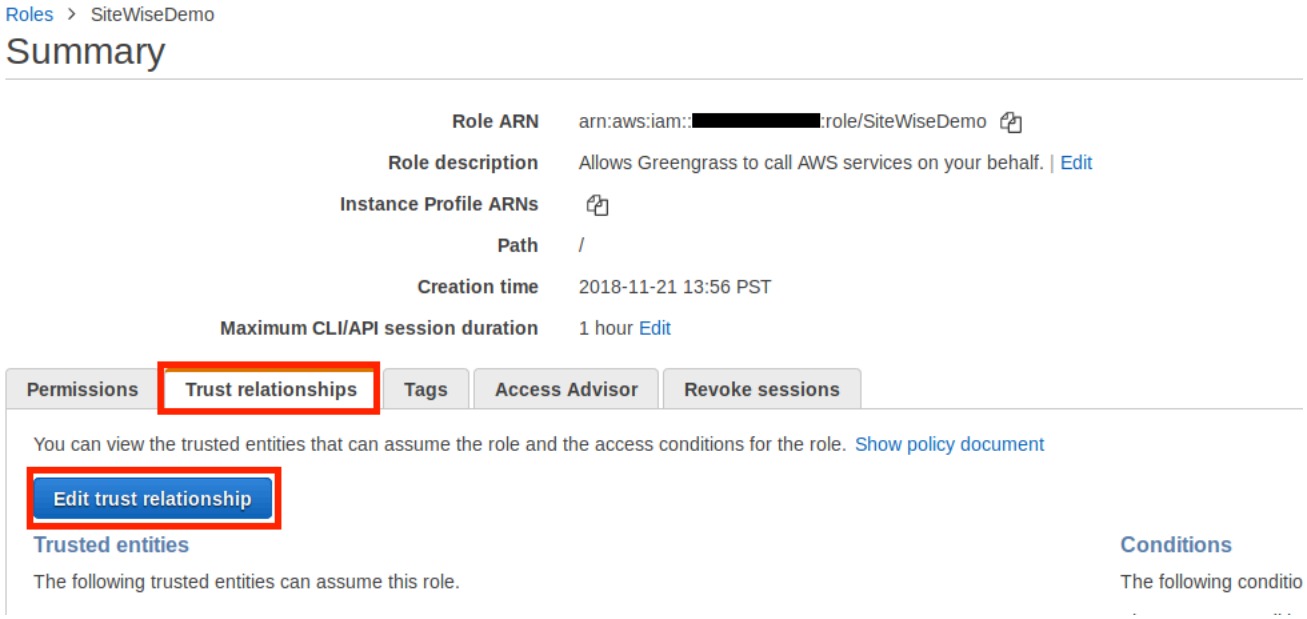
9. (Optional) Fügen Sie Tags zu Ihrer Rolle hinzu und wählen Sie dann Next: Review (Weiter: Prüfen) aus.
10. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und wählen Sie dann Create role (Rolle erstellen) aus.



11. Wählen Sie im grünen Banner den Link zu Ihrer neuen Rolle. Sie können auch das Suchfeld verwenden, um die Rolle zu finden.



12. Klicken Sie auf der Registerkarte Trust Relationships (Vertrauensbeziehungen) auf Edit Trust Relationship (Vertrauensbeziehungen bearbeiten).



13. Ersetzen Sie den aktuellen Inhalt des Richtlinienfelds durch Folgendes und wählen Sie dann Update Trust Policy (Vertrauensrichtlinie aktualisieren) aus.

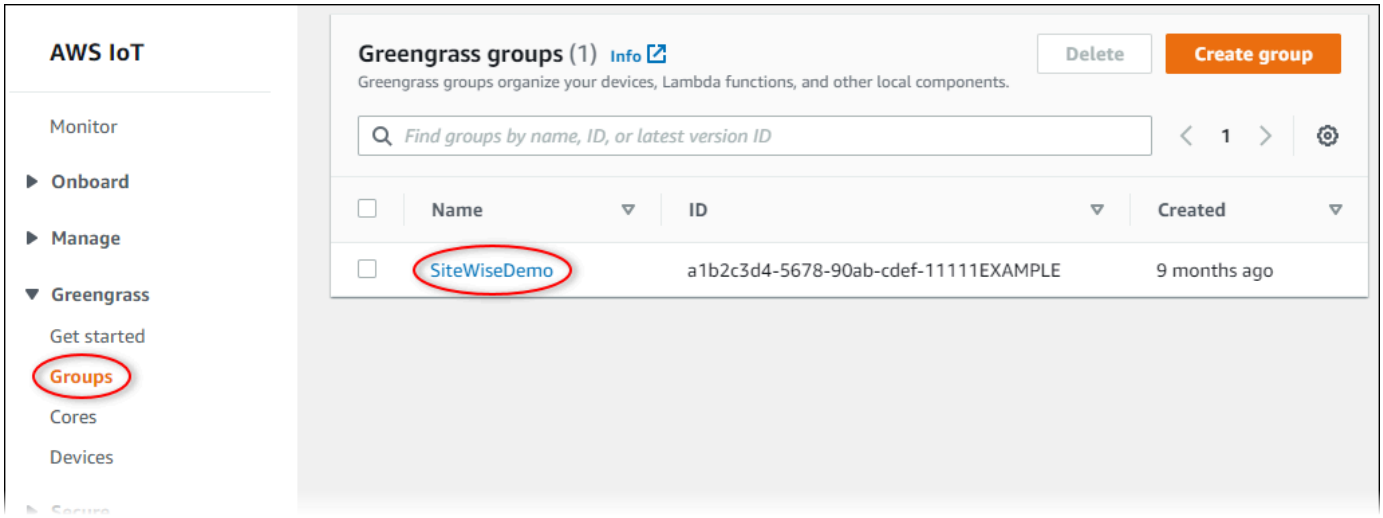
```
{
        "Version": "2012-10-17",
        "Statement": [
```

```
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "greengrass.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
```

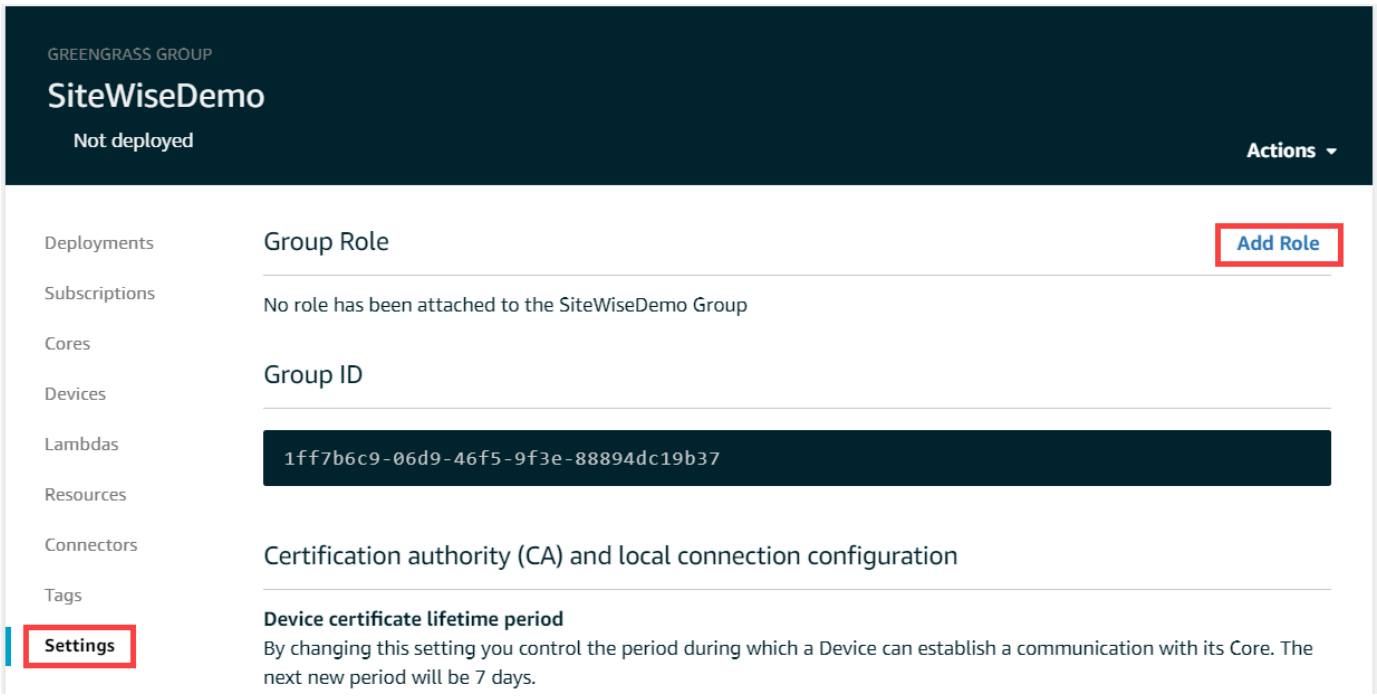
Eine AWS IoT Greengrass Gruppe konfigurieren

Um einer Gruppe eine IAM-Rolle zuzuweisen und den Stream-Manager zu aktivieren

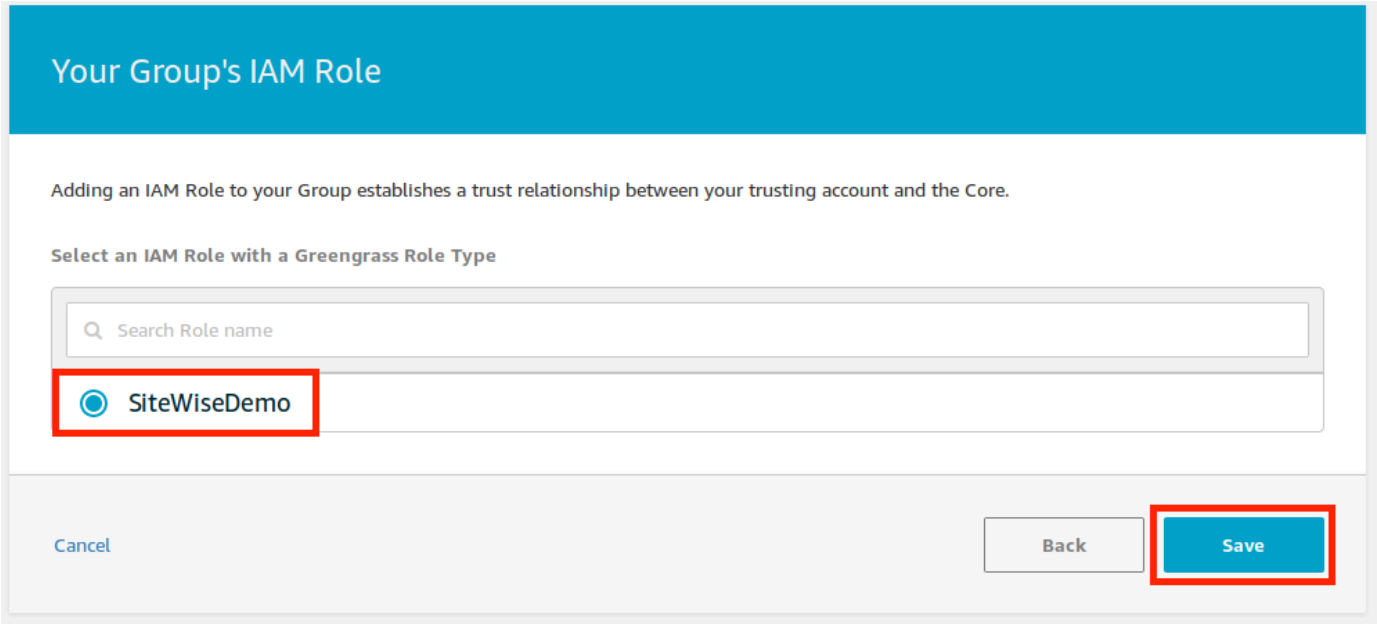
1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im linken Navigationsbereich unter Greengrass die Option Groups (Gruppen) und dann die Gruppe aus, die Sie in Einrichtung der SiteWise Edge-Gateway-Umgebung erstellt haben.



3. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus. Wählen Sie im Abschnitt Group Role (Gruppenrolle) die Option Add Role (Rolle hinzufügen).



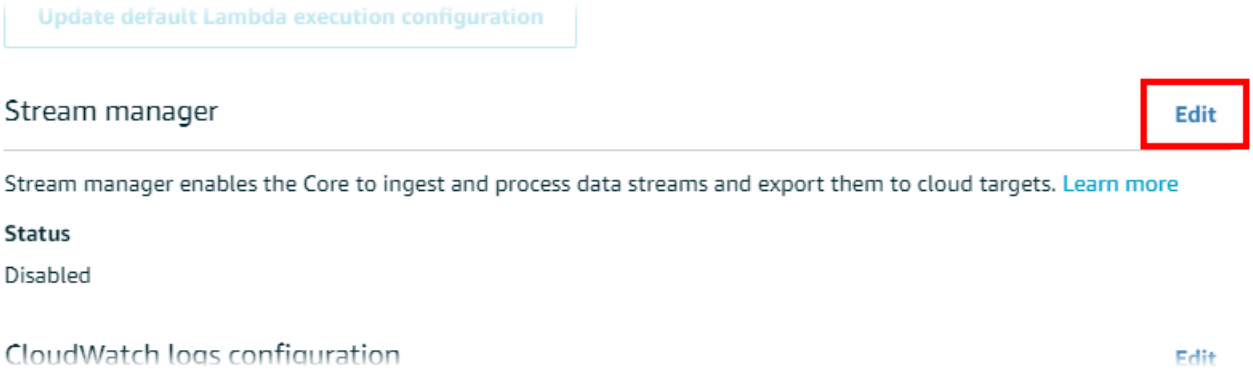
4. Wählen Sie die Rolle, die Sie in Eine IAM-Richtlinie und -Rolle erstellen erstellt haben, und dann Save (Speichern) aus.



5. Wählen Sie auf der Seite Settings (Einstellungen) im Abschnitt Stream-Manager die Option Edit (Bearbeiten).

   Stream Manager ist eine Funktion AWS IoT Greengrass , mit der Ihr AWS IoT Greengrass Core Daten in die AWS Cloud streamen kann. SiteWise Edge-Gateways erfordern, dass der Stream-

Manager aktiviert ist. Weitere Informationen finden Sie unter Verwalten von Datenströmen auf dem AWS IoT Greengrass Core im AWS IoT Greengrass Version 1 Entwicklerhandbuch.



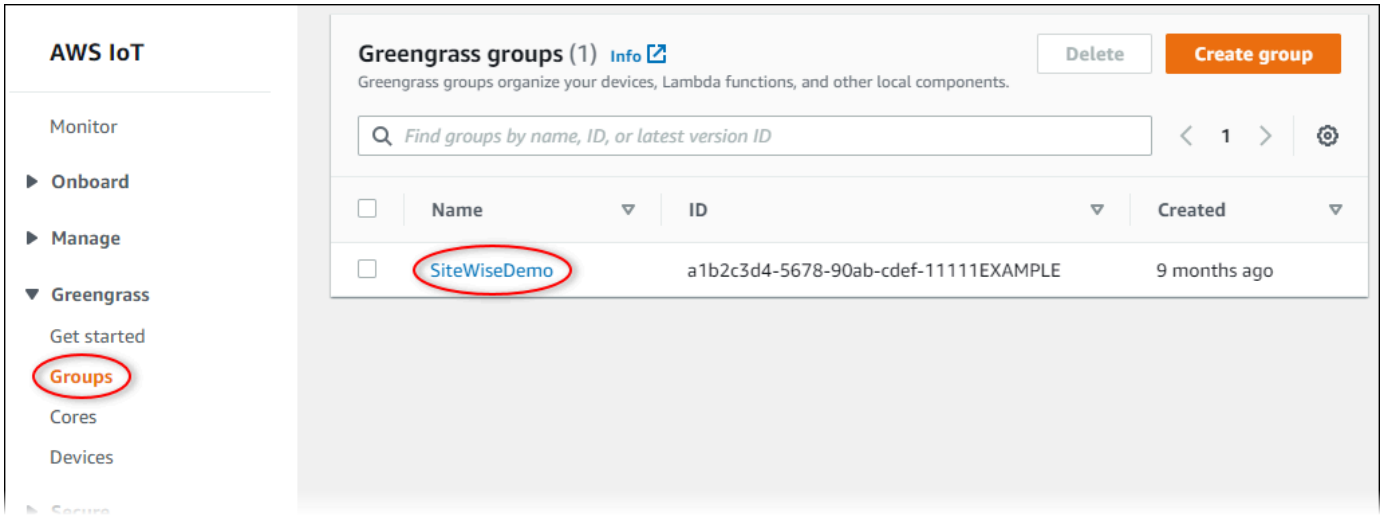
6. Wählen Sie Enable (Aktivieren) und anschließend Save (Speichern) aus.
7. Wählen Sie links oben Services aus, um sich auf das nächste Verfahren vorzubereiten.

Konfiguration des AWS IoT SiteWise Connectors

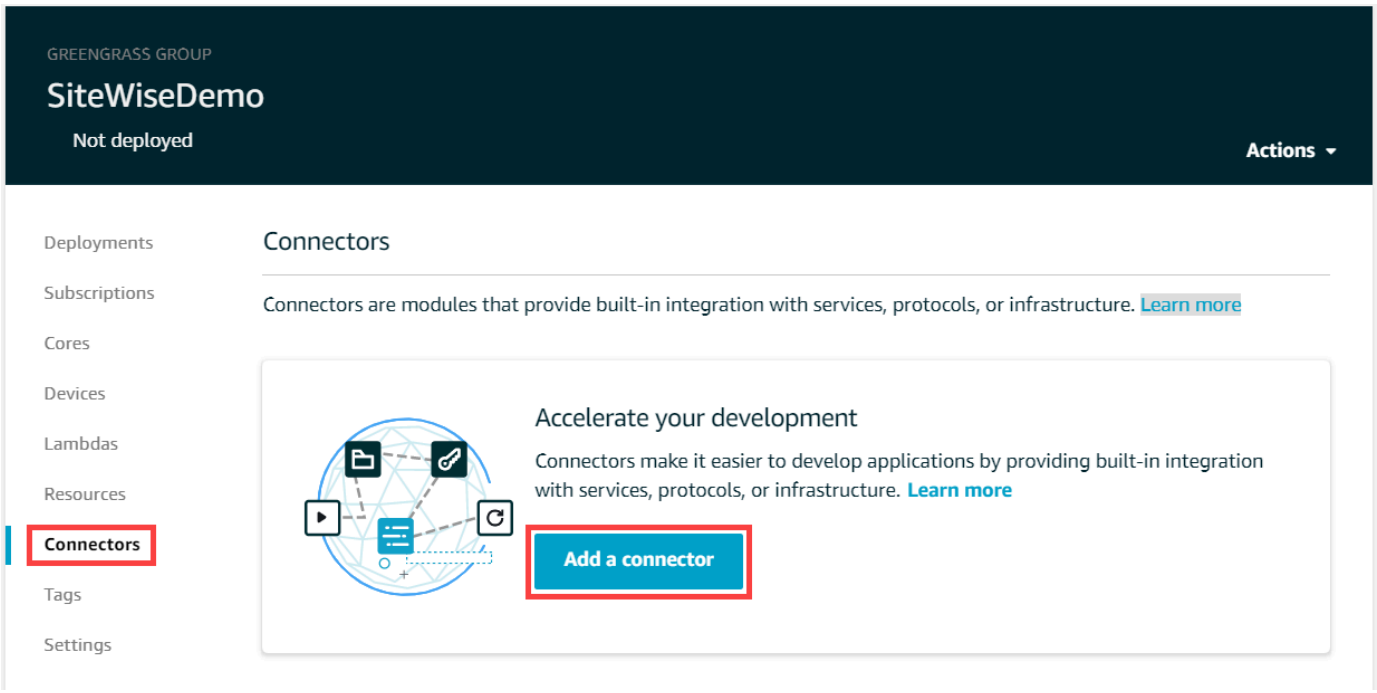
In diesem Verfahren konfigurieren Sie den AWS IoT SiteWise Connector in Ihrer Greengrass-Gruppe. Bei Komponenten handelt es sich um vorgefertigte Module, die den Entwicklungszyklus für Common Edge-Szenarien beschleunigen. Weitere Informationen finden Sie unter AWS IoT Greengrass Konnektoren im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

Um den AWS IoT SiteWise Konnektor zu konfigurieren

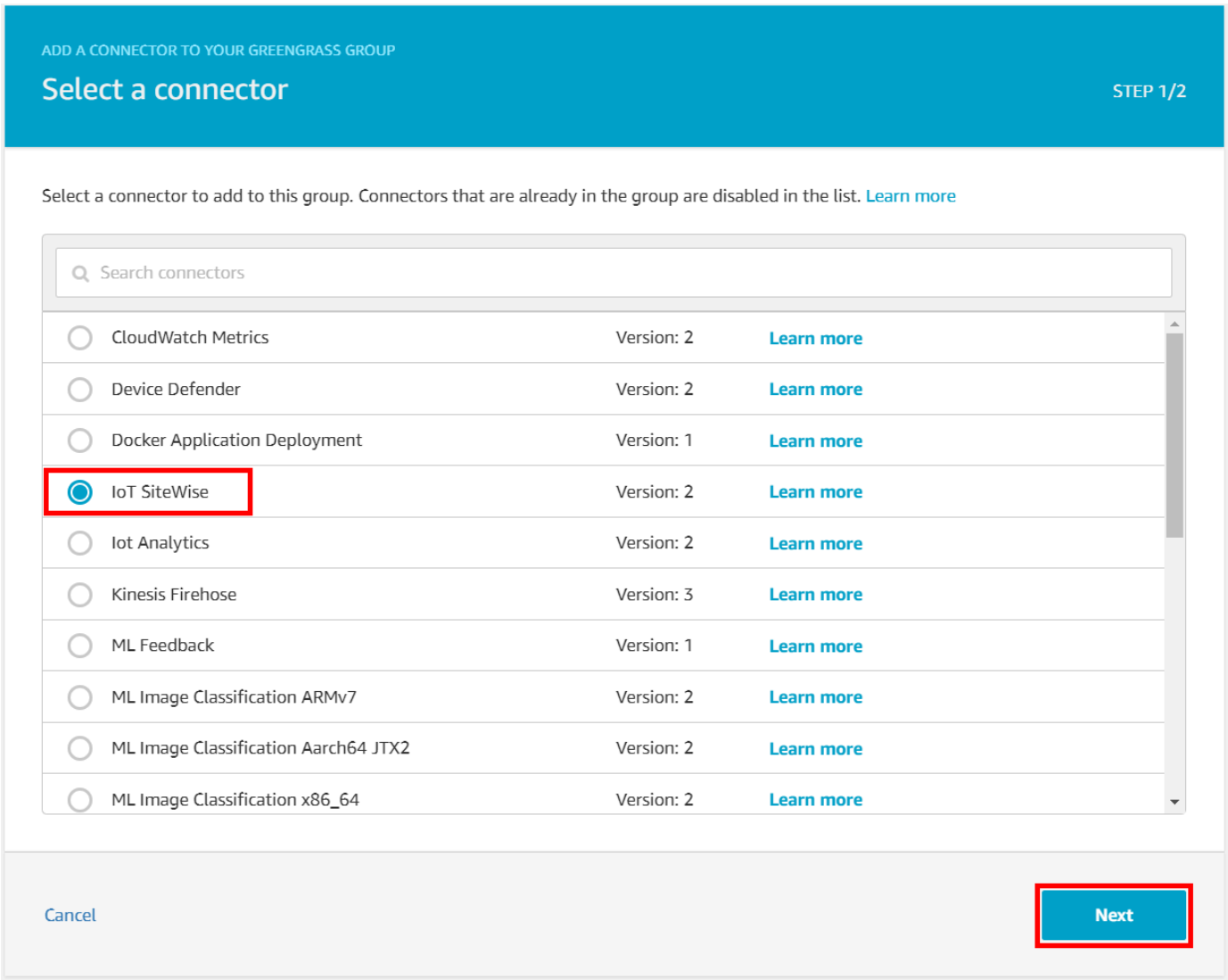
1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im linken Navigationsbereich unter Greengrass die Option Groups (Gruppen) und dann die Gruppe aus, die Sie in Einrichtung der SiteWise Edge-Gateway-Umgebung erstellt haben.



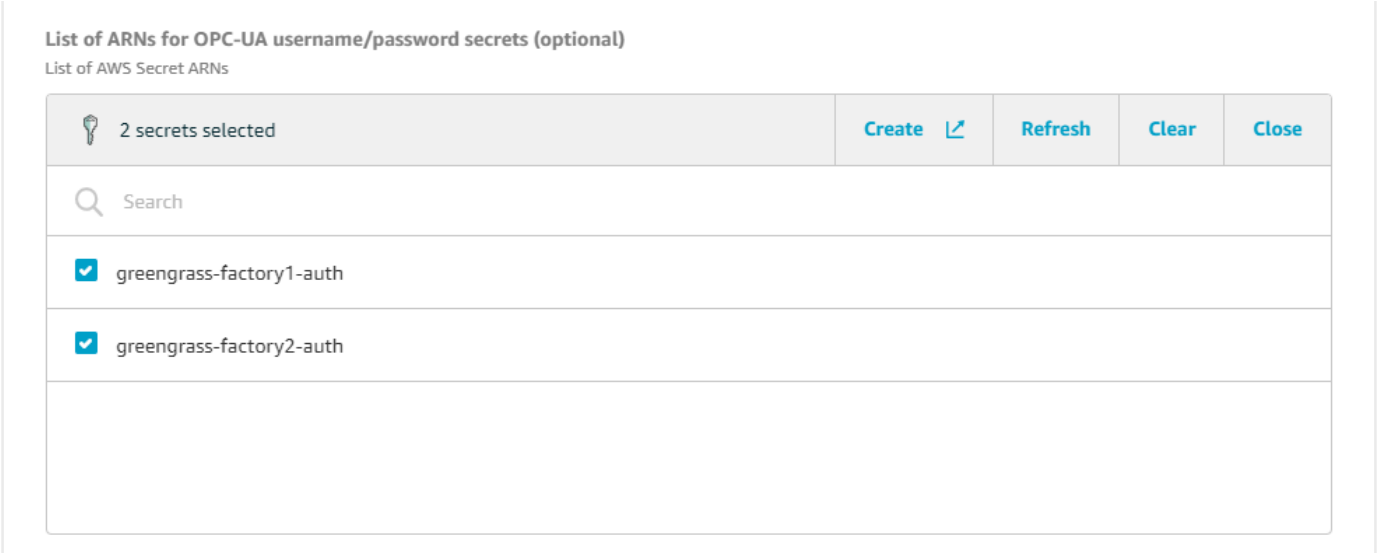
3. Wählen Sie im linken Navigationsbereich die Option Connectors aus. Wählen Sie auf der Seite Connectors die Option Add a Connector (Connector hinzufügen) aus.



4. Wählen Sie IoT SiteWise aus der Liste aus und klicken Sie auf Weiter.



5. Wenn Ihr Server eine Authentifizierung erfordert, können Sie geheime AWS Secrets Manager Daten mit dem Benutzernamen und dem Passwort des Servers erstellen. Anschließend können Sie jedes Geheimnis an Ihre Greengrass-Gruppe anhängen und es unter Liste der ARNs für Benutzername/Passwort-Geheimnisse auswählen. Weitere Informationen zum Erstellen und Konfigurieren von Secrets finden Sie unter Konfigurieren der Quellauthentifizierung. Sie können Ihrem Connector auch später noch Secrets hinzufügen.



6. Wenn Sie Ihr SiteWise Edge-Gateway mit einem anderen Pfad als einrichten`/var/sitewise`, geben Sie diesen Pfad für Lokaler Speicherpfad ein.
7. (Optional) Geben Sie eine maximale Datenträgerpuffergröße für den Connector ein. Wenn der AWS IoT Greengrass Core die Verbindung zur AWS Cloud verliert, speichert der Connector Daten im Cache, bis er erfolgreich eine Verbindung herstellen kann. Wenn die Cachegröße die maximale Datenträgerpuffergröße überschreitet, verwirft der Konnektor die ältesten Daten aus der Warteschlange.
8. Wählen Sie Hinzufügen aus.
9. Wählen Sie rechts oben im Menü Actions (Aktionen) die Option Deploy (Bereitstellen) aus.
10. Wählen Sie Automatic detection (Automatische Erkennung) aus, um die Bereitstellung zu starten.

    Wenn die Bereitstellung fehlschlägt, wählen Sie erneut Deploy (Bereitstellen) aus. Wenn die Bereitstellung weiterhin fehlschlägt, finden Sie weitere Informationen im Abschnitt zur Fehlerbehebung für die AWS IoT Greengrass -Bereitstellung.

Hinzufügen des SiteWise Edge-Gateways zu AWS IoT SiteWise

In diesem Verfahren fügen Sie die Greengrass-Gruppe Ihres SiteWise Edge-Gateways zu AWS IoT SiteWise hinzu. Nachdem Sie Ihr SiteWise Edge-Gateway bei registriert haben AWS IoT SiteWise, kann der Dienst Ihre Datenquellenkonfigurationen auf Ihrem SiteWise Edge-Gateway bereitstellen.

Um das SiteWise Edge-Gateway hinzuzufügen AWS IoT SiteWise

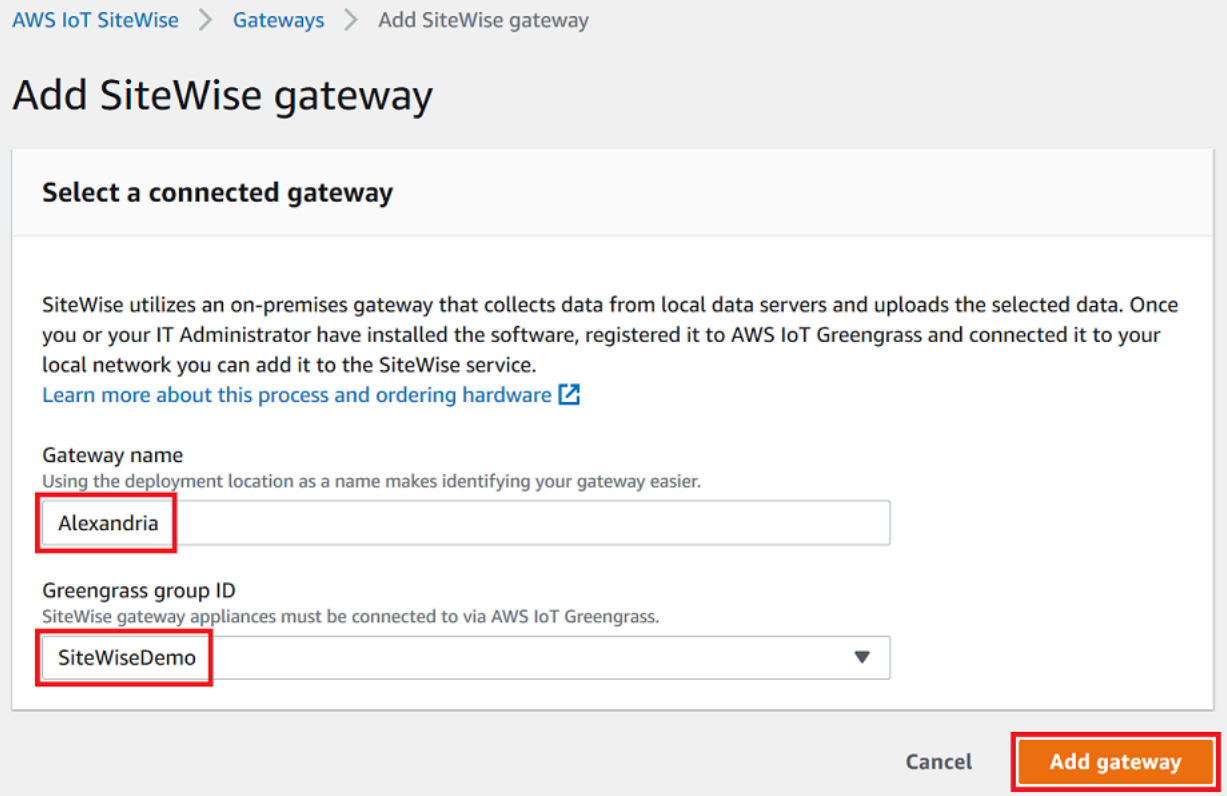
1. Navigieren Sie zur AWS IoT SiteWise -Konsole.

2. Wählen Sie Add gateway (Gateway hinzufügen) aus.
3. Gehen Sie auf der Seite SiteWise Gateway hinzufügen wie folgt vor:

   a. Geben Sie einen Namen für das SiteWise Edge-Gateway ein. Erwägen Sie, den Standort des SiteWise Edge-Gateways in den Namen aufzunehmen, damit Sie es leicht identifizieren können.

   b. Wählen Sie als Greengrass-Gruppen-ID die Greengrass-Gruppe aus, die Sie zuvor erstellt haben.

      Example



   c. (Optional) Wählen Sie für Edge-Funktionen das Datenverarbeitungspaket aus. Dies ermöglicht die Kommunikation zwischen Ihrem SiteWise Edge-Gateway und allen für den Edge konfigurierten Anlagenmodellen und Anlagen. Weitere Informationen finden Sie unter the section called “Aktivierung der Edge-Datenverarbeitung”.

> **Important**
>
> Wenn Sie das Datenverarbeitungspaket zu Ihrem SiteWise Edge-Gateway hinzufügen, müssen Sie den SiteWise Edge-Connector in Ihrer AWS IoT

Greengrass Gruppe konfigurieren und bereitstellen. Folgen Sie den nächsten Schritten.

d. Wählen Sie Add gateway (Gateway hinzufügen) aus.

4. Wenn Sie das Datenverarbeitungspaket zu Ihrem SiteWise Edge-Gateway hinzufügen, konfigurieren Sie den AWS IoT SiteWise Datenprozessor-Connector und stellen Sie ihn in Ihrer AWS IoT Greengrass Gruppe bereit. Folgen Sie den Schritten unterthe section called "Konfiguration des AWS IoT SiteWise Connectors", um den AWS IoT SiteWise Datenprozessor-Connector zu konfigurieren:

   a. Wählen Sie für Wählen Sie in der AWS IoT Greengrass Konsole einen Konnektor aus die Option AWS IoT SiteWise Datenprozessor.

   b. Geben Sie unter Lokaler Speicherpfad den Pfad zu Ihrem SiteWise Edge-Gateway ein.

   c. Wählen Sie Hinzufügen aus.

   d. Wählen Sie in der oberen rechten Ecke im Menü Aktionen die Option Bereitstellen und dann Automatische Erkennung aus, um die Bereitstellung zu starten.

Nach der Bereitstellung Ihres SiteWise Edge-Gateways können Sie für jede Industrieanlage, von der Ihr SiteWise Edge-Gateway Daten aufnehmen soll, eine Quelle hinzufügen. Weitere Informationen finden Sie unter Konfigurieren von Datenquellen.

Sie können CloudWatch Amazon-Metriken einsehen, um zu überprüfen, ob Ihr SiteWise Edge-Gateway eine Verbindung herstellt AWS IoT SiteWise. Weitere Informationen finden Sie unter AWS IoT Greengrass Version 1 Gateway-Metriken.

Konfiguration von Datenquellen auf AWS IoT Greengrass V1 SiteWise Edge-Gateways

Nachdem Sie ein AWS IoT SiteWise Edge-Gateway eingerichtet haben, können Sie Datenquellen so konfigurieren, dass Ihr SiteWise Edge-Gateway Daten von lokalen Industrieanlagen aufnehmen kann. AWS IoT SiteWise Jede Quelle steht für einen lokalen Server, z. B. einen OPC-UA-Server, mit dem Ihr SiteWise Edge-Gateway eine Verbindung herstellt und industrielle Datenströme abruft. Weitere Informationen zum Einrichten eines SiteWise Edge-Gateways finden Sie unter. Konfiguration eines AWS IoT Greengrass V1 SiteWise Edge-Gateways

> **Note**
>
> AWS IoT SiteWise startet Ihr SiteWise Edge-Gateway jedes Mal neu, wenn Sie eine Quelle hinzufügen oder bearbeiten. Ihr SiteWise Edge-Gateway nimmt während des Neustarts keine Daten auf. Die Zeit für den Neustart Ihres SiteWise Edge-Gateways hängt von der Anzahl der Tags in den Quellen Ihres SiteWise Edge-Gateways ab. Die Neustartzeit kann zwischen einigen Sekunden (für ein SiteWise Edge-Gateway mit wenigen Tags) und mehreren Minuten (für ein SiteWise Edge-Gateway mit vielen Tags) liegen.

Nachdem Sie Quellen erstellt haben, können Sie Ihre Datenströme mit Asset-Eigenschaften verknüpfen. Weitere Informationen zum Erstellen und Verwenden von Assets finden Sie unter Modellieren von industriellen Komponenten undZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Sie können CloudWatch Messwerte anzeigen, um zu überprüfen, ob eine Datenquelle verbunden ist AWS IoT SiteWise. Weitere Informationen finden Sie unter AWS IoT Greengrass Version 1 Gateway-Metriken.

AWS IoT SiteWise Unterstützt derzeit die folgenden Datenquellenprotokolle:

- OPC-UA — Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung.
- Modbus TCP — Ein Datenkommunikationsprotokoll, das als Schnittstelle zu speicherprogrammierbaren Steuerungen (SPS) verwendet wird.
- EtherNet/IP (EIP) — Ein industrielles Netzwerkprotokoll, das das Common Industrial Protocol (CIP) an Standard-Ethernet anpasst.

> **Note**
>
> SiteWise Edge-Gateways, auf denen sie laufen, unterstützen AWS IoT Greengrass V2 derzeit keine Modbus-TCP- und Ethernet-IP-Quellen.

Themen

- Konfigurieren Sie eine Modbus-TCP-Quelle
- Konfigurieren Sie eine EtherNet/IP (EIP) -Quelle

- Konfigurieren der Quellauthentifizierung
- Aktualisieren eines Connectors

Konfigurieren Sie eine Modbus-TCP-Quelle

Sie können die AWS IoT SiteWise Konsole oder eine AWS IoT SiteWise Edge-Gateway-Funktion verwenden, um eine Modbus-TCP-Quelle zu definieren und Ihrem SiteWise Edge-Gateway hinzuzufügen. Diese Quelle stellt einen lokalen Modbus-TCP-Server dar.

> **Note**
>
> - SiteWise Edge-Gateways, auf denen AWS IoT Greengrass V2 derzeit läuft, unterstützen keine Modbus-TCP-Quellen.
> - Sie müssen den AWS IoT SiteWise Connector installieren, um eine Modbus-TCP-Quelle verwenden zu können.

Sie können die Modbus-TCP-Quelle verwenden, um den Datentyp aus Ihrer Quelle in einen anderen Datentyp zu konvertieren, wenn er auf Ihrem SiteWise Edge-Gateway empfangen wird. Der Quelldatentyp bestimmt die Datentypen, die Sie für Ihre Zieldaten auswählen können. Sie können sich auch dafür entscheiden, Bytes mithilfe der Modbus-TCP-Quelle auszutauschen. Die folgende Tabelle enthält weitere Informationen zu den kompatiblen Quelldatentypen, Zieldatentypen und Swap-Modi.

Weitere Informationen zu Swap-Modi finden Sie im Artikel How Real (Floating Point) and 32-bit Data is Encoded in Modbus RTU Messages zur Modbus-Nachrichtenkodierung.

Quelldatentyp	Kompatible Zieldatentypen	Kompatible Swap-Modi	Kompatible Steckerversionen
ASCII	String	Kein Swap	2
UTF8	String	Kein Swap	2
ISO8859	String	Kein Swap	2

Quelldatentyp	Kompatible Zieldatentypen	Kompatible Swap-Modi	Kompatible Steckerversionen
Int. 16	Ganzzahl, Doppelzahl, Zeichenfolge	Kein Tausch	1 und 2
Int32	Ganzzahl, Doppelzahl, Zeichenfolge	Kein Swap, ByteSwap byteWordSwap, WordSwap	1 und 2
Gleitkommazahl	Doppelt, Schnur	Kein Swap, ByteSwap byteWordSwap, WordSwap	1 und 2
Boolesch	Boolesch	Kein Swap	1 und 2
Hex-Dump	String	Kein Swap	1 und 2

Themen

Konfigurieren Sie eine Modbus-TCP-Quelle (Konsole)

Um eine Modbus-TCP-Quelle zu konfigurieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Gateways aus.
3. Wählen Sie auf dem SiteWise Edge-Gateway, für das Sie eine Quelle erstellen möchten, Verwalten und dann Details anzeigen aus.
4. Wählen Sie rechts oben die Option New source (Neue Quelle) aus.
5. Wählen Sie für Protokolloptionen Modbus TCP aus.
6. Geben Sie für die Modbus-TCP-Quellkonfiguration einen Namen für die Quelle ein.
7. Geben Sie unter IP-Adresse die IP-Adresse für den Datenquellenserver ein.
8. (Optional) Geben Sie den Port und die Einheiten-ID für den Quellserver ein.

9. (Optional) Geben Sie unter Mindestdauer zwischen Anfragen das Zeitintervall zwischen aufeinanderfolgenden Anfragen ein, die an Ihren Server gesendet werden. Ihr SiteWise Edge-Gateway berechnet automatisch das zulässige Mindestintervall auf der Grundlage Ihres Geräts und der Anzahl Ihrer Register.
10. Geben Sie für Eigenschaftsgruppen einen Namen ein.
11. Für Eigenschaften:
    a. Geben Sie unter Tag einen Eigenschaftsalias für Ihren Registersatz ein. z. B. **`TT-001`**.
    b. Geben Sie unter Registeradresse die Registeradresse ein, mit der der Registersatz beginnt.
    c. Wählen Sie als Quelldatentyp den Modbus-TCP-Datentyp aus, aus dem Sie Daten konvertieren möchten. Dies ist standardmäßig Hex-Dump.

       > **Note**
       >
       > Der von Ihnen gewählte Quelldatentyp bestimmt die Datengröße, den Zieldatentyp und den Swap-Modus, den Sie wählen können. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie eine Modbus-TCP-Quelle”.

    d. Geben Sie unter Datengröße die Anzahl der Register ein, die gelesen werden sollen, wenn Sie von der Registeradresse ausgehen. Dies wird durch den Quelldatentyp bestimmt, den Sie für diese Quelle auswählen.
    e. Wählen Sie unter Zieldatentyp den AWS IoT SiteWise Datentyp aus, in den Ihre Daten konvertiert werden sollen. Die Standardeinstellung ist Zeichenfolge. Der Zieltyp muss mit dem Quelldatentyp kompatibel sein, den Sie für diese Quelle auswählen. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie eine Modbus-TCP-Quelle”.
    f. Wählen Sie für den Swap-Modus den Datenaustauschmodus aus, den Sie zum Lesen von Daten aus Ihrem Registersatz verwenden möchten. Der Swap-Modus muss mit dem Quelldatentyp kompatibel sein, den Sie für diese Quelle wählen. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie eine Modbus-TCP-Quelle”.
12. Aktualisieren Sie unter Scanrate die Rate, mit der das SiteWise Edge-Gateway Ihre Register lesen soll. AWS IoT SiteWise berechnet automatisch die minimal zulässige Scanrate für Ihr SiteWise Edge-Gateway.
13. (Optional) Wählen Sie unter Ziel aus, wohin die Quelldaten gesendet werden sollen. Standardmäßig sendet Ihre Quelle Daten an. AWS IoT SiteWise Sie können stattdessen einen

AWS IoT Greengrass Stream verwenden, um Ihre Daten an ein lokales Ziel oder in die AWS Cloud zu exportieren.

> **Note**
>
> Sie müssen AWS IoT SiteWise als Ziel für Ihre Quelldaten auswählen, ob Sie Daten aus dieser Quelle am Edge mit AWS IoT SiteWise verarbeiten möchten. Weitere Informationen zur Verarbeitung von Daten am Edge finden Sie unterthe section called “Aktivierung der Edge-Datenverarbeitung”.

So senden Sie Ihre Daten an ein anderes Ziel:

a. Wählen Sie unter Zieloptionen die Option Andere Ziele aus.

b. Geben Sie als Greengrass-Streamname den genauen Namen Ihres AWS IoT Greengrass Streams ein.

> **Note**
>
> Sie können einen Stream verwenden, den Sie bereits erstellt haben, oder Sie können einen neuen AWS IoT Greengrass Stream erstellen, um Ihre Daten zu exportieren. Wenn Sie einen vorhandenen Stream verwenden möchten, müssen Sie den genauen Namen des Streams eingeben. Andernfalls wird ein neuer Stream erstellt.
> Weitere Informationen zur Arbeit mit AWS IoT Greengrass Streams finden Sie unter Datenstreams verwalten im AWS IoT Greengrass Entwicklerhandbuch.

14. Wählen Sie Add source (Quelle hinzufügen) aus.

    AWS IoT SiteWise stellt die SiteWise Edge-Gateway-Konfiguration auf Ihrem AWS IoT Greengrass Core bereit. Sie müssen eine Bereitstellung nicht manuell starten.

Konfiguration einer Modbus-TCP-Quelle (CLI)

Sie können Modbus-TCP-Datenquellen in einer SiteWise Edge-Gateway-Funktion definieren. Sie müssen alle Ihre Modbus-TCP-Quellen in einer einzigen Funktionskonfiguration definieren.

> **Note**
>
> Sie müssen den AWS IoT SiteWise Connector installieren, um eine Modbus-TCP-Quelle verwenden zu können.

Diese Funktion hat die folgenden Versionen.

Version	Namespace
1	`iotsitewise:modbuscollector:1`

Konfigurationsparameter für die Modbus-TCP-Fähigkeit

Wenn Sie Modbus-TCP-Quellen in einer Funktionskonfiguration definieren, müssen Sie die folgenden Informationen im `capabilityConfiguration` JSON-Dokument angeben:

Quellen

Eine Liste von Modbus-TCP-Quelldefinitionsstrukturen, die jeweils die folgenden Informationen enthalten:

Name

Ein eindeutiger und aussagekräftiger Name für die Quelle.

measurementDataStreamPräfix

(Optional) Eine Zeichenfolge, die allen Datenströmen aus der Quelle vorangestellt wird. Das SiteWise Edge-Gateway fügt dieses Präfix allen Datenströmen aus dieser Quelle hinzu. Verwenden Sie ein Datenstrom-Präfix, um zwischen Datenströmen mit demselben Namen aus verschiedenen Quellen zu unterscheiden. Jeder Datenstrom sollte einen eindeutigen Namen in Ihrem Konto haben.

Ziel

Eine Zielstruktur, die die folgenden Informationen enthält:

Typ

Der Typ des Ziels.

Streamname

Der Name des AWS IoT Greengrass Streams.

streamBufferSize

Die Größe des Stream-Puffers.

Endpunkt

Eine Endpunktstruktur, die die folgenden Informationen enthält:

ipAddress

Die IP-Adresse der Modbus-TCP-Quelle.

port

(Optional) Der Port der Modbus-TCP-Quelle.

UnitID

(Optional) Die UnitID. Dies ist standardmäßig auf den Wert 1 eingestellt.

minimumInterRequestDauer

Die Mindestdauer zwischen den einzelnen Anfragen in Millisekunden.

Eigenschaftengruppen

Die Liste der Eigenschaftsgruppen, die die vom Protokoll angeforderte Tag-Definition definieren.

Name

Der Name der Eigenschaftsgruppe. Dies sollte ein eindeutiger Bezeichner sein.

tagPathDefinitions

Der Ort der Messung innerhalb der Quelle. Zum Beispiel die Byte- und Wortreihenfolge, die Adresse und der Transformationstyp. Die Struktur jedes einzelnen `MeasurementPathDefinition` wird durch den Konnektor definiert.

Scan-Modus

Definiert das Verhalten im Scanmodus und konfigurierbare Parameter für die Quelle.

Konfigurieren Sie eine EtherNet/IP (EIP) -Quelle

Sie können die AWS IoT SiteWise Konsole oder eine SiteWise Edge-Gateway-Funktion verwenden, um eine Ethernet-IP-Quelle zu definieren und Ihrem SiteWise Edge-Gateway hinzuzufügen. Diese Quelle stellt einen lokalen Ethernet-IP-Server dar.

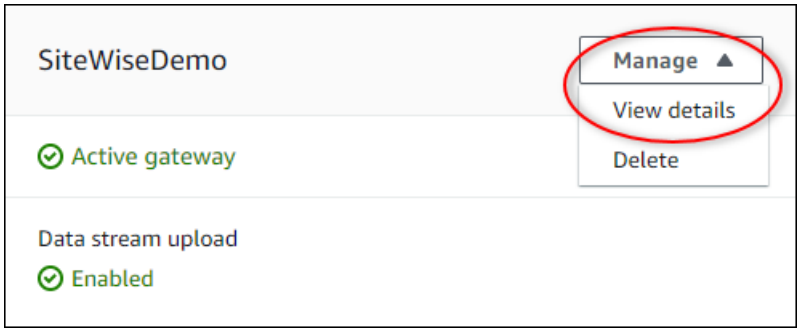
> **Note**
>
> - SiteWise Edge-Gateways, auf denen AWS IoT Greengrass V2 derzeit läuft, unterstützen keine Ethernet-IP-Quellen.
> - Sie müssen den AWS IoT SiteWise Connector installieren, um eine Ethernet-IP-Quelle verwenden zu können.

Themen

Konfigurieren Sie eine EtherNet/IP-Quelle (Konsole)

Um eine EtherNet/IP-Quelle zu konfigurieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Gateways aus.
3. Wählen Sie auf dem SiteWise Edge-Gateway, für das Sie eine Quelle erstellen möchten, Verwalten und dann Details anzeigen aus.



4. Wählen Sie rechts oben die Option New source (Neue Quelle) aus.
5. Wählen Sie für Protokolloptionen EtherNet/IP (EIP).

6. Geben Sie für die EtherNet/IP-Quellkonfiguration einen Namen für die Quelle ein.
7. Geben Sie unter IP-Adresse die IP-Adresse für den Datenquellenserver ein.
8. (Optional) Geben Sie den Port für den Quellserver ein.
9. Geben Sie unter Mindestdauer zwischen Anfragen das Zeitintervall zwischen aufeinanderfolgenden Anfragen ein, die an Ihren Server gesendet werden. Ihr SiteWise Edge-Gateway berechnet automatisch das zulässige Mindestintervall auf der Grundlage Ihres Geräts und der Anzahl Ihrer Register.
10. Geben Sie für Eigenschaftsgruppen einen Namen ein.
11. Für Eigenschaften:

    a. Geben Sie unter Tag den Eigenschaftsalias für Ihren Registersatz ein. z. B. **`boiler.inlet.temperature.value`**.

    b. Wählen Sie unter Zieldatentyp den AWS IoT SiteWise Datentyp aus, in den Ihre Daten konvertiert werden sollen. Die Standardeinstellung ist Zeichenfolge.
12. Aktualisieren Sie unter Scanrate die Rate, mit der das SiteWise Edge-Gateway Ihre Register lesen soll. AWS IoT SiteWise berechnet automatisch die minimal zulässige Scanrate für Ihr SiteWise Edge-Gateway.
13. (Optional) Wählen Sie unter Ziel aus, wohin die Quelldaten gesendet werden sollen. Standardmäßig sendet Ihre Quelle Daten an. AWS IoT SiteWise Sie können stattdessen einen AWS IoT Greengrass Stream verwenden, um Ihre Daten an ein lokales Ziel oder in die AWS Cloud zu exportieren.

    > **Note**
    >
    > Sie müssen AWS IoT SiteWise als Ziel für Ihre Quelldaten auswählen, ob Sie Daten aus dieser Quelle am Edge mit AWS IoT SiteWise verarbeiten möchten. Weitere Informationen zur Verarbeitung von Daten am Edge finden Sie unterthe section called “Aktivierung der Edge-Datenverarbeitung”.

    So senden Sie Ihre Daten an ein anderes Ziel:

    a. Wählen Sie unter Zieloptionen die Option Andere Ziele aus.

    b. Geben Sie als Greengrass-Streamname den genauen Namen Ihres AWS IoT Greengrass Streams ein.

> **Note**
>
> Sie können einen Stream verwenden, den Sie bereits erstellt haben, oder Sie können einen neuen AWS IoT Greengrass Stream erstellen, um Ihre Daten zu exportieren. Wenn Sie einen vorhandenen Stream verwenden möchten, müssen Sie den genauen Namen des Streams eingeben. Andernfalls wird ein neuer Stream erstellt.
> Weitere Informationen zur Arbeit mit AWS IoT Greengrass Streams finden Sie unter Datenstreams verwalten im AWS IoT Greengrass Entwicklerhandbuch.

14. Wählen Sie Add source (Quelle hinzufügen) aus.

    AWS IoT SiteWise stellt die SiteWise Edge-Gateway-Konfiguration auf Ihrem AWS IoT Greengrass Core bereit. Sie müssen eine Bereitstellung nicht manuell starten.

Konfiguration einer EtherNet/IP-Quelle (CLI)

Sie können EIP-Datenquellen in einer SiteWise Edge-Gateway-Funktion definieren. Sie müssen alle Ihre EIP-Quellen in einer einzigen Funktionskonfiguration definieren.

> **Note**
>
> Sie müssen den AWS IoT SiteWise Connector installieren, um eine Ethernet-IP-Quelle verwenden zu können.

Diese Funktion hat die folgenden Versionen.

Version	Namespace
1	`iotsitewise:eipcollector:1`

Konfigurationsparameter für die EIP-Fähigkeit

Wenn Sie EIP-Quellen in einer Capability-Konfiguration definieren, müssen Sie die folgenden Informationen im `capabilityConfiguration` JSON-Dokument angeben:

Quellen

Eine Liste von EIP-Quelldefinitionsstrukturen, die jeweils die folgenden Informationen enthalten:

Name

Ein eindeutiger und aussagekräftiger Name für die Quelle. Dies kann bis zu 256 Zeichen lang sein.

destinationPathPrefix

(Optional) Eine Zeichenfolge, die allen Datenströmen aus der Quelle vorangestellt wird. Das SiteWise Edge-Gateway fügt dieses Präfix allen Datenströmen aus dieser Quelle hinzu. Verwenden Sie ein Datenstrom-Präfix, um zwischen Datenströmen mit demselben Namen aus verschiedenen Quellen zu unterscheiden. Jeder Datenstrom sollte einen eindeutigen Namen in Ihrem Konto haben.

Ziel

Eine Zielstruktur, die die folgenden Informationen enthält:

Typ

Der Typ des Ziels.

Streamname

Der Name des AWS IoT Greengrass Streams.

streamBufferSize

Die Größe des Stream-Puffers.

Endpunkt

Eine Endpunktstruktur, die die folgenden Informationen enthält:

ipAddress

Die IP-Adresse der EIP-Quelle.

port

(Optional) Der Port der EIP-Quelle. Zulässige Werte sind Zahlen zwischen 1 und 65535.

minimumInterRequestDauer

(Optional) Die Mindestdauer zwischen den einzelnen Anfragen in Millisekunden.

Eigenschaftengruppen

Die Liste der Eigenschaftsgruppen, die die vom Protokoll angeforderte Tag-Definition definieren. Jede Quelle kann eine Eigenschaftsgruppe haben.

Name

Der Name der Eigenschaftsgruppe. Dies sollte ein eindeutiger Bezeichner mit einer maximalen Länge von 256 Zeichen sein.

tagPathDefinitions

Die Liste der Strukturen, die die Daten spezifizieren, die vom EtherNet/IP-Gerät gesammelt werden sollen, und wie sie für die Ausgabe transformiert werden sollen.

Typ

Der Typ der `tagPathDefinition`. z. B. `EIPTagPath`.

path

Der Pfad des. `tagPathDefinition` Jedes Tag in einem Pfad kann eine maximale Länge von 40 Zeichen haben und mit einem Buchstaben oder einem Unterstrich beginnen. Tags dürfen keine aufeinanderfolgenden oder nachfolgenden Unterstriche enthalten. Dem Pfad wird ein beliebiger Wert von vorangestellt. destinationPathPrefix

dstDataType

Der Datentyp für die Ausgabe der Tag-Daten. Zulässige Werte sind `integer`double,`string`, und`boolean`.

Scanmodus

Definiert das Verhalten im Scanmodus und konfigurierbare Parameter für die Quelle.

Typ

Der Typ des Verhaltens im Scanmodus. Zulässige Werte sind`POLL`.

bewerten

Die Rate in Millisekunden, mit der der Connector Tags von der EtherNet/IP-Quelle lesen sollte.

Konfigurieren der Quellauthentifizierung

Wenn Ihre OPC-UA-Server Authentifizierungsanmeldeinformationen benötigen, um eine Verbindung herzustellen, können Sie einen Benutzernamen und ein Passwort in einem Secret für jede Quelle in AWS Secrets Manager definieren. Anschließend fügen Sie das Geheimnis zu Ihrer Greengrass-Gruppe und Ihrem SiteWise IoT-Connector hinzu, um das Geheimnis für Ihr SiteWise Edge-Gateway verfügbar zu machen. Weitere Informationen finden Sie unter Deploy Secrets to the AWS IoT Greengrass Core im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

Sobald ein Geheimnis für Ihr SiteWise Edge-Gateway verfügbar ist, können Sie es bei der Konfiguration einer Quelle auswählen. Anschließend verwendet das SiteWise Edge-Gateway die Authentifizierungsdaten aus dem Secret, wenn es eine Verbindung zur Quelle herstellt. Weitere Informationen finden Sie unter Konfigurieren von Datenquellen.

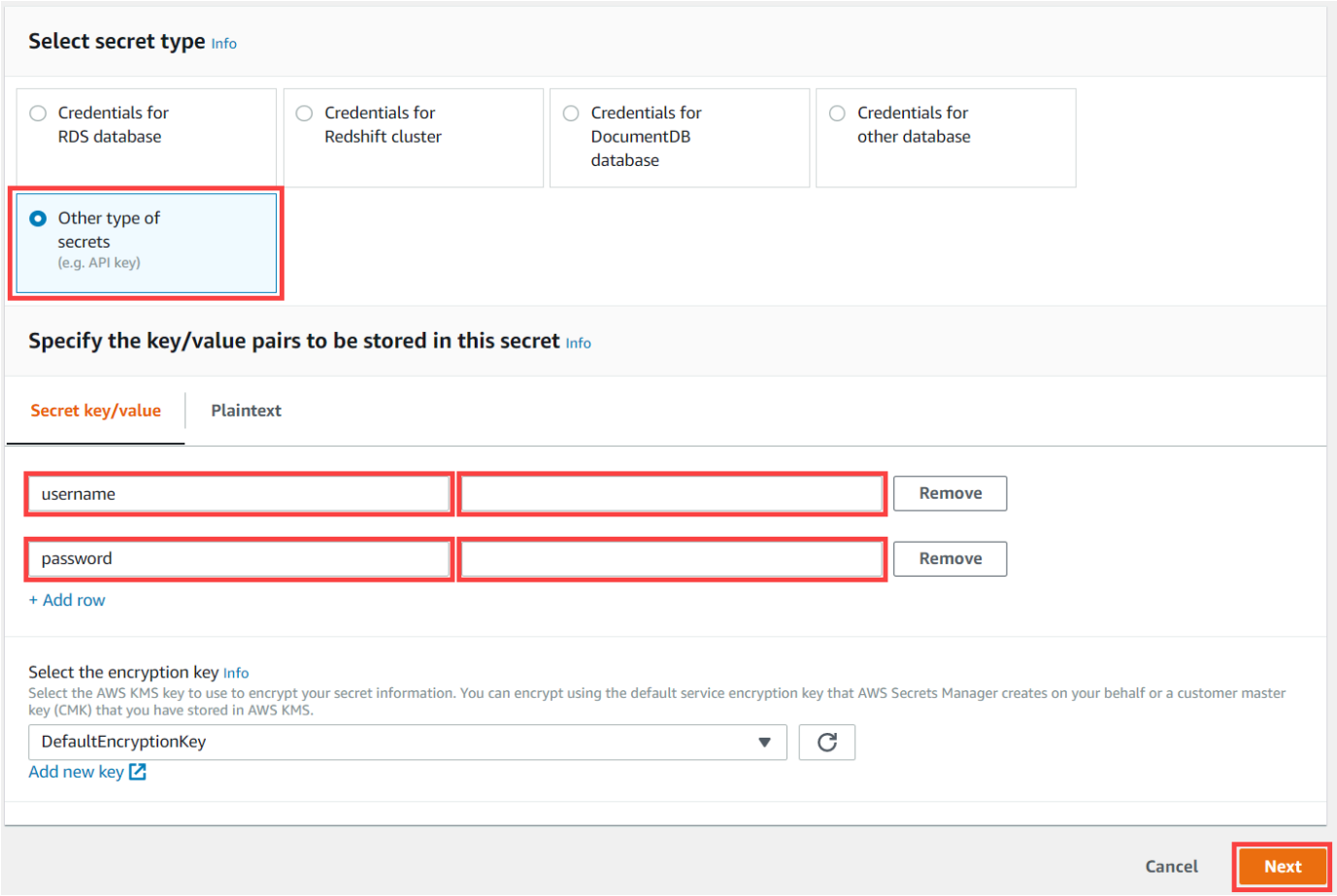
Themen

Erstellen von Secrets für die Quellauthentifizierung

In diesem Verfahren erstellen Sie ein Authentifizierungsgeheimnis für Ihre Quelle in Secrets Manager. Definieren Sie in dem Secret **`username`**- und **`password`**-Schlüssel-Wert-Paare, die Authentifizierungsdetails für Ihre Quelle enthalten.

So erstellen Sie ein Secret zur Quellauthentifizierung

1. Navigieren Sie zur Secrets Manager Manager-Konsole.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Wählen Sie unter Select secret type (Secret-Typ auswählen) die Option Other type of secrets (Anderer Secret-Typ) aus.
4. Geben Sie **`username`**- und **`password`**-Schlüssel-Wert-Paare für die Authentifizierungswerte Ihres OPC-UA-Servers ein und wählen Sie dann Next (Weiter) aus.



5. Geben Sie einen Secret name (Secret-Namen) ein, der mit `greengrass-` beginnt, etwa **`greengrass-factory1-auth`**.

> **Important**
>
> Sie müssen das Präfix `greengrass-` für die Standard-Servicerolle AWS IoT Greengrass verwenden, um auf Ihre Secrets zuzugreifen. Wenn Sie Ihre Geheimnisse ohne dieses Präfix benennen möchten, müssen Sie AWS IoT Greengrass benutzerdefinierte Berechtigungen für den Zugriff auf Ihre Geheimnisse gewähren. Weitere Informationen finden Sie unter Zulassen des AWS IoT Greengrass Abrufs geheimer Werte im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

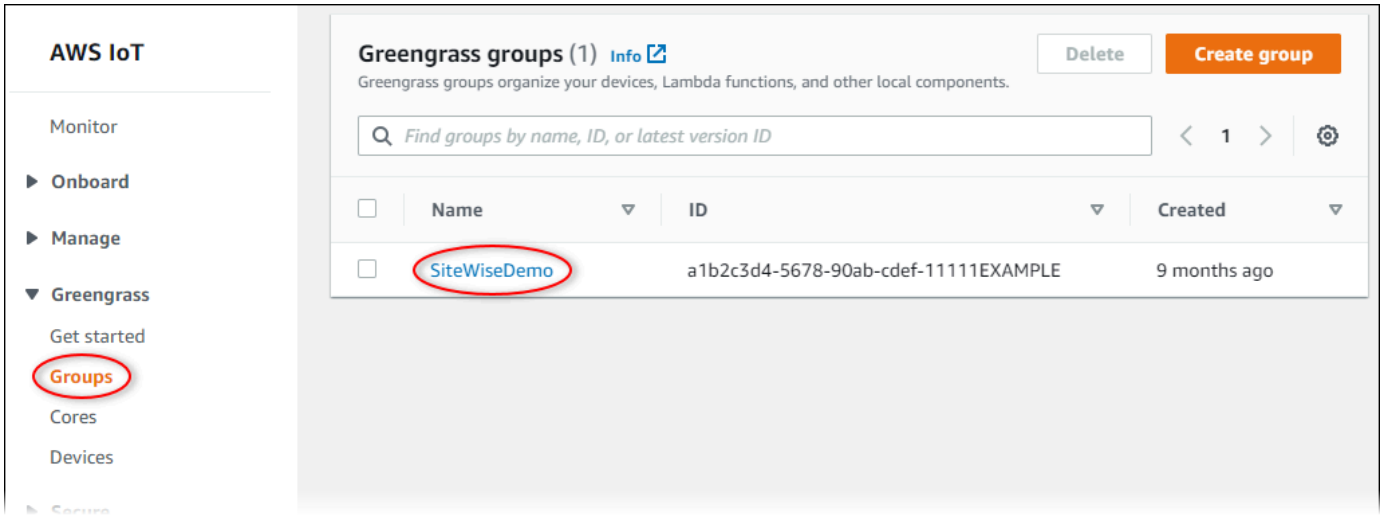
6. Geben Sie eine Description (Beschreibung) ein und wählen Sie Next (Weiter).
7. (Optional) Konfigurieren Sie auf der Seite Configure automatic rotation (Automatische Rotation konfigurieren) die automatische Rotation für Ihre Secrets. Wenn Sie die automatische Rotation konfigurieren, müssen Sie Ihre Greengrass-Gruppe jedes Mal neu bereitstellen, wenn ein Geheimnis rotiert.
8. Wählen Sie auf der Seite Configure automatic rotation (Automatische Rotation konfigurieren) die Option Next (Weiter) aus.
9. Überprüfen Sie das neue Secret und wählen Sie Store (Speichern) aus.

Geheimnisse zu einer Greengrass-Gruppe hinzufügen

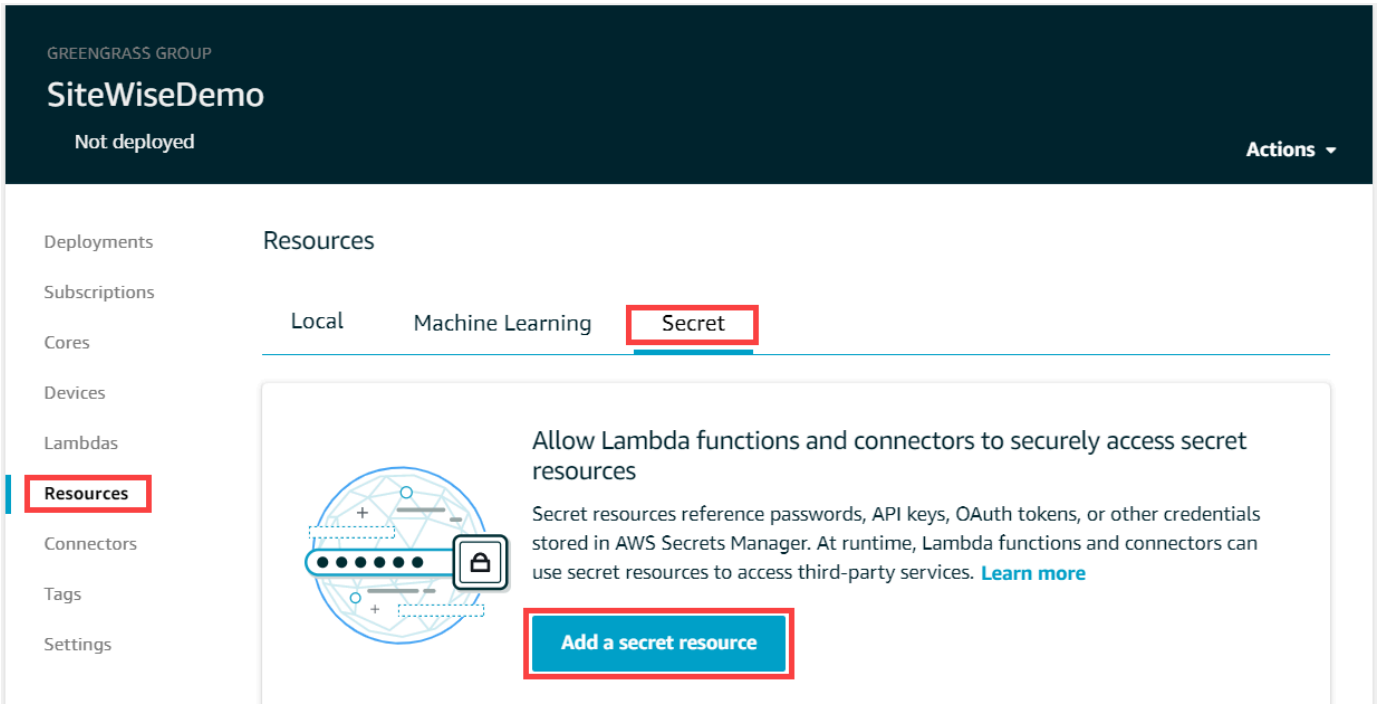
In diesem Verfahren fügen Sie Ihrer AWS IoT Greengrass Gruppe Ihre Quellauthentifizierungsgeheimnisse hinzu, um sie Ihrem SiteWise IoT-Connector zur Verfügung zu stellen.

So fügen Sie Ihrer Greengrass-Gruppe ein Geheimnis hinzu

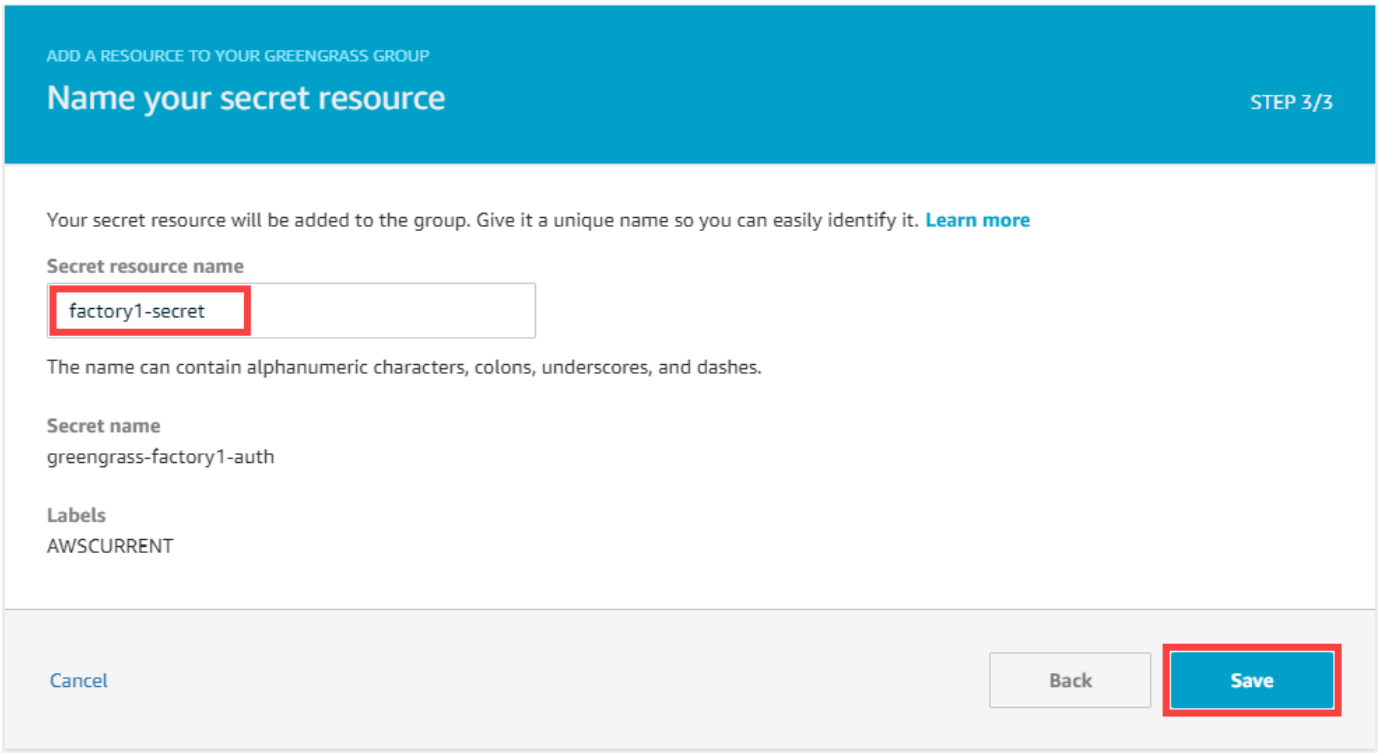
1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im Navigationsbereich unter Greengrass die Option Gruppen und dann Ihre Gruppe aus.



3. Wählen Sie auf der Navigationsseite Ressourcen aus.
4. Wählen Sie auf der Seite Resources (Ressourcen) die Registerkarte Secret (Geheimnis) und dann Add a secret resource (Geheime Ressource hinzufügen) aus.



5. Wählen Sie Select (Auswählen) und anschließend Ihr Secret aus der Liste aus.
6. Wählen Sie Weiter aus.
7. Geben Sie unter Secret Resource name (Name der Secret-Ressource) einen Namen für Ihre Secret-Ressource ein und wählen Sie Save (Speichern) aus.

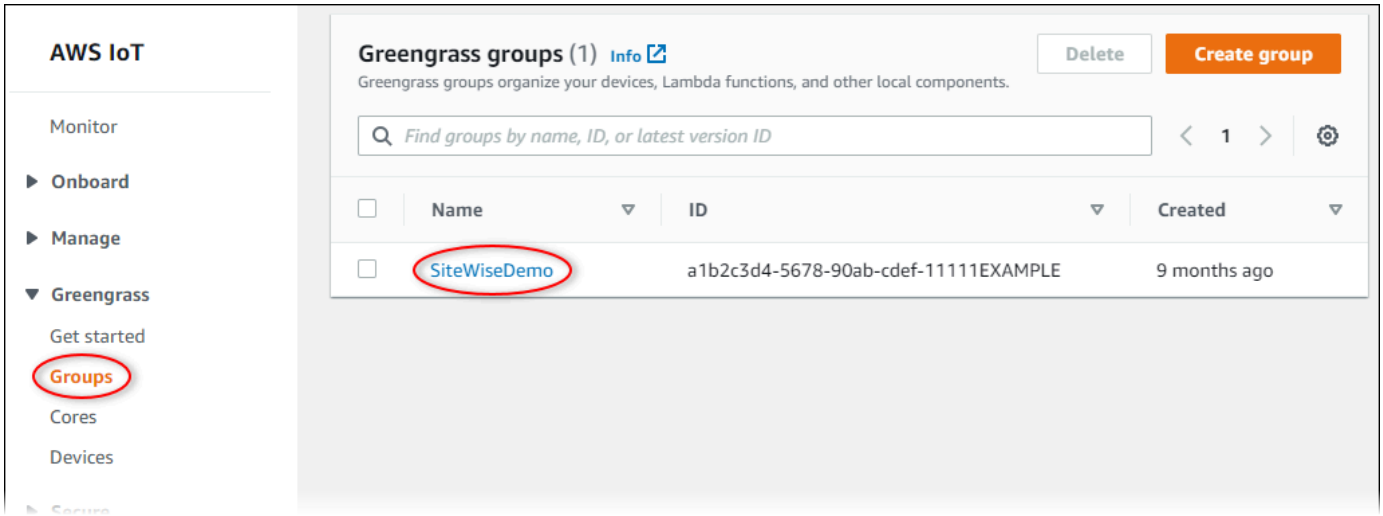


Geheimnisse zu einem SiteWise IoT-Connector hinzufügen

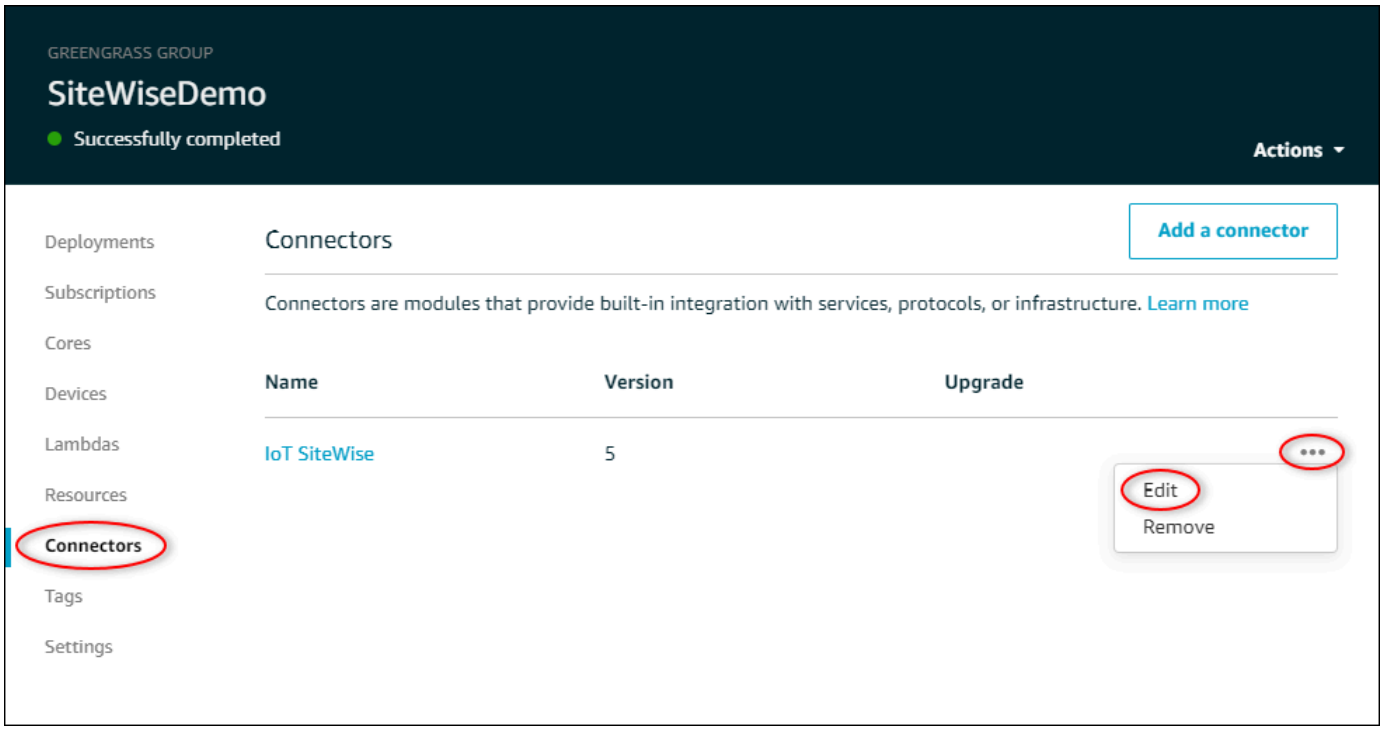
In diesem Verfahren fügen Sie Ihrem SiteWise IoT-Connector Ihre Quellauthentifizierungsgeheimnisse hinzu, um sie für AWS IoT SiteWise und Ihr SiteWise Edge-Gateway verfügbar zu machen.

So fügen Sie Ihrem SiteWise IoT-Connector ein Geheimnis hinzu

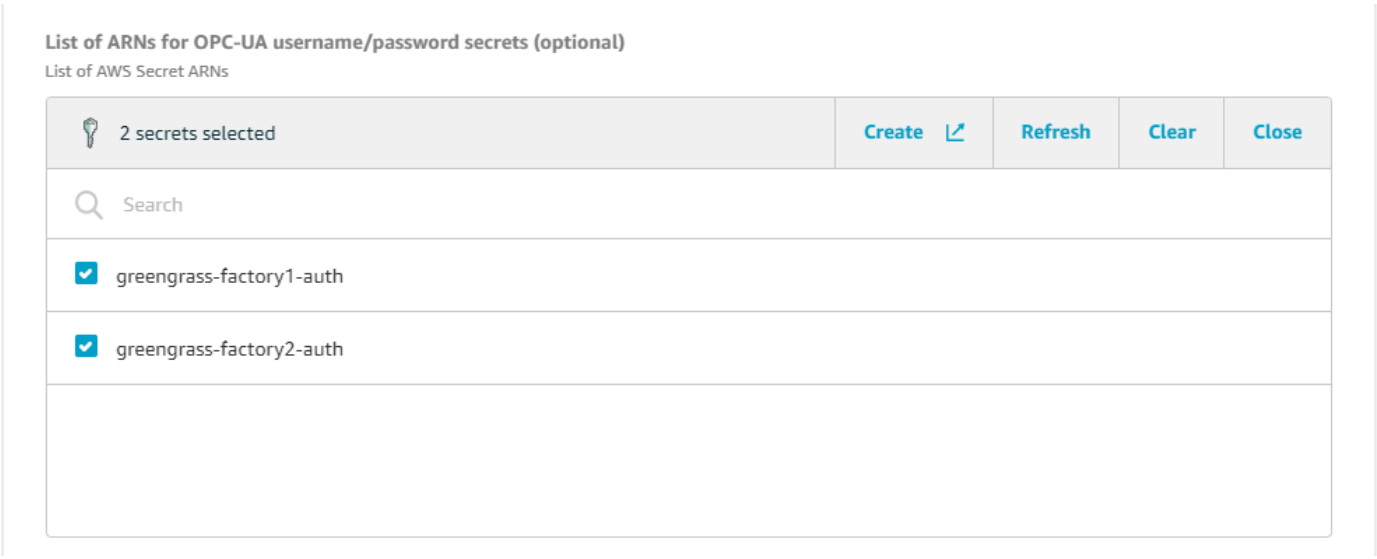
1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im Navigationsbereich unter Greengrass die Option Gruppen und dann Ihre Gruppe aus.



3. Wählen Sie auf der Navigationsseite Connectors aus.
4. Wählen Sie das Ellipsensymbol für den SiteWiseIoT-Connector, um das Optionsmenü zu öffnen, und wählen Sie dann Bearbeiten.



5. Wählen Sie unter Liste der ARNs für OPC-UA-Benutzernamen/Kennwortgeheimnisse die Option Auswählen und wählen Sie dann jedes Geheimnis aus, das zu diesem Edge-Gateway hinzugefügt werden soll. SiteWise Informationen zum Erstellen von Secrets finden Sie unter Erstellen von Secrets für die Quellauthentifizierung.



Wenn Ihr Secret nicht angezeigt wird, wählen Sie Refresh (Aktualisieren). Wenn Ihr Geheimnis immer noch nicht angezeigt wird, überprüfen Sie, ob Sie das Geheimnis zu Ihrer Greengrass-Gruppe hinzugefügt haben.

6. Wählen Sie Speichern.
7. Wählen Sie rechts oben im Menü Actions (Aktionen) die Option Deploy (Bereitstellen) aus.
8. Wählen Sie Automatic detection (Automatische Erkennung) aus, um die Bereitstellung zu starten.

   Wenn die Bereitstellung fehlschlägt, wählen Sie erneut Deploy (Bereitstellen) aus. Wenn die Bereitstellung weiterhin fehlschlägt, finden Sie weitere Informationen im Abschnitt zur Fehlerbehebung für die AWS IoT Greengrass -Bereitstellung.

   Nachdem Ihre Gruppe bereitgestellt wurde, können Sie eine Quelle konfigurieren, die das neue Secret verwendet. Weitere Informationen finden Sie unter Konfigurieren von Datenquellen.

Aktualisieren eines Connectors

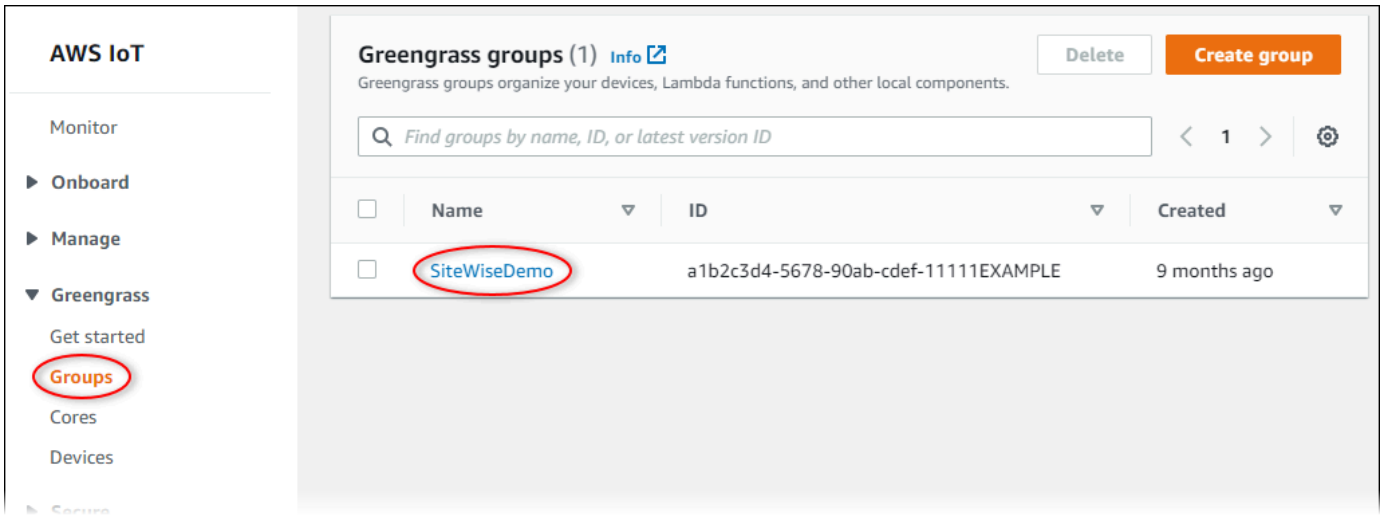
> **Important**
>
> Version 6 des SiteWise IoT-Connectors führt neue Anforderungen ein: AWS IoT Greengrass Kernsoftware v1.10.0 und Stream-Manager. Bevor Sie Ihren Connector aktualisieren, überprüfen Sie, ob Ihr SiteWise Edge-Gateway diese Anforderungen erfüllt. Andernfalls können Sie Ihr SiteWise Edge-Gateway nicht bereitstellen.

Sie können den Connector Ihres SiteWise Edge-Gateways problemlos aktualisieren, nachdem eine neue SiteWise IoT-Connector-Version veröffentlicht wurde.

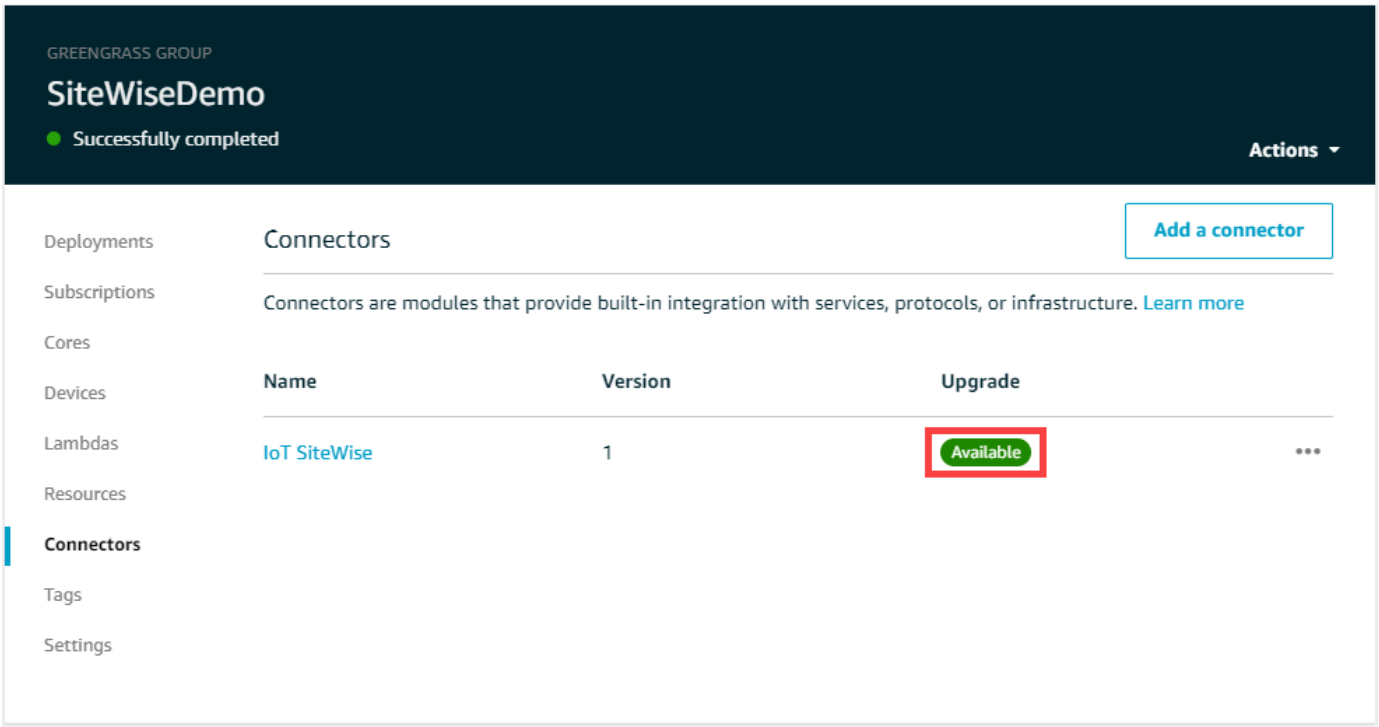
> **Note**
>
> In diesem Verfahren stellen Sie Ihre Greengrass-Gruppe erneut bereit und starten Ihr SiteWise Edge-Gateway neu. Ihr SiteWise Edge-Gateway nimmt während des Neustarts keine Daten auf. Die Zeit für den Neustart Ihres SiteWise Edge-Gateways hängt von der Anzahl der Tags in den Quellen Ihres SiteWise Edge-Gateways ab. Die Neustartzeit kann zwischen einigen Sekunden (für ein SiteWise Edge-Gateway mit wenigen Tags) und mehreren Minuten (für ein SiteWise Edge-Gateway mit vielen Tags) liegen.

Um einen SiteWise IoT-Connector zu aktualisieren

1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im Navigationsbereich unter Greengrass die Option Gruppen und dann die Gruppe aus, die Sie bei der Einrichtung Ihres SiteWise Edge-Gateways erstellt haben.



3. Wählen Sie im Navigationsbereich Connectors aus.
4. Wählen Sie auf der Seite Connectors neben dem SiteWiseIoT-Connector die Option Verfügbar aus.



Wenn das Element Available (Verfügbar) nicht angezeigt wird, ist dies bereits die neueste Version des Connectors.

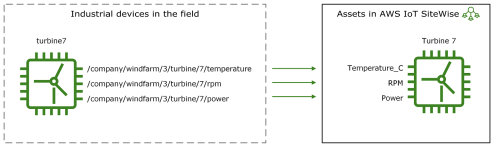
5. Geben Sie auf der Seite Upgrade connector (Connector aktualisieren) die Parameter Ihres Connectors ein und wählen Sie dann Upgrade (Aktualisieren) aus.
6. Wählen Sie rechts oben im Menü Actions (Aktionen) die Option Deploy (Bereitstellen) aus.
7. Wählen Sie Automatic detection (Automatische Erkennung) aus, um die Bereitstellung zu starten.

   Wenn die Bereitstellung fehlschlägt, wählen Sie erneut Deploy (Bereitstellen) aus. Wenn die Bereitstellung weiterhin fehlschlägt, finden Sie weitere Informationen im Abschnitt zur Fehlerbehebung für die AWS IoT Greengrass -Bereitstellung.

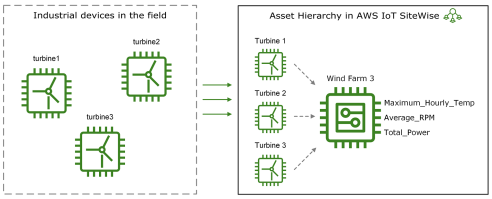
Modellieren von industriellen Komponenten

Sie können virtuelle Repräsentationen Ihres Industriebetriebs mit AWS IoT SiteWise Anlagen erstellen. Ein Asset steht für ein Gerät, eine Ausrüstung oder einen Prozess, der einen oder mehrere Datenströme in den AWS Cloud hochlädt. Ein Komponentengerät kann beispielsweise eine Windturbine sein, die Lufttemperatur, Drehzahl der Propeller und Zeitreihen für die Leistungsausgabe an Komponenteneigenschaften in AWS IoT SiteWise sendet.

Jeder Daten-Stream entspricht einem eindeutigen Alias der Eigenschaft. Beispielsweise dient der Alias `/company/windfarm/3/turbine/7/temperature` zur eindeutigen Identifizierung des Temperaturdaten-Streams von Turbine 7 in Windpark 3. Sie können AWS IoT SiteWise Anlagen so konfigurieren, dass eingehende Messdaten mithilfe mathematischer Ausdrücke transformiert werden, z. B. um Temperaturdaten von Celsius in Fahrenheit umzuwandeln.



Eine Komponente kann auch eine logische Gruppierung von Geräten darstellen, etwa einen gesamten Windpark. Sie können Anlagen mit anderen Anlagen verknüpfen, um Anlagenhierarchien zu erstellen, die komplexe Industriebetriebe repräsentieren. Anlagen können auf die Daten in ihren zugehörigen untergeordneten Anlagen zugreifen. Auf diese Weise können Sie AWS IoT SiteWise Ausdrücke verwenden, um aggregierte Kennzahlen zu berechnen, z. B. die Nettoleistung eines Windparks.



Sie müssen jedes Asset aus einem Asset-Modell erstellen. Komponentenmodelle sind deklarative Strukturen zur Standardisierung des Formats Ihrer Komponenten. Inventarmodelle setzen konsistente Informationen für mehrere Anlagen desselben Typs voraus, sodass Sie Daten in Anlagen verarbeiten können, die Gerätegruppen repräsentieren. Im obigen Diagramm verwenden Sie dasselbe Komponentenmodell für alle drei Turbinen, da alle Turbinen über einen gemeinsamen Satz von Eigenschaften verfügen.

Sie können auch Komponentenmodelle erstellen. Ein Komponentenmodell ist ein besonderer Typ von Anlagenmodell, das Sie in Anlagenmodelle oder andere Komponentenmodelle aufnehmen können. Sie können Komponentenmodelle verwenden, um allgemeine wiederverwendbare Unterbaugruppen wie Sensoren, Motoren usw. zu definieren, die Sie in mehreren Anlagenmodellen gemeinsam verwenden.

Nachdem Sie Ihre Komponentenmodelle definiert haben, können Sie Ihre industriellen Komponenten erstellen. Wählen Sie zum Erstellen einer Komponente ein `ACTIVE`-Komponentenmodell aus, um eine Komponente anhand von diesem Modell zu erstellen. Anschließend können Sie komponentenspezifische Informationen wie Daten-Stream-Aliase und Attribute eintragen. Im obigen Diagramm erstellen Sie drei Turbinenkomponenten von einem Komponentenmodell ausgehend und ordnen dann Daten-Stream-Aliase wie `/company/windfarm/3/turbine/7/temperature` für jede Turbine zu.

Sie können auch vorhandene Objekte, Anlagenmodelle und Komponentenmodelle aktualisieren und löschen. Wenn Sie ein Komponentenmodell aktualisieren, spiegelt jede Komponente, die auf diesem Komponentenmodell basiert, alle Änderungen wider, die Sie am zugrunde liegenden Modell vornehmen. Wenn Sie ein Komponentenmodell aktualisieren, gilt dies für jedes Asset, das auf jedem Asset-Modell basiert, das auf das Komponentenmodell verweist.

Ihre Anlagenmodelle können sehr komplex sein, z. B. wenn Sie ein kompliziertes Gerät mit vielen Unterkomponenten modellieren. Um solche Anlagenmodelle zu organisieren und zu verwalten, können Sie benutzerdefinierte Verbundmodelle verwenden, um zusammengehörige Eigenschaften zu gruppieren oder gemeinsam genutzte Komponenten wiederzuverwenden. Weitere Informationen finden Sie unter Benutzerdefinierte zusammengesetzte Modelle (Komponenten).

Themen

- Aktualisieren von Komponenten und Modellen
- Löschen von Komponenten und Modellen
- Massenoperationen mit Assets und Modellen

Komponenten- und Modellzustände

Wenn Sie ein Asset, ein Assetmodell oder ein Komponentenmodell erstellen, aktualisieren oder löschen, dauert es einige Zeit, bis die Änderungen übernommen werden. AWS IoT SiteWise löst diese Vorgänge asynchron auf und aktualisiert den Status jeder Ressource. Jedes Asset-, Asset- und Komponentenmodell verfügt über ein Statusfeld, das den Status der Ressource und etwaige Fehlermeldungen enthält. Der Zustand kann einer der folgenden Werte sein:

- `ACTIVE`— Die Ressource ist aktiv. Dies ist der einzige Status, in dem Sie Ressourcen, Anlagenmodelle und Komponentenmodelle abfragen und mit ihnen interagieren können.
- `CREATING`— Die Ressource wird gerade erstellt.
- `UPDATING`— Die Ressource wird aktualisiert.
- `DELETING`— Die Ressource wird gelöscht.
- `PROPAGATING`— (nur Asset-Modelle und Komponentenmodelle) Die Änderungen werden auf alle abhängigen Ressourcen übertragen (vom Asset-Modell zu den Assets oder vom Komponentenmodell zu den Asset-Modellen).
- `FAILED`— Die Ressource konnte während eines Erstellungs- oder Aktualisierungsvorgangs nicht validiert werden, möglicherweise aufgrund eines Zirkelverweises in einem Ausdruck. Sie können Ressourcen löschen, die sich im `FAILED` Status befinden.

Bei einigen Vorgängen zum Erstellen, Aktualisieren und Löschen wird ein AWS IoT SiteWise Objekt, ein Anlagenmodell oder ein Komponentenmodell in einen anderen Zustand versetzt, als `ACTIVE` wenn der Vorgang aufgelöst wird. Um eine Ressource abzufragen oder mit ihr zu interagieren, nachdem Sie einen dieser Vorgänge ausgeführt haben, müssen Sie warten, bis sich der Status auf `ACTIVE` ändert. Andernfalls schlagen Ihre Anfragen fehl.

Themen

- Überprüfen des Status einer Komponente
- Überprüfen des Status eines Asset- oder Komponentenmodells

Überprüfen des Status einer Komponente

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um den Status eines Assets zu überprüfen.

Themen

Überprüfen des Status eines Komponente (Konsole)

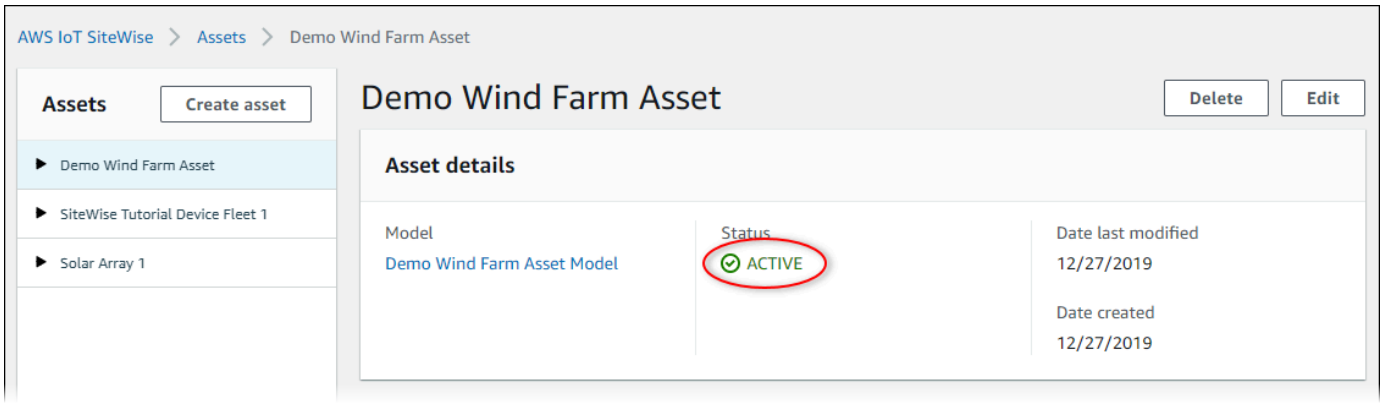
Gehen Sie wie folgt vor, um den Status einer Komponente in der AWS IoT SiteWise -Konsole zu überprüfen.

So überprüfen Sie den Status einer Komponente (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die zu prüfende Komponente aus.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Suchen Sie den Status im Bereich Komponentendetails.



Den Status eines Assets überprüfen (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um den Status eines Assets zu überprüfen.

Um den Status eines Assets zu überprüfen, verwenden Sie die DescribeAssetOperation mit dem `assetId` Parameter.

Um den Status eines Assets zu überprüfen (AWS CLI)

- Verwenden Sie den folgenden Befehl, um die Komponente zu beschreiben. Ersetzen Sie die *`Asset-ID`* durch die ID oder die externe ID des Assets. Die externe ID ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

  ```
  aws iotsitewise describe-asset --asset-id asset-id
  ```

  Die Operation gibt eine Antwort zurück, die Details der Komponente enthält. Die Antwort enthält ein `assetStatus` Objekt mit der folgenden Struktur:

  ```
  {
      ...
      "assetStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  Der Status der Komponente befindet sich in `assetStatus.state` im JSON-Objekt.

Überprüfen des Status eines Asset- oder Komponentenmodells

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um den Status eines Asset- oder Komponentenmodells zu überprüfen.

Themen

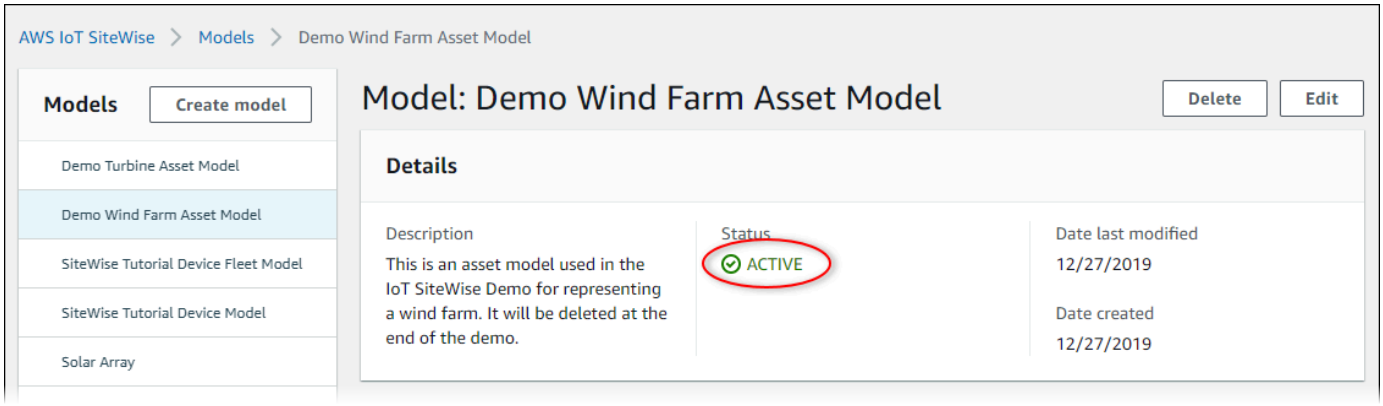
Überprüfen des Status eines Asset- oder Komponentenmodells (Konsole)

Gehen Sie wie folgt vor, um den Status eines Asset- oder Komponentenmodells in der AWS IoT SiteWise Konsole zu überprüfen.

> **Tip**
>
> Objektmodelle und Komponentenmodelle werden beide im Navigationsbereich unter Modelle aufgeführt. Der Bereich „Details“ des ausgewählten Asset- oder Komponentenmodells gibt an, um welchen Typ es sich handelt.

Um den Status eines Asset- oder Komponentenmodells (Konsole) zu überprüfen

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das zu überprüfende Modell aus.
4. Suchen Sie den Status im Bereich Details.



Überprüfen des Status eines Asset- oder Komponentenmodells (AWS CLI)

Sie können das verwenden AWS CLI , um den Status eines Asset- oder Komponentenmodells zu überprüfen.

Um den Status eines Asset- oder Komponentenmodells zu überprüfen, verwenden Sie die DescribeAssetModel-Operation mit dem `assetModelId` Parameter.

> **Tip**
>
> Der AWS CLI definiert Komponentenmodelle als eine Art von Anlagenmodell. Daher verwenden Sie dieselbe DescribeAssetModelloperation für beide Modelltypen. Das `assetModelType` Feld in der Antwort gibt an, ob es sich um ein `ASSET_MODEL` oder ein handelt`COMPONENT_MODEL`.

Um den Status eines Asset- oder Komponentenmodells zu überprüfen (AWS CLI)

- Führen Sie den folgenden Befehl aus, um das Modell zu beschreiben. Ersetzen Sie *`asset-model-id`* durch die ID oder die externe ID des Asset- oder Komponentenmodells. Die externe ID ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

  ```
  aws iotsitewise describe-asset-model --asset-model-id asset-model-id
  ```

  Die Operation gibt eine Antwort zurück, die die Details des Modells enthält. Die Antwort enthält ein `assetModelStatus`-Objekt, das die folgende Struktur aufweist.

  ```
  {
      ...
      "assetModelStatus": {
        "state": "String",
        "error": {
           "code": "String",
           "message": "String"
        }
      }
    }
  ```

  Der Status des Modells befindet sich `assetModelStatus.state` im JSON-Objekt in.

Benutzerdefinierte zusammengesetzte Modelle (Komponenten)

Wenn Sie eine besonders komplexe Industrieanlage modellieren, z. B. eine komplizierte Maschine mit vielen Teilen, kann es zu einer Herausforderung werden, Ihre Anlagenmodelle zu organisieren und zu warten.

In solchen Fällen können Sie Ihren vorhandenen Anlagen- und Komponentenmodellen benutzerdefinierte Verbundmodelle oder Komponenten hinzufügen, wenn Sie die Konsole verwenden. Diese helfen Ihnen, organisiert zu bleiben, indem sie verwandte Eigenschaften gruppieren und Unterkomponentendefinitionen wiederverwenden.

Es gibt zwei Arten von benutzerdefinierten Verbundmodellen:

- Benutzerdefinierte Verbundmodelle definieren eine Reihe von gruppierten Eigenschaften, die für das Asset- oder Komponentenmodell gelten, zu dem das benutzerdefinierte Verbundmodell gehört. Sie verwenden sie, um verwandte Eigenschaften zu gruppieren. Sie bestehen aus einem Namen, einer Beschreibung und einer Reihe von Objektmodelleigenschaften. Sie sind nicht wiederverwendbar.
- Auf Komponentenmodellen basierende benutzerdefinierte Verbundmodelle verweisen auf ein Komponentenmodell, das Sie in Ihr Asset- oder Komponentenmodell aufnehmen möchten. Sie verwenden sie, um Standard-Unterbaugruppen in Ihr Modell aufzunehmen. Sie bestehen aus einem Namen, einer Beschreibung und der ID des Komponentenmodells, auf das sie verweisen. Sie haben keine eigenen Eigenschaften; das referenzierte Komponentenmodell stellt die zugehörigen Eigenschaften allen erstellten Objekten zur Verfügung.

In den folgenden Abschnitten wird veranschaulicht, wie Sie benutzerdefinierte Verbundmodelle in Ihren Entwürfen verwenden können.

Themen

Integrierte benutzerdefinierte Verbundmodelle

Benutzerdefinierte zusammengesetzte Inline-Modelle bieten eine Möglichkeit, Ihr Asset-Modell zu organisieren, indem verwandte Eigenschaften gruppiert werden.

Nehmen wir zum Beispiel an, Sie möchten ein Roboter-Asset modellieren. Der Roboter umfasst einen Servomotor, eine Stromversorgung und eine Batterie. Jeder dieser Bestandteile hat seine eigenen Eigenschaften, die Sie in das Modell aufnehmen möchten. Sie könnten ein Objektmodell mit dem Namen definieren`robot_model`, das Eigenschaften wie die folgenden hat.

- `robot_model`
  - `servo_status` (Ganzzahl)
  - `servo_position` (doppelt)
  - `powersupply_status` (Ganzzahl)
  - `powersupply_temperature` (doppelt)
  - `battery_status` (Ganzzahl)
  - `battery_charge` (doppelt)

In einigen Fällen kann es jedoch viele Unterbaugruppen geben, oder die Unterbaugruppen selbst können viele Eigenschaften haben. In diesen Fällen sind möglicherweise so viele Eigenschaften vorhanden, dass es schwierig wird, sie zu referenzieren und sie in einer einzigen flachen Liste im Modellstamm zu verwalten, wie im vorherigen Beispiel.

Um mit solchen Situationen umzugehen, können Sie ein benutzerdefiniertes Verbundmodell verwenden, um Eigenschaften zu gruppieren. Ein benutzerdefiniertes Verbundmodell ist ein benutzerdefiniertes Verbundmodell, das seine eigenen Eigenschaften definiert. Sie könnten Ihren Roboter beispielsweise wie folgt modellieren.

- `robot_model`
  - `servo`
    - `status`(Ganzzahl)
    - `position`(doppelt)
  - `powersupply`
    - `status`(Ganzzahl)

    - `temperature` (doppelt)
  - `battery`
    - `status`(Ganzzahl)
    - `charge`(doppelt)

Im vorherigen Beispiel `battery` sind `servopowersupply`, und die Namen von benutzerdefinierten Verbundwerkstoffmodellen, die innerhalb des `robot_model` Asset-Modells definiert sind. Jedes dieser zusammengesetzten Modelle definiert dann seine eigenen Eigenschaften.

> **Note**
>
> In diesem Fall definiert jedes benutzerdefinierte Verbundmodell seine eigenen Eigenschaften, sodass alle Eigenschaften Teil des Asset-Modells selbst sind (`robot_model`in diesem Fall). Diese Eigenschaften werden nicht mit anderen Asset- oder Komponentenmodellen gemeinsam genutzt. Wenn Sie beispielsweise ein anderes Asset-Modell erstellt haben, für das auch ein benutzerdefiniertes Inline-Verbundmodell aufgerufen wurde`servo`, `robot_model` hätte eine Änderung an der `servo` Innenseite keinen Einfluss auf die `servo` Definition des anderen Asset-Modells.
> Wenn Sie eine solche gemeinsame Nutzung implementieren möchten (z. B. um nur eine Definition für ein Servo zu haben, die alle Ihre Asset-Modelle gemeinsam nutzen können), würden Sie stattdessen ein Komponentenmodell dafür erstellen und dann komponentenmodellbasierte Verbundmodelle erstellen, die darauf verweisen. Einzelheiten finden Sie im folgenden Abschnitt.

Informationen zum Erstellen benutzerdefinierter Inline-Verbundmodelle finden Sie unterErstellen von benutzerdefinierten Verbundmodellen (Komponenten).

C omponent-model-based benutzerdefinierte Verbundmodelle

Sie können ein Komponentenmodell erstellen, AWS IoT SiteWise um eine wiederverwendbare Standardunterbaugruppe zu definieren. Sobald Sie ein Komponentenmodell erstellt haben, können Sie Referenzen darauf in Ihren anderen Objektmodellen und Komponentenmodellen hinzufügen. Dazu fügen Sie jedem Modell, in dem Sie die Komponente referenzieren möchten, ein component-model-based benutzerdefiniertes Verbundmodell hinzu. Sie können Referenzen aus vielen Modellen oder mehrfach innerhalb desselben Modells zu Ihrer Komponente hinzufügen.

Auf diese Weise können Sie vermeiden, dass dieselben Definitionen modellübergreifend dupliziert werden. Es vereinfacht auch die Verwaltung Ihrer Modelle, da alle Änderungen, die Sie an einem Komponentenmodell vornehmen, in allen Asset-Modellen, die es verwenden, übernommen werden.

Nehmen wir beispielsweise an, dass Ihre Industrieanlage über viele Arten von Geräten verfügt, die alle dieselbe Art von Servomotor verwenden. Einige von ihnen haben viele Servomotoren in einem einzigen Gerät. Sie erstellen für jeden Gerätetyp ein Anlagenmodell, möchten aber nicht `servo` jedes Mal die Definition duplizieren. Sie möchten es nur einmal modellieren und es in Ihren verschiedenen Anlagenmodellen verwenden. Wenn Sie später eine Änderung an der Definition von vornehmen`servo`, wird sie für alle Ihre Modelle und Anlagen aktualisiert.

Um den Roboter aus dem vorherigen Beispiel auf diese Weise zu modellieren, könnten Sie Servomotoren, Stromversorgungen und Batterien wie folgt als Komponentenmodelle definieren.

- `servo_component_model`
  - `status`(Ganzzahl)
  - `position`(doppelt)

- `powersupply_component_model`
  - `status`(Ganzzahl)
  - `temperature` (doppelt)

- `battery__component_model`
  - `status`(Ganzzahl)
  - `charge`(doppelt)

Anschließend könnten Sie Asset-Modelle definieren, die z. `robot_model` B. auf diese Komponenten verweisen. Mehrere Anlagenmodelle können auf dasselbe Komponentenmodell verweisen. Sie können dasselbe Komponentenmodell auch mehrfach in einem Anlagenmodell referenzieren, z. B. wenn Ihr Roboter mehrere Servomotoren enthält.

- `robot_model`

- `servo1`(Referenz:) `servo_component_model`
- `servo2`(Referenz:`servo_component_model`)
- `servo3`(Referenz:`servo_component_model`)
- `powersupply` (Referenz:`powersupply_component_model`)
- `battery`(Referenz:`battery_component_model`)

Informationen zum Erstellen von Komponentenmodellen finden Sie unterKomponentenmodelle erstellen.

Informationen darüber, wie Sie Ihre Komponentenmodelle in anderen Modellen referenzieren können, finden Sie unterErstellen von benutzerdefinierten Verbundmodellen (Komponenten).

Verwenden von Pfaden zum Verweisen auf benutzerdefinierte Eigenschaften von Verbundmodellen

Wenn Sie eine Eigenschaft in einem Objektmodell, Komponentenmodell oder benutzerdefinierten Verbundmodell erstellen, können Sie sie von anderen Eigenschaften aus referenzieren, die ihren Wert verwenden, z. B. Transformationen und Metriken.

AWS IoT SiteWise bietet Ihnen verschiedene Möglichkeiten, auf Ihre Immobilie zu verweisen. Am einfachsten ist es oft, die zugehörige Eigenschafts-ID zu verwenden. Wenn sich die Eigenschaft, auf die Sie verweisen möchten, jedoch in einem benutzerdefinierten Verbundmodell befindet, ist es möglicherweise sinnvoller, sie stattdessen über einen Pfad zu referenzieren.

Ein Pfad ist eine geordnete Abfolge von Pfadsegmenten, die eine Eigenschaft in Bezug auf ihre Position innerhalb der verschachtelten Verbundmodelle innerhalb eines Objektmodells und eines Verbundmodells spezifiziert.

Abrufen von Eigenschaftspfaden

Sie können den Pfad einer Eigenschaft aus dem `path` Feld ihrer AssetModelEigenschaft abrufen.

Nehmen wir beispielsweise an, Sie haben ein Objektmodell`robot_model`, das ein benutzerdefiniertes zusammengesetztes Modell enthält`servo`, das über eine Eigenschaft verfügt`position`. Wenn Sie DescribeAssetModelCompositeModel on aufrufen`servo`, würde die `position` Eigenschaft ein `path` Feld auflisten, das wie folgt aussieht:

```
"path": [
```

```
    {
       "id": "asset model ID",
       "name": "robot_model"
    },
    {
       "id": "composite model ID",
       "name": "servo"
    },
    {
       "id": "property ID",
       "name": "position"
    }
]
```

Eigenschaftspfade verwenden

Sie können einen Eigenschaftenpfad verwenden, wenn Sie eine Eigenschaft definieren, die auf andere Eigenschaften verweist, z. B. eine Transformation oder eine Metrik.

Eine Eigenschaft verwendet eine Variable, um auf eine andere Eigenschaft zu verweisen. Weitere Hinweise zum Arbeiten mit Variablen finden Sie unterVerwenden von Variablen in Formelausdrücken.

Wenn Sie eine Variable definieren, die auf eine Eigenschaft verweist, können Sie entweder die ID der Eigenschaft oder ihren Pfad verwenden.

Um eine Variable zu definieren, die den Pfad der referenzierten Eigenschaft verwendet, geben Sie das `propertyPath` Feld ihres Werts an.

Um beispielsweise ein Asset-Modell mit einer Metrik zu definieren, die mithilfe eines Pfads auf eine Eigenschaft verweist, könnten Sie CreateAssetModel eine Payload wie die folgende übergeben:

```
{
    ...
    "assetModelProperties": [
        {
            ...
            "type": {
                "metric": {
                    ...
                    "variables": [
                        {
                            "name": "variable name",
                            "value": {
```

```
                            "propertyPath": [
                                path segments
                            ]
                        }
                    }
                ],
                ...
            }
        },
        ...
    },
    ...
],
...
}
```

Mit Objekt-IDs arbeiten

AWS IoT SiteWise definiert verschiedene Typen persistenter Objekte, wie z. B. Objekte, Objektmodelle, Eigenschaften und Hierarchien. All diese Objekte verfügen über eindeutige Kennungen, mit denen Sie sie abrufen, aktualisieren und löschen können.

AWS IoT SiteWise bietet Kunden verschiedene Optionen für die ID-Erstellung. AWS IoT SiteWise generiert standardmäßig eine für Sie zum Zeitpunkt der Objekterstellung. Benutzer können Ihren Objekten auch ihre eigenen IDs zuweisen.

Themen

Mit Objekt-UUIDs arbeiten

Jedes persistente Objekt AWS IoT SiteWise hat eine UUID, um es zu identifizieren. Asset-Modelle haben beispielsweise eine Asset-Modell-ID, Assets haben eine Asset-ID und so weiter. Diese ID wird bei der Erstellung des Objekts zugewiesen und bleibt während der gesamten Lebensdauer des Objekts unverändert.

Wenn Sie ein neues Objekt erstellen, AWS IoT SiteWise generiert standardmäßig eine eindeutige ID für Sie. Sie können bei der Erstellung auch Ihre eigene ID im UUID-Format angeben.

> **Note**
>
> UUIDs müssen innerhalb der AWS Region, in der sie erstellt wurden, und für denselben Objekttyp global eindeutig sein. Wenn AWS IoT SiteWise automatisch eine ID für Sie generiert wird, ist sie immer einzigartig. Wenn Sie Ihre eigene ID wählen, stellen Sie sicher, dass sie eindeutig ist.

Wenn Sie beispielsweise ein neues Asset-Modell erstellen, indem Sie CreateAssetModel aufrufen, können Sie Ihre eigene UUID in das optionale `assetModelId` Feld der Anfrage eingeben.

Wenn Sie dagegen in der Anfrage etwas weglassen, wird `assetModelId` eine UUID für das neue Asset-Modell AWS IoT SiteWise generiert.

Verwendung externer IDs

Um Ihre eigene ID in einem anderen Format als UUID zu definieren, können Sie eine externe ID zuweisen. Sie können dies beispielsweise tun, wenn Sie eine ID, die Sie verwenden, in einem System wiederverwenden, das dies nicht ist AWS, oder um sie für Menschen lesbarer zu machen. Externe IDs haben ein flexibleres Format. Sie können sie verwenden, um bei AWS IoT SiteWise API-Vorgängen auf Ihre Objekte zu verweisen, bei denen Sie sonst die UUID verwenden würden.

Wie bei den UUIDs muss jede externe ID in ihrem Kontext eindeutig sein. Sie können beispielsweise nicht zwei Asset-Modelle mit derselben externen ID haben. Ebenso wie die UUIDs kann ein Objekt während seiner Lebensdauer nur eine externe ID haben, die sich nicht ändern kann.

Unterschiede zwischen externen IDs und UUIDs

Externe IDs unterscheiden sich in folgenden Punkten von UUIDs:

- Jedes Objekt hat eine UUID, externe IDs sind jedoch optional.
- AWS IoT SiteWise generiert niemals externe IDs. Sie stellen diese selbst zur Verfügung.
- Falls das Objekt noch keine hat, können Sie jederzeit eine externe ID vergeben.

Format der externen IDs

Eine gültige externe ID hat die folgenden Eigenschaften:

- Ist zwischen 2 und 128 Zeichen lang.
- Das erste und das letzte Zeichen müssen alphanumerisch sein (A-Z, a-z, 0-9).
- Andere Zeichen als das erste und das letzte müssen entweder alphanumerisch oder eines der folgenden Zeichen sein: `_-.:`

Eine externe ID muss beispielsweise dem folgenden regulären Ausdruck entsprechen:

```
[a-zA-Z0-9][a-zA-Z0-9_\-.:]*[a-zA-Z0-9]+
```

Objekte mit externen IDs referenzieren

An vielen Stellen, an denen Sie mithilfe seiner UUID auf ein Objekt verweisen könnten, können Sie stattdessen dessen externe ID verwenden, falls es eine hat. Hängen Sie dazu die externe ID an die Zeichenfolge an. `externalId:`

Nehmen wir beispielsweise an, Sie haben ein Asset-Modell, dessen UUID (Asset Model ID) lautet`a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`, das auch die externe ID enthält. `myExternalId` Rufen Sie DescribeAssetModel auf, um weitere Informationen zu erhalten. Sie könnten einen der folgenden Werte als Wert für verwenden`assetModelId`:

- Mit der Asset Model ID (UUID) selbst: `a1b2c3d4-5678-90ab-cdef-11111EXAMPLE`
- Mit der externen ID: `externalId:myExternalId`

```
aws iotsitewise describe-asset-model --asset-model-id a1b2c3d4-5678-90ab-
cdef-11111EXAMPLE
aws iotsitewise describe-asset-model --asset-model-id externalId:myExternalId
```

> **Note**
>
> Das `externalId:` Präfix selbst ist nicht Teil der externen ID. Sie müssen das Präfix nur angeben, wenn Sie eine externe ID für einen API-Vorgang angeben, der entweder UUIDs oder externe IDs akzeptiert. Geben Sie beispielsweise das Präfix an, wenn Sie ein vorhandenes Objekt abfragen oder aktualisieren.
> Wenn Sie eine externe ID für ein Objekt definieren, z. B. wenn Sie ein Asset-Modell erstellen, geben Sie das Präfix nicht an.

Auf diese Weise können Sie externe IDs anstelle von UUIDs für viele API-Operationen verwenden AWS IoT SiteWise, aber nicht für alle. Beispielsweise muss der GetAssetPropertyValueUUIDs verwenden; die Verwendung externer IDs wird nicht unterstützt.

Informationen darüber, ob ein bestimmter API-Vorgang diese Verwendung unterstützt, finden Sie in der API-Referenz.

Erstellung von Asset- und Komponentenmodellen

AWS IoT SiteWise Anlagenmodelle und Komponentenmodelle fördern die Standardisierung Ihrer Industriedaten. Ein Anlagenmodell oder Komponentenmodell enthält einen Namen, eine Beschreibung, Anlageneigenschaften und (optional) benutzerdefinierte Verbundmodelle, die Eigenschaften gruppieren oder auf Komponentenmodelle für Unterbaugruppen verweisen.

- Sie verwenden ein Objektmodell, um Objekte zu erstellen. Zusätzlich zu den oben aufgeführten Funktionen kann ein Anlagenmodell auch Hierarchiedefinitionen enthalten, die Beziehungen zwischen Anlagen definieren.
- Ein Komponentenmodell stellt eine Unterbaugruppe innerhalb eines Anlagenmodells oder eines anderen Komponentenmodells dar. Wenn Sie ein Komponentenmodell erstellen, können Sie Referenzen darauf in Objektmodellen und anderen Komponentenmodellen hinzufügen. Sie können Objekte jedoch nicht direkt aus Komponentenmodellen erstellen.

Nachdem Sie ein Objekt- oder Komponentenmodell erstellt haben, können Sie benutzerdefinierte Verbundmodelle erstellen, um Eigenschaften zu gruppieren oder auf vorhandene Komponentenmodelle zu verweisen.

Einzelheiten zum Erstellen von Asset- und Komponentenmodellen finden Sie in den folgenden Abschnitten.

Themen

Erstellen von Komponentenmodellen

AWS IoT SiteWise Anlagenmodelle treiben die Standardisierung Ihrer Industriedaten voran. Ein Komponentenmodell enthält einen Namen, eine Beschreibung, Komponenteneigenschaften und Definitionen der Komponentenhierarchie. Sie können beispielsweise ein Windturbinenmodell mit Temperatur, Umdrehungen pro Minute (RPM) und Leistungseigenschaften definieren. Anschließend können Sie ein Windparkmodell mit einer Nettoleistungseigenschaft und einer Windturbinenhierarchiedefinition definieren.

> **Note**
>
> - Es empfiehlt sich, bei der Modellierung mit den Knoten der untersten Ebene zu beginnen. Erstellen Sie das Windturbinenmodell beispielsweise vor dem Windparkmodell. Komponentenhierarchiedefinitionen enthalten Verweise auf vorhandene Komponentenmodelle. Wenn Sie diesen Ansatz verfolgen, können Sie Komponentenhierarchien bei der Modellerstellung definieren.
> - Anlagenmodelle können keine anderen Anlagenmodelle enthalten. Wenn Sie ein Modell definieren müssen, das Sie als Unterbaugruppe in einem anderen Modell referenzieren können, sollten Sie stattdessen ein Komponenten--> Modell erstellen. Weitere Informationen finden Sie unter Komponentenmodelle erstellen.

In den folgenden Abschnitten wird beschrieben, wie Sie die AWS IoT SiteWise Konsole oder API verwenden, um Objektmodelle zu erstellen. In den folgenden Abschnitten werden auch die verschiedenen Arten von Komponenteneigenschaften und Komponentenhierarchien beschrieben, die Sie zum Erstellen von Modellen verwenden können.

Themen

Erstellen eines Komponentenmodells (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um ein Asset-Modell zu erstellen. Die AWS IoT SiteWise Konsole bietet verschiedene Funktionen, z. B. die auto Vervollständigung von Formeln, mit denen Sie gültige Anlagenmodelle definieren können.

So erstellen Sie ein Komponentenmodell (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie Modell erstellen aus.
4. Gehen Sie auf der Seite Modell erstellen wie folgt vor:

    a. Geben Sie unter Name einen Namen für das Komponentenmodell ein, z. B. **`Wind Turbine`** oder **`Wind Turbine Model`**. Dieser Name muss für alle Modelle in Ihrem Konto in dieser Region eindeutig sein.

    b. (Optional) Fügen Sie eine externe ID für das Modell hinzu. Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

    c. (Optional) Fügen Sie Messungsdefinitionen für das Modell hinzu. Messungen stellen Datenströme von Ihren Geräten dar. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).

    d. (Optional) Fügen Sie Transformationsdefinitionen für das Modell hinzu. Transformationen sind Formeln, die Daten von einem Formular auf ein anderes abbilden. Weitere Informationen finden Sie unter Daten transformieren (transformiert).

    e. (Optional) Fügen Sie Metrik-Definitionen für das Modell hinzu. Metriken sind Formeln, die Daten über Zeitintervalle aggregieren. Mit Metriken können Daten aus zugehörigen Anlagen eingegeben werden, sodass Sie Werte berechnen können, die Ihren Betrieb oder einen Teil Ihres Betriebs repräsentieren. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

    f. (Optional) Fügen Sie Hierarchiedefinitionen für das Modell hinzu. Hierarchien sind Beziehungen zwischen Anlagen. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.

    g. (Optional) Fügen Sie Tags für das Komponentenmodell hinzu. Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.

    h. Wählen Sie Modell erstellen aus.

Wenn Sie ein Asset-Modell erstellen, navigiert die AWS IoT SiteWise Konsole zur Seite des neuen Modells. Auf dieser Seite sehen Sie den Status, des Modells, der anfänglich WIRD ERSTELLT lautet. Diese Seite wird automatisch aktualisiert. Sie können daher einfach abwarten, bis der Status des Modells aktualisiert wird.

> **Note**
>
> Das Erstellen von Komponentenmodellen kann für komplexe Modelle einige Minuten in Anspruch nehmen. Wenn der Status des Asset-Modells AKTIV ist, können Sie das Asset-Modell verwenden, um Assets zu erstellen. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

5. (Optional) Nachdem Sie Ihr Asset-Modell erstellt haben, können Sie Ihr Asset-Modell für den Edge konfigurieren. Weitere Informationen zu SiteWise Edge finden Sie unterAktivierung der Edge-Datenverarbeitung.

   a. Wählen Sie auf der Modellseite Configure for Edge aus.

   b. Wählen Sie auf der Seite mit der Modellkonfiguration die Edge-Konfiguration für Ihr Modell aus. Dadurch wird gesteuert, AWS IoT SiteWise wo die mit diesem Asset-Modell verknüpften Eigenschaften berechnet und gespeichert werden können. Weitere Informationen zur Konfiguration Ihres Modells für den Edge finden Sie unterthe section called “Edge-Fähigkeit einrichten”.

   c. Wählen Sie für die benutzerdefinierte Kantenkonfiguration den Standort aus, AWS IoT SiteWise an dem Sie die einzelnen Eigenschaften Ihres Asset-Modells berechnen und speichern möchten.

      > **Note**
      >
      > Die zugehörigen Transformationen und Metriken müssen für denselben Standort konfiguriert werden. Weitere Informationen zur Konfiguration Ihres Modells für den Edge finden Sie unterthe section called “Edge-Fähigkeit einrichten”.

   d. Wählen Sie Speichern. Auf der Modellseite sollte Ihre Edge-Konfiguration jetzt konfiguriert sein.

Ein Asset-Modell erstellen (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein Asset-Modell zu erstellen.

Verwenden Sie die CreateAssetModel-Operation, um ein Asset-Modell mit Eigenschaften und Hierarchien zu erstellen. Diese Operation erwartet eine Nutzlast mit der folgenden Struktur.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition
}
```

Um ein Asset-Modell zu erstellen ()AWS CLI

1. Erstellen Sie eine Datei namens `asset-model-payload.json` und kopieren Sie dann das folgende JSON-Objekt in die Datei.

   ```
   {
     "assetModelType": "ASSET_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ],
     "assetModelHierarchies": [

     ],
     "assetModelCompositeModels": [

     ]
   }
   ```

2. Verwenden Sie Ihren bevorzugten JSON-Texteditor, um die Datei `asset-model-payload.json` für Folgendes zu bearbeiten:

   a. Geben Sie einen Namen (`assetModelName`) für das Komponentenmodell ein, z. B. **`Wind Turbine`** oder **`Wind Turbine Model`**. Dieser Name muss in diesem Fall für alle Asset- und Komponentenmodelle in Ihrem Konto eindeutig sein AWS-Region.

b. (Optional) Geben Sie eine externe ID (`assetModelExternalId`) für das Asset-Modell ein. Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

c. (Optional) Geben Sie eine Beschreibung (`assetModelDescription`) für das Komponentenmodell ein oder entfernen Sie das `assetModelDescription`-Schlüssel-Wert-Paar.

d. (Optional) Definieren Sie Komponenteneigenschaften (`assetModelProperties`) für das Modell. Weitere Informationen finden Sie unter Definieren von Dateneigenschaften.

e. (Optional) Definieren Sie Komponentenhierarchien (`assetModelHierarchies`) für das Modell. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.

f. (Optional) Definieren Sie Alarme für das Modell. Alarme überwachen andere Eigenschaften, sodass Sie erkennen können, wann Geräte oder Prozesse besondere Aufmerksamkeit erfordern. Jede Alarmdefinition ist ein zusammengesetztes Modell (`assetModelCompositeModels`), das die vom Alarm verwendeten Eigenschaften standardisiert. Weitere Informationen finden Sie unter Daten mit Alarmen überwachen und Definition von Alarmen für Anlagenmodelle.

g. (Optional) Fügen Sie Tags (`tags`) für das Komponentenmodell hinzu. Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.

3. Führen Sie den folgenden Befehl aus, um aus der Definition in der JSON-Datei ein Komponentenmodell zu erstellen.

```
aws iotsitewise create-asset-model --cli-input-json file://asset-model-payload.json
```

Die Operation gibt eine Antwort zurück, die die `assetModelId` enthält, auf die Sie beim Erstellen einer Komponente verweisen. Die Antwort enthält auch den Zustand des Modells (`assetModelStatus.state`), der anfänglich `CREATING` lautet. Der Status des Komponentenmodells ist `CREATING`, bis die Änderungen weitergegeben werden.

> **Note**
>
> Das Erstellen von Komponentenmodellen kann für komplexe Modelle einige Minuten in Anspruch nehmen. Um den aktuellen Status Ihres Anlagenmodells zu überprüfen, verwenden Sie die Operation DescribeAssetModell, indem Sie die `assetModelId` angeben. Wenn der Status des Komponentenmodells „`ACTIVE`“ lautet, können mit dem

Komponentenmodell Komponenten erstellen. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

4. (Optional) Erstellen Sie benutzerdefinierte Verbundmodelle für Ihr Anlagenmodell. Mit benutzerdefinierten Verbundmodellen können Sie Eigenschaften innerhalb des Modells gruppieren oder eine Unterbaugruppe einbeziehen, indem Sie auf ein Komponentenmodell verweisen. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Verbundmodellen (Komponenten).

Beispiel für Komponentenmodelle

Dieser Abschnitt enthält Beispieldefinitionen für Objektmodelle, die Sie verwenden können, um Objektmodelle mit den SDKs AWS CLI und AWS IoT SiteWise zu erstellen. Diese Anlagenmodelle stellen eine Windturbine und einen Windpark dar. Windkraftanlagen nehmen Sensorrohdaten auf und berechnen Werte wie Leistung und durchschnittliche Windgeschwindigkeit. Windparkanlagen berechnen Werte wie die Gesamtleistung aller Windturbinen im Windpark.

Themen

- Windturbinen-Komponentenmodell
- Windpark-Komponentenmodell

Windturbinen-Komponentenmodell

Das folgende Komponentenmodell stellt eine Turbine in einem Windpark dar. Die Windturbine nimmt Sensordaten auf, um Werte wie Leistung und durchschnittliche Windgeschwindigkeit zu berechnen.

> **Note**
>
> Dieses Beispielmodell ähnelt dem Windturbinenmodell aus der AWS IoT SiteWise Demo. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo verwenden.

```
{
  "assetModelType": "ASSET_MODEL",
  "assetModelName": "Wind Turbine Asset Model",
  "assetModelDescription": "Represents a turbine in a wind farm.",
  "assetModelProperties": [
    {
```

```
      "name": "Location",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Renton"
        }
      }
    },
    {
      "name": "Make",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Amazon"
        }
      }
    },
    {
      "name": "Model",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "500"
        }
      }
    },
    {
      "name": "Torque (KiloNewton Meter)",
      "dataType": "DOUBLE",
      "unit": "kNm",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Wind Direction",
      "dataType": "DOUBLE",
      "unit": "Degrees",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "RotationsPerMinute",
```

```
      "dataType": "DOUBLE",
      "unit": "RPM",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Wind Speed",
      "dataType": "DOUBLE",
      "unit": "m/s",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "RotationsPerSecond",
      "dataType": "DOUBLE",
      "unit": "RPS",
      "type": {
        "transform": {
          "expression": "rpm / 60",
          "variables": [
            {
              "name": "rpm",
              "value": {
                "propertyId": "RotationsPerMinute"
              }
            }
          ]
        }
      }
    },
    {
      "name": "Overdrive State",
      "dataType": "DOUBLE",
      "type": {
        "transform": {
          "expression": "gte(torque, 3)",
          "variables": [
            {
              "name": "torque",
              "value": {
                "propertyId": "Torque (KiloNewton Meter)"
              }
```

```
          }
        ]
      }
    }
  },
  {
    "name": "Average Power",
    "dataType": "DOUBLE",
    "unit": "Watts",
    "type": {
      "metric": {
        "expression": "avg(torque) * avg(rps) * 2 * 3.14",
        "variables": [
          {
            "name": "torque",
            "value": {
              "propertyId": "Torque (Newton Meter)"
            }
          },
          {
            "name": "rps",
            "value": {
              "propertyId": "RotationsPerSecond"
            }
          }
        ],
        "window": {
          "tumbling": {
            "interval": "5m"
          }
        }
      }
    }
  },
  {
    "name": "Average Wind Speed",
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "metric": {
        "expression": "avg(windspeed)",
        "variables": [
          {
            "name": "windspeed",
```

```
            "value": {
              "propertyId": "Wind Speed"
            }
          }
        ],
        "window": {
          "tumbling": {
            "interval": "5m"
          }
        }
      }
    }
  },
  {
    "name": "Torque (Newton Meter)",
    "dataType": "DOUBLE",
    "unit": "Nm",
    "type": {
      "transform": {
        "expression": "knm * 1000",
        "variables": [
          {
            "name": "knm",
            "value": {
              "propertyId": "Torque (KiloNewton Meter)"
            }
          }
        ]
      }
    }
  },
  {
    "name": "Overdrive State Time",
    "dataType": "DOUBLE",
    "unit": "Seconds",
    "type": {
      "metric": {
        "expression": "statetime(overdrive_state)",
        "variables": [
          {
            "name": "overdrive_state",
            "value": {
              "propertyId": "Overdrive State"
            }
```

```
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
    }
  ],
  "assetModelHierarchies": []
}
```

Windpark-Komponentenmodell

Das folgende Komponentenmodell stellt einen Windpark dar, der aus mehreren Windturbinen besteht. Dieses Anlagenmodell definiert eine Hierarchie für das Windturbinenmodell. Auf diese Weise kann der Windpark Werte (z. B. die Durchschnittsleistung) anhand von Daten für alle Windturbinen im Windpark berechnen.

> **Note**
>
> Dieses Beispielmodell ähnelt dem Windparkmodell aus der AWS IoT SiteWise Demo. Weitere Informationen finden Sie unter Die AWS IoT SiteWise Demo verwenden.

Dieses Komponentenmodell hängt von der Windturbinen-Komponentenmodell ab. Ersetzen Sie die Werte `propertyId` und `childAssetModelId` durch die Werte eines vorhandenen Komponentenmodells für Windturbinen.

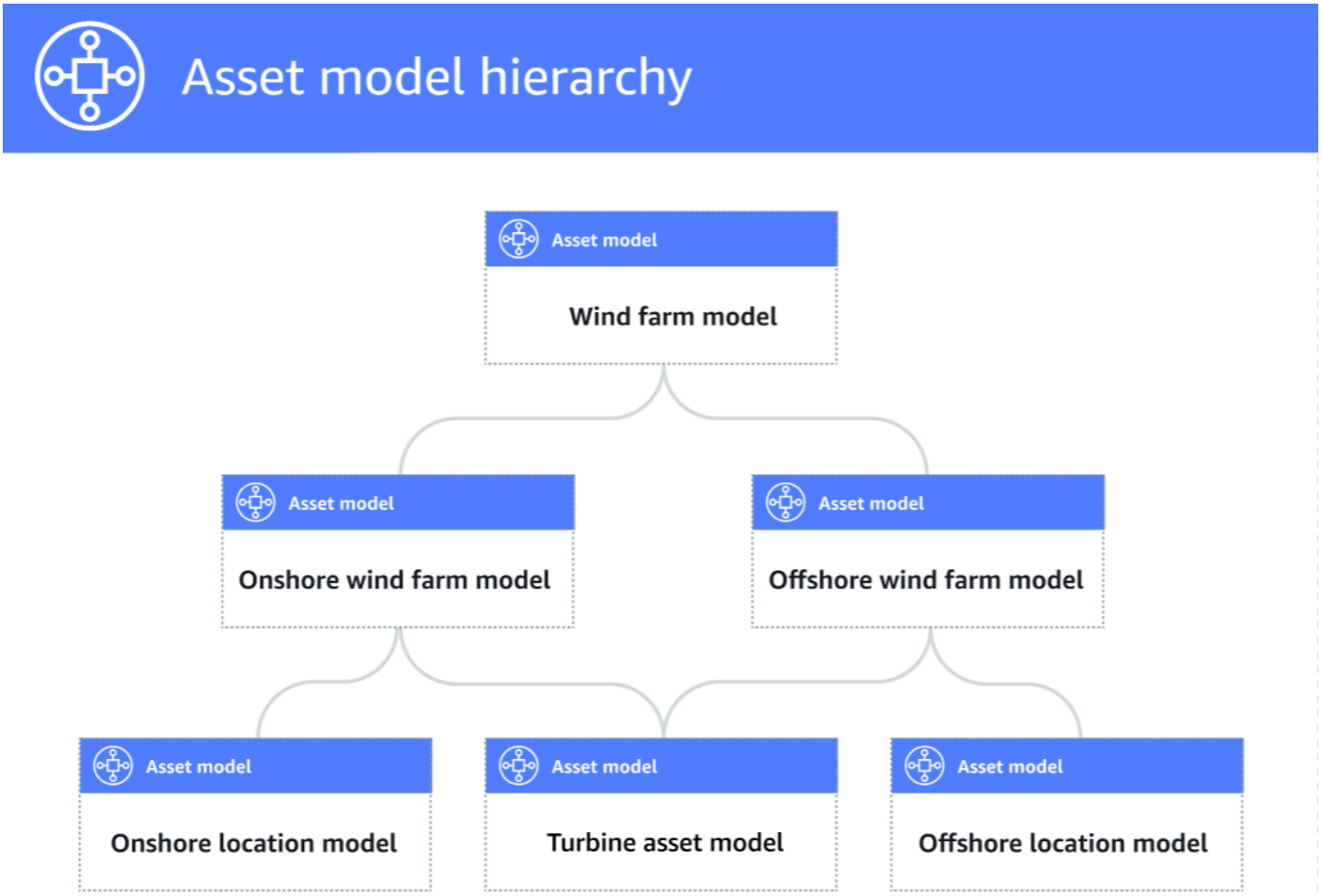
```
{
  "assetModelName": "Wind Farm Asset Model",
  "assetModelDescription": "Represents a wind farm.",
  "assetModelProperties": [
    {
      "name": "Code",
      "dataType": "INTEGER",
      "type": {
        "attribute": {
          "defaultValue": "300"
        }
```

```
      }
    },
    {
      "name": "Location",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Renton"
        }
      }
    },
    {
      "name": "Reliability Manager",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Mary Major"
        }
      }
    },
    {
      "name": "Total Overdrive State Time",
      "dataType": "DOUBLE",
      "unit": "seconds",
      "type": {
        "metric": {
          "expression": "sum(overdrive_state_time)",
          "variables": [
            {
              "name": "overdrive_state_time",
              "value": {
                "propertyId": "ID of Overdrive State Time property in Wind Turbine
Asset Model",
                "hierarchyId": "Turbine Asset Model"
              }
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
```

```
    },
    {
      "name": "Total Average Power",
      "dataType": "DOUBLE",
      "unit": "Watts",
      "type": {
        "metric": {
          "expression": "sum(turbine_avg_power)",
          "variables": [
            {
              "name": "turbine_avg_power",
              "value": {
                "propertyId": "ID of Average Power property in Wind Turbine Asset
 Model",
                "hierarchyId": "Turbine Asset Model"
              }
            }
          ],
          "window": {
            "tumbling": {
              "interval": "5m"
            }
          }
        }
      }
    }
  ],
  "assetModelHierarchies": [
    {
      "name": "Turbine Asset Model",
      "childAssetModelId": "ID of Wind Turbine Asset Model"
    }
  ]
}
```

Definition von Hierarchien für Anlagenmodelle

Sie können Anlagenmodellhierarchien definieren, um logische Verknüpfungen zwischen den Anlagenmodellen in Ihrem Industriebetrieb herzustellen. Sie können beispielsweise einen Windpark definieren, der aus Onshore- und Offshore-Windparks besteht. Ein Onshore-Windpark umfasst eine Turbine und einen Standort an Land. Ein Offshore-Windpark umfasst eine Turbine und einen Offshore-Standort.



Wenn Sie ein untergeordnetes Anlagenmodell über eine Hierarchie einem übergeordneten Anlagenmodell zuordnen, können die Metriken des übergeordneten Anlagenmodells Daten aus den Kennzahlen des untergeordneten Anlagenmodells eingeben. Sie können die Hierarchien und Kennzahlen des Anlagenmodells verwenden, um Statistiken zu berechnen, die Aufschluss über Ihren Betrieb oder einen Teil Ihres Betriebs geben. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

Jede Hierarchie definiert eine Beziehung zwischen einem übergeordneten Anlagemodell und einem untergeordneten Anlagenmodell. In einem übergeordneten Anlagenmodell können Sie mehrere Hierarchien für dasselbe untergeordnete Anlagemodell definieren. Wenn Sie beispielsweise in Ihren Windparks über zwei verschiedene Typen von Windturbinen verfügen, bei denen alle Windturbinen durch dasselbe Anlagenmodell repräsentiert werden, können Sie für jeden Typ eine Hierarchie definieren. Anschließend können Sie im Windparkmodell Metriken definieren, um unabhängige und kombinierte Statistiken für jeden Windturbinentyp zu berechnen.

Ein übergeordnetes Anlagenmodell kann mehreren untergeordneten Vermögensmodellen zugeordnet werden. Wenn Sie beispielsweise einen Onshore-Windpark und einen Offshore-Windpark haben, die durch zwei verschiedene Anlagenmodelle repräsentiert werden, können Sie diese Anlagenmodelle demselben übergeordneten Windpark-Anlagenmodell zuordnen.

Ein untergeordnetes Anlagenmodell kann auch mehreren übergeordneten Vermögensmodellen zugeordnet werden. Wenn Sie beispielsweise über zwei verschiedene Arten von Windparks verfügen, bei denen alle Windturbinen durch dasselbe Anlagenmodell repräsentiert werden, können Sie das Anlagenmodell der Windturbine unterschiedlichen Windpark-Assetmodellen zuordnen.

> **Note**
>
> Wenn Sie eine Anlagenmodellhierarchie definieren, muss es sich bei dem untergeordneten Anlagenmodell um eine frühere Version handeln `ACTIVE` oder eine frühere `ACTIVE` Version haben. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Nachdem Sie hierarchische Komponentenmodelle definiert und Komponenten erstellt haben, können Sie die Komponenten zuordnen, um die Beziehung zwischen über- und untergeordneten Komponenten herzustellen. Weitere Informationen finden Sie unter Erstellen von Komponenten und Zuordnen und Aufheben der Zuordnung von Komponenten.

Themen

- Definieren von Anlagenmodellhierarchien (Konsole)
- Definieren von Asset-Hierarchien ()AWS CLI

Definieren von Anlagenmodellhierarchien (Konsole)

Wenn Sie in der AWS IoT SiteWise Konsole eine Hierarchie für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- Hierarchiename — Der Name der Hierarchie, z. **`Wind Turbines`** B.
- Hierarchiemodell — Das Modell der untergeordneten Anlage.
- Externe Hierarchie-ID (optional) — Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Weitere Informationen finden Sie unter Erstellen eines Komponentenmodells (Konsole).

Definieren von Asset-Hierarchien ()AWS CLI

Wenn Sie mit der AWS IoT SiteWise API eine Hierarchie für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- `name`— Der Name der Hierarchie, z. **`Wind Turbines`** B.
- `childAssetModelId`— Die ID oder die externe ID des untergeordneten Asset-Modells für die Hierarchie. Sie können die Operation ListAssetModels verwenden, um die ID eines vorhandenen Asset-Modells zu ermitteln.

Example Beispiel für eine Hierarchiedefinition

Das folgende Beispiel zeigt eine Anlagenmodellhierarchie, die die Beziehung eines Windparks zu Windturbinen darstellt. Dieses Objekt ist ein Beispiel für eine AssetModelHierarchie. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI).

```
{
  ...
  "assetModelHierarchies": [
    {
      "name": "Wind Turbines",
      "childAssetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
    },
  ]
}
```

Komponentenmodelle erstellen

Verwenden Sie AWS IoT SiteWise Komponentenmodelle, um Unterbaugruppen zu definieren, auf die Sie anhand von Objektmodellen oder anderen Komponentenmodellen verweisen können. Auf diese Weise können Sie die Definition der Komponente in mehreren anderen Modellen oder mehrfach innerhalb desselben Modells wiederverwenden.

Der Prozess der Definition eines Komponentenmodells ist der Definition eines Asset-Modells sehr ähnlich. Wie ein Asset-Modell hat auch ein Komponentenmodell einen Namen, eine Beschreibung und Asset-Eigenschaften. Komponentenmodelle können jedoch keine Definitionen der Asset-Hierarchie enthalten, da die Komponentenmodelle selbst nicht zur direkten Erstellung von Objekten verwendet werden können. Komponentenmodelle können auch keine Alarme definieren.

Sie können beispielsweise eine Komponente für einen Servomotor mit Eigenschaften für Motortemperatur, Encodertemperatur und Isolationswiderstand definieren. Anschließend können Sie ein Anlagenmodell für Geräte definieren, die Servomotoren enthalten, z. B. eine CNC-Maschine.

> **Note**
>
> - Es empfiehlt sich, bei der Modellierung mit den Knoten der untersten Ebene zu beginnen. Erstellen Sie beispielsweise Ihre Servomotorkomponente, bevor Sie das Anlagenmodell Ihrer CNC-Maschine erstellen. Objektmodelle enthalten Verweise auf bestehende Komponentenmodelle.
> - Sie können ein Asset nicht direkt aus einem Komponentenmodell erstellen. Um ein Asset zu erstellen, das Ihre Komponente verwendet, müssen Sie ein Asset-Modell für Ihr Asset erstellen. Anschließend erstellen Sie dafür ein benutzerdefiniertes Verbundmodell, das auf Ihre Komponente verweist. Weitere Informationen zum Erstellen von Objektmodellen finden Sie unter Weitere Informationen Erstellen von Komponentenmodellen zum Erstellen von benutzerdefinierten Verbundmodellen finden Sie unterErstellen von benutzerdefinierten Verbundmodellen (Komponenten).

In den folgenden Abschnitten wird beschrieben, wie Sie die AWS IoT SiteWise API zum Erstellen von Komponentenmodellen verwenden.

Themen

Erstellen eines Komponentenmodells (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein Komponentenmodell zu erstellen.

Verwenden Sie die Operation CreateAssetModel, um ein Komponentenmodell mit Eigenschaften zu erstellen. Für diesen Vorgang wird eine Nutzlast mit der folgenden Struktur erwartet:

```
{
  "assetModelType": "COMPONENT_MODEL",
  "assetModelName": "String",
```

```
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
}
```

Um ein Komponentenmodell zu erstellen ()AWS CLI

1. Erstellen Sie eine Datei mit dem Namen `component-model-payload.json` und kopieren Sie dann das folgende JSON-Objekt in die Datei:

   ```
   {
     "assetModelType": "COMPONENT_MODEL",
     "assetModelName": "",
     "assetModelDescription": "",
     "assetModelProperties": [

     ]
   }
   ```

2. Verwenden Sie Ihren bevorzugten JSON-Texteditor, um die Datei `component-model-payload.json` für Folgendes zu bearbeiten:

   a. Geben Sie einen Namen (`assetModelName`) für das Komponentenmodell ein, z. B. **`Servo Motor`** oder**`Servo Motor Model`**. Dieser Name muss in diesem Fall für alle Asset- und Komponentenmodelle in Ihrem Konto eindeutig sein AWS-Region.

   b. (Optional) Geben Sie eine externe ID (`assetModelExternalId`) für das Komponentenmodell ein. Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

   c. (Optional) Geben Sie eine Beschreibung (`assetModelDescription`) für das Komponentenmodell ein oder entfernen Sie das `assetModelDescription`-Schlüssel-Wert-Paar.

   d. (Optional) Definieren Sie Asset-Eigenschaften (`assetModelProperties`) für das Komponentenmodell. Weitere Informationen finden Sie unter Definieren von Dateneigenschaften.

   e. (Optional) Fügen Sie Tags (`tags`) für das Komponentenmodell hinzu. Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.

3. Führen Sie den folgenden Befehl aus, um ein Komponentenmodell aus der Definition in der JSON-Datei zu erstellen.

```
aws iotsitewise create-asset-model --cli-input-json file://component-model-
payload.json
```

Der Vorgang gibt eine Antwort zurück, die die Antwort enthält, auf `assetModelId` die Sie sich beziehen, wenn Sie einen Verweis auf Ihr Komponentenmodell in einem Asset-Modell oder einem anderen Komponentenmodell hinzufügen. Die Antwort enthält auch den Zustand des Modells (`assetModelStatus.state`), der anfänglich `CREATING` lautet. Der Status des Komponentenmodells ist so `CREATING` lange gültig, bis die Änderungen übernommen werden.

> **Note**
>
> Die Erstellung des Komponentenmodells kann bei komplexen Modellen bis zu einigen Minuten dauern. Um den aktuellen Status Ihres Komponentenmodells zu überprüfen, verwenden Sie die Operation DescribeAssetModell, indem Sie die angeben`assetModelId`. Sobald der Status des Komponentenmodells lautet`ACTIVE`, können Sie Verweise auf Ihr Komponentenmodell in Objektmodellen oder anderen Komponentenmodellen hinzufügen. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

4. (Optional) Erstellen Sie benutzerdefinierte Verbundmodelle für Ihr Komponentenmodell. Bei benutzerdefinierten Verbundmodellen können Sie Eigenschaften innerhalb des Modells gruppieren oder eine Unterbaugruppe einbeziehen, indem Sie auf ein anderes Komponentenmodell verweisen. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Verbundmodellen (Komponenten).

Beispiel für ein Komponentenmodell

Dieser Abschnitt enthält eine Beispieldefinition für ein Komponentenmodell, mit der Sie ein Komponentenmodell mit den AWS IoT SiteWise SDKs AWS CLI und erstellen können. Dieses Komponentenmodell stellt einen Servomotor dar, der in einem anderen Gerät, z. B. einer CNC-Maschine, verwendet werden kann.

Themen

- Komponentenmodell des Servomotors

Komponentenmodell des Servomotors

Das folgende Komponentenmodell stellt einen Servomotor dar, der in Geräten wie CNC-Maschinen verwendet werden kann. Der Servomotor bietet verschiedene Messwerte, z. B. für Temperaturen und elektrischen Widerstand. Diese Messungen sind als Eigenschaften für Objekte verfügbar, die aus Objektmodellen erstellt wurden, die auf das Komponentenmodell des Servomotors verweisen.

```
{
    "assetModelName": "ServoMotor",
    "assetModelType": "COMPONENT_MODEL",
    "assetModelProperties": [
        {
            "dataType": "DOUBLE",
            "name": "Servo Motor Temperature",
            "type": {
            "measurement": {}
            },
            "unit": "Celsius"
        },
        {
            "dataType": "DOUBLE",
            "name": "Spindle speed",
            "type": {
            "measurement": {}
            },
            "unit": "rpm"
        }
    ]
}
```

Definieren von Dateneigenschaften

Asset-Eigenschaften sind die Strukturen innerhalb jedes Assets, die Asset-Daten enthalten. Bei den Komponenteneigenschaften kann es sich um folgende Typen handeln:

- Attribute — Die im Allgemeinen statischen Eigenschaften eines Assets, z. B. Gerätehersteller oder geografische Region. Weitere Informationen finden Sie unter Definition statischer Daten (Attribute).
- Messungen — Die Sensordatenströme eines Geräts im Rohformat, z. B. mit Zeitstempel versehene Drehzahlwerte oder Temperaturwerte mit Zeitstempel in Celsius. Eine Messung wird durch einen Daten-Stream-Alias definiert. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).

- Transformationen — Die transformierten Zeitreihenwerte eines Assets, z. B. Temperaturwerte mit Zeitstempel in Fahrenheit. Eine Transformation wird durch einen Ausdruck und die Variablen definiert, die mit diesem Ausdruck verwendet werden sollen. Weitere Informationen finden Sie unter Daten transformieren (transformiert).
- Metriken — Die Daten einer Anlage, die über ein bestimmtes Zeitintervall aggregiert wurden, z. B. die stündliche Durchschnittstemperatur. Eine Metrik wird durch ein Zeitintervall, einen Ausdruck und die Variablen definiert, die mit diesem Ausdruck verwendet werden sollen. Metrische Ausdrücke können die metrischen Eigenschaften der zugehörigen Anlagen eingeben, sodass Sie Metriken berechnen können, die Ihren Betrieb oder einen Teil Ihres Betriebs repräsentieren. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen.

Ein Beispiel für die Verwendung von Messungen, Transformationen und Metriken zur Berechnung der Gesamtanlageneffektivität (Overall Equipment Effectiveness, OEE) finden Sie unter Berechnung der Gesamtanlageneffektivität in AWS IoT SiteWise.

Themen

- Definition statischer Daten (Attribute)
- Definition von Datenströmen aus Geräten (Messungen)
- Daten transformieren (transformiert)
- Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken)
- Verwenden von Formelausdrücken

Definition statischer Daten (Attribute)

Asset-Attribute stellen Informationen dar, die im Allgemeinen statisch sind, z. B. Gerätehersteller oder geografischer Standort. Jede Komponente, die Sie anhand eines Komponentenmodells erstellen, enthält die Attribute dieses Modells.

Themen

- Definieren von Attributen (Konsole)
- Attribute definieren ()AWS CLI

Definieren von Attributen (Konsole)

Wenn Sie in der AWS IoT SiteWise Konsole ein Attribut für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- Name — Der Name der Immobilie.
- Standardwert — (Optional) Der Standardwert für dieses Attribut. Aus dem Modell erstellte Komponenten haben diesen Wert für das Attribut. Weitere Informationen zum Überschreiben des Standardwerts in einer aus einem Modell erstellten Komponente finden Sie unter Aktualisieren von Attributwerten.
- Datentyp — Der Datentyp der Eigenschaft, der einer der folgenden ist:
  - Zeichenfolge — Eine Zeichenfolge mit bis zu 1024 Byte.
  - Integer — Eine 32-Bit-Ganzzahl mit Vorzeichen und einem Bereich von [-2.147.483.648, 2.147.483.647].
  - Double — Eine Gleitkommazahl mit einem Bereich [-10^100, 10^100] und einer doppelten IEEE-754-Genauigkeit.
  - **`false`**Boolean — **`true`** oder.
- Externe ID — (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Weitere Informationen finden Sie unter Erstellen eines Komponentenmodells (Konsole).

Attribute definieren ()AWS CLI

Wenn Sie mit der AWS IoT SiteWise API ein Attribut für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- `name`— Der Name der Immobilie.
- `defaultValue`— (Optional) Der Standardwert für dieses Attribut. Aus dem Modell erstellte Komponenten haben diesen Wert für das Attribut. Weitere Informationen zum Überschreiben des Standardwerts in einer aus einem Modell erstellten Komponente finden Sie unter Aktualisieren von Attributwerten.
- `dataType`— Der Datentyp der Eigenschaft, der einer der folgenden ist:
  - `STRING`— Eine Zeichenfolge mit bis zu 1024 Byte.
  - `INTEGER`— Eine 32-Bit-Ganzzahl mit Vorzeichen im Bereich [-2.147.483.648, 2.147.483.647].

  - `DOUBLE`— Eine Fließkommazahl mit einem Bereich [-10^100, 10^100] und einer doppelten IEEE-754-Genauigkeit.
  - `BOOLEAN`— `true` oder. `false`
- `externalId`— (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Example Beispiel für eine Attributdefinition

Im folgenden Beispiel wird ein Attribut veranschaulicht, das die Modellnummer einer Komponente mit einem Standardwert darstellt. Dieses Objekt ist ein Beispiel für eine AssetModelEigenschaft, die ein Attribut enthält. Sie können dieses Objekt als Teil der Payload der CreateAssetModel-Anforderung angeben, um eine Attributeigenschaft zu erstellen. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI).

```
{
...
"assetModelProperties": [
{
  "name": "Model number",
  "dataType": "STRING",
  "type": {
    "attribute": {
      "defaultValue": "BLT123"
    }
  }
}
],
...
}
```

Definition von Datenströmen aus Geräten (Messungen)

Eine Messung stellt den rohen Sensordatenstrom eines Geräts dar, z. B. Temperaturwerte mit Zeitstempel oder Werte für Umdrehungen pro Minute (U/min) mit Zeitstempel.

Themen

- Definieren von Messungen (Konsole)
- Messungen definieren ()AWS CLI

Definieren von Messungen (Konsole)

Wenn Sie in der AWS IoT SiteWise Konsole eine Messung für ein Anlagenmodell definieren, geben Sie die folgenden Parameter an:

- Name — Der Name der Immobilie.
- Einheit — (Optional) Die wissenschaftliche Einheit für die Eigenschaft, z. B. mm oder Celsius.
- Datentyp — Der Datentyp der Eigenschaft, der einer der folgenden ist:
  - Zeichenfolge — Eine Zeichenfolge mit bis zu 1024 Byte.
  - Integer — Eine 32-Bit-Ganzzahl mit Vorzeichen und einem Bereich von [-2.147.483.648, 2.147.483.647].
  - Double — Eine Gleitkommazahl mit einem Bereich [-10^100, 10^100] und einer doppelten IEEE-754-Genauigkeit.
  - **`false`**Boolean — **`true`** oder.
- Externe ID — (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Weitere Informationen finden Sie unter Erstellen eines Komponentenmodells (Konsole).

Messungen definieren ()AWS CLI

Wenn Sie mit der AWS IoT SiteWise API eine Messung für ein Anlagenmodell definieren, geben Sie die folgenden Parameter an:

- `name`— Der Name der Immobilie.
- `dataType`— Der Datentyp der Eigenschaft, der einer der folgenden ist:
  - `STRING`— Eine Zeichenfolge mit bis zu 1024 Byte.
  - `INTEGER`— Eine 32-Bit-Ganzzahl mit Vorzeichen im Bereich [-2.147.483.648, 2.147.483.647].
  - `DOUBLE`— Eine Fließkommazahl mit einem Bereich [-10^100, 10^100] und einer doppelten IEEE-754-Genauigkeit.
  - `BOOLEAN`— `true` oder. `false`
- `unit`— (Optional) Die wissenschaftliche Einheit für die Eigenschaft, z. B. mm oder Celsius.
- `externalId`— (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Example Beispiel für eine Messdefinition

Das folgende Beispiel zeigt eine Messung, die die Messwerte der Temperatursensoren einer Komponente darstellt. Dieses Objekt ist ein Beispiel für eine AssetModelEigenschaft, die eine Messung enthält. Sie können dieses Objekt als Teil der Payload der CreateAssetModel-Anforderung angeben, um eine Messeigenschaft zu erstellen. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI).

Die Messstruktur ist eine leere Struktur, wenn Sie ein Asset-Modell definieren, da Sie später jedes Asset so konfigurieren, dass es eindeutige Gerätedatenströme verwendet. Weitere Informationen darüber, wie Sie die Messeigenschaft einer Anlage mit dem Sensordatenstrom eines Geräts verbinden, finden Sie unterZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

```
{
      ...
      "assetModelProperties": [
      {
          "name": "Temperature C",
          "dataType": "DOUBLE",
          "type": {
              "measurement": {}
          },
          "unit": "Celsius"
      }
  ],
      ...
}
```

Daten transformieren (transformiert)

Transformationen sind mathematische Ausdrücke, die die Datenpunkte von Asset-Eigenschaften einem Formular einem anderen zuordnen. Ein Transformationsausdruck besteht aus Variablen, Literalen, Operatoren und Funktionen für Asset-Eigenschaften. Die transformierten Datenpunkte stehen in einer one-to-one Beziehung zu den Eingabedatenpunkten. AWS IoT SiteWise berechnet jedes Mal, wenn eine der Eingabeeigenschaften einen neuen Datenpunkt erhält, einen neuen transformierten Datenpunkt.

Wenn Ihre Komponente beispielsweise über einen Temperaturmessungs-Stream namens `Temperature_C` mit Einheiten in Celsius verfügt, können Sie jeden Datenpunkt mit der Formel `Temperature_F = 9/5 * Temperature_C + 32` in Fahrenheit konvertieren. Jedes Mal,

wenn ein Datenpunkt im `Temperature_C` Messstrom AWS IoT SiteWise empfangen wird, wird der entsprechende `Temperature_F` Wert innerhalb weniger Sekunden berechnet und ist als `Temperature_F` Eigenschaft verfügbar.

Wenn Ihre Transformation mehr als eine Variable enthält, leitet der Datenpunkt, der früher eintrifft, die Berechnung sofort ein. Stellen Sie sich ein Beispiel vor, bei dem ein Teilehersteller eine Transformation verwendet, um die Produktqualität zu überwachen. Der Hersteller verwendet je nach Bauteiltyp eine andere Norm und verwendet die folgenden Maße, um den Prozess darzustellen:

- `Part_Number`- Eine Zeichenfolge, die den Teiletyp identifiziert.
- `Good_Count`- Eine Ganzzahl, die um eins erhöht wird, wenn das Teil der Norm entspricht.
- `Bad_Count`- Eine Ganzzahl, die um eins erhöht wird, wenn das Teil nicht der Norm entspricht.

Der Hersteller erstellt außerdem eine Transformation,`Quality_Monitor`, die entspricht. `if(eq(Part_Number, "BLT123") and (Bad_Count / (Good_Count + Bad_Count) > 0.1), "Caution", "Normal")`

Diese Transformation überwacht den Prozentsatz fehlerhafter Teile, die für einen bestimmten Teiletyp hergestellt wurden. Wenn die Artikelnummer BLT123 lautet und der Prozentsatz fehlerhafter Teile 10 Prozent (0,1) übersteigt, gibt die Transformation Folgendes zurück. `"Caution"` Andernfalls kehrt die Transformation zurück. `"Normal"`

> **Note**
>
> - Wenn vor anderen Messungen ein neuer Datenpunkt `Part_Number` empfangen wird, verwendet die `Quality_Monitor` Transformation den neuen `Part_Number` Wert und die neuesten `Good_Count` `Bad_Count` UND-Werte. Um Fehler zu vermeiden, setzen `Good_Count` Sie das `Bad_Count` Gerät vor dem nächsten Fertigungslauf zurück.
> - Verwenden Sie Metriken, wenn Sie Ausdrücke erst auswerten möchten, nachdem alle Variablen neue Datenpunkte erhalten haben.

Themen

- Definieren von Transformationen (Konsole)
- Transformationen definieren ()AWS CLI

Definieren von Transformationen (Konsole)

Wenn Sie in der AWS IoT SiteWise Konsole eine Transformation für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- Name — Der Name der Immobilie.
- Einheit — (Optional) Die wissenschaftliche Einheit für die Eigenschaft, z. B. mm oder Celsius.
- Datentyp — Der Datentyp der Transformation, der Double oder String sein kann.
- Externe ID — (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- Formel — Der Transformationsausdruck. Transformationsausdrücke können keine Aggregationsfunktionen oder Temporalfunktionen verwenden. Um die Funktion zur auto Vervollständigung zu öffnen, beginnen Sie mit der Eingabe oder drücken Sie die NACH-UNTEN-TASTE. Weitere Informationen finden Sie unter Verwenden von Formelausdrücken.

> **Important**
>
> Transformationen können Eigenschaften vom Typ Integer, Double, Boolean oder Zeichenfolge eingeben. Boolesche Werte werden in `0` (falsch) und (wahr) konvertiert. 1 Transformationen müssen eine oder mehrere Eigenschaften, die keine Attribute sind, und eine beliebige Anzahl von Attributeigenschaften eingeben. AWS IoT SiteWise berechnet jedes Mal einen neuen transformierten Datenpunkt, wenn die Eingabeeigenschaft, bei der es sich nicht um ein Attribut handelt, einen neuen Datenpunkt erhält. Neue Attributwerte starten keine Transformationsaktualisierungen. Für Ergebnisse der Transformationsberechnung gilt dieselbe Anforderungsrate für API-Operationen mit Objektdaten.
> Formelausdrücke können nur Doppelwerte oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

Weitere Informationen finden Sie unter Erstellen eines Komponentenmodells (Konsole).

Transformationen definieren ()AWS CLI

Wenn Sie mit der AWS IoT SiteWise API eine Transformation für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- `name`— Der Name der Immobilie.
- `unit`— (Optional) Die wissenschaftliche Einheit für die Eigenschaft, z. B. mm oder Celsius.
- `dataType`— Der Datentyp der Transformation, der `DOUBLE` oder sein muss`STRING`.
- `externalId`— (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- `expression`— Der Transformationsausdruck. Transformationsausdrücke können keine Aggregationsfunktionen oder temporale Funktionen verwenden. Weitere Informationen finden Sie unter Verwenden von Formelausdrücken.
- `variables`— Die Liste der Variablen, die die anderen Eigenschaften Ihres Assets definiert, die im Ausdruck verwendet werden sollen. Jede Variablenstruktur enthält einen einfachen Namen, der in dem Ausdruck verwendet werden soll, sowie eine `value`-Struktur zur Identifizierung der mit dieser Variablen zu verknüpfenden Eigenschaft. Die `value`-Struktur enthält folgende Informationen:
  - `propertyId`— Die ID der Eigenschaft, aus der Werte eingegeben werden sollen. Sie können den Namen der Eigenschaft anstelle der ID verwenden.

> **Important**
>
> Transformationen können Eigenschaften vom Typ Integer, Double, Boolean oder Zeichenfolge eingeben. Boolesche Werte werden in `0` (falsch) und (wahr) konvertiert. `1`
> Transformationen müssen eine oder mehrere Eigenschaften, die keine Attribute sind, und eine beliebige Anzahl von Attributeigenschaften eingeben. AWS IoT SiteWise berechnet jedes Mal einen neuen transformierten Datenpunkt, wenn die Eingabeeigenschaft, bei der es sich nicht um ein Attribut handelt, einen neuen Datenpunkt erhält. Neue Attributwerte starten keine Transformationsaktualisierungen. Für Ergebnisse der Transformationsberechnung gilt dieselbe Anforderungsrate für API-Operationen mit Objektdaten.
> Formelausdrücke können nur Doppelwerte oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der

boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

Example Definition transformieren

Das folgende Beispiel zeigt eine Transformationseigenschaft, die die Temperaturmessdaten einer Komponente von Celsius in Fahrenheit konvertiert. Dieses Objekt ist ein Beispiel für eine AssetModelEigenschaft, die eine Transformation enthält. Sie können dieses Objekt als Teil der Payload der CreateAssetModel-Anforderung angeben, um eine Transformationseigenschaft zu erstellen. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI).

```
{
...
"assetModelProperties": [
...
{
  "name": "Temperature F",
  "dataType": "DOUBLE",
  "type": {
    "transform": {
      "expression": "9/5 * temp_c + 32",
      "variables": [
        {
          "name": "temp_c",
          "value": {
            "propertyId": "Temperature C"
          }
        }
      ]
    }
  },
  "unit": "Fahrenheit"
}
],
...
}
```

Example Transformationsdefinition, die drei Variablen enthält

Das folgende Beispiel zeigt eine Transform-Eigenschaft, die eine Warnmeldung (`"Caution"`) zurückgibt, wenn mehr als 10 Prozent der BLT123-Teile nicht dem Standard entsprechen. Andernfalls wird eine Informationsmeldung () `"Normal"` zurückgegeben.

```
{
...
"assetModelProperties": [
...
{
"name": "Quality_Monitor",
"dataType": "STRING",
"type": {
    "transform": {
        "expression": "if(eq(Part_Number,"BLT123") and (Bad_Count / (Good_Count +
 Bad_Count) > 0.1), "Caution", "Normal")",
        "variables": [
            {
                "name": "Part_Number",
                "value": {
                    "propertyId": "Part Number"
                }
            },
            {
                "name": "Good_Count",
                "value": {
                    "propertyId": "Good Count"
                }
            },
            {
                "name": "Bad_Count",
                "value": {
                    "propertyId": "Bad Count"
                }
            }
        ]
    }
}
}
...
}
```

Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken)

Metriken sind mathematische Ausdrücke, die Aggregationsfunktionen verwenden, um alle Eingabedatenpunkte zu verarbeiten und einen einzelnen Datenpunkt pro festgelegtem Zeitintervall auszugeben. Eine Metrik kann beispielsweise die stündliche Durchschnittstemperatur aus einem Temperaturdaten-Stream berechnen.

Metriken können Daten aus Metriken zugehöriger Komponenten eingeben, sodass Sie Statistiken berechnen können, die einen Einblick in die Operation oder eine Teilmenge der Operation gewähren. Beispielsweise kann eine Metrik die durchschnittliche stündliche Temperatur für alle Windturbinen in einem Windpark berechnen. Weitere Informationen zum Definieren von Verknüpfungen zwischen Komponenten finden Sie unter Definition von Hierarchien für Anlagenmodelle.

Metriken können auch Daten aus anderen Eigenschaften eingeben, ohne die Daten für jedes Zeitintervall zu aggregieren. Wenn Sie ein Attribut in einer Formel angeben, AWS IoT SiteWise verwendet es bei der Berechnung der Formel den neuesten Wert für dieses Attribut. Wenn Sie eine Metrik in einer Formel angeben, AWS IoT SiteWise verwendet es den letzten Wert für das Zeitintervall, über das die Formel berechnet wird. Das bedeutet, dass Sie Metriken wie `OEE = Availability * Quality * Performance` `AvailabilityQuality`, wo und wie alle anderen Metriken für dasselbe Asset-Modell `Performance` sind, definieren können.

AWS IoT SiteWise berechnet außerdem automatisch eine Reihe grundlegender Aggregationsmetriken für alle Asset-Eigenschaften. Um Berechnungskosten zu reduzieren, können Sie diese Aggregate verwenden, anstatt benutzerdefinierte Metriken für grundlegende Berechnungen zu definieren. Weitere Informationen finden Sie unter Abfragen von Komponenteneigenschaften-Aggregaten.

Themen

- Definieren von Metriken (Konsole)
- Metriken definieren ()AWS CLI

Definieren von Metriken (Konsole)

Wenn Sie in der AWS IoT SiteWise Konsole eine Metrik für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- Name — Der Name der Immobilie.
- Datentyp — Der Datentyp der Transformation, der Double oder String sein kann.

- Externe ID — (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- Formel — Der metrische Ausdruck. Metrische Ausdrücke können Aggregationsfunktionen verwenden, um Daten aus einer Eigenschaft für alle zugehörigen Anlagen in einer Hierarchie einzugeben. Beginnen Sie mit der Eingabe oder drücken Sie die Abwärtspfeiltaste, um die Funktion zur auto Vervollständigung zu öffnen. Weitere Informationen finden Sie unter Verwenden von Formelausdrücken.

  > **Important**
  >
  > Bei Metriken kann es sich nur um Eigenschaften vom Typ Integer, Double, Boolean oder Zeichenfolge handeln. Boolesche Werte werden in `0` (falsch) und `1` (wahr) konvertiert. Wenn Sie Metrikeingabevariablen im Ausdruck einer Metrik definieren, muss für diese Eingaben dasselbe Zeitintervall wie für die Ausgabemetrik gelten.
  > Formelausdrücke können nur Doppelwerte oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

- Zeitintervall — Das metrische Zeitintervall. AWS IoT SiteWise unterstützt die folgenden Zeitintervalle im Taumelfenster, wobei jedes Intervall beginnt, wenn das vorherige endet:
  - 1 Minute — 1 Minute, berechnet am Ende jeder Minute (00:00:00 Uhr, 12:01:00 Uhr, 12:02:00 Uhr usw.).
  - 5 Minuten — 5 Minuten, berechnet am Ende aller fünf Minuten, beginnend mit der vollen Stunde (00:00:00 Uhr, 12:05:00 Uhr, 00:10:00 Uhr usw.).
  - 15 Minuten — 15 Minuten, berechnet am Ende aller fünfzehn Minuten, beginnend mit der vollen Stunde (00:00:00 Uhr, 00:15:00 Uhr, 12:30:00 Uhr usw.).
  - 1 Stunde — 1 Stunde (60 Minuten), berechnet am Ende jeder Stunde in UTC (12:00:00 Uhr, 01:00:00 Uhr, 02:00:00 Uhr usw.).
  - 1 Tag — 1 Tag (24 Stunden), berechnet am Ende eines jeden Tages in UTC (Montag 12:00:00 Uhr, Dienstag 12:00:00 Uhr usw.).
  - 1 Woche — 1 Woche (7 Tage), berechnet am Ende jedes Sonntags in UTC (jeden Montag um 00:00:00 Uhr).

  - Benutzerdefiniertes Intervall — Sie können ein beliebiges Zeitintervall zwischen einer Minute und einer Woche eingeben.
- Offsetdatum — (Optional) Das Referenzdatum, ab dem Daten aggregiert werden sollen.
- Offsetzeit — (Optional) Die Referenzzeit, ab der Daten aggregiert werden sollen. Die Offsetzeit muss zwischen 00:00:00 und 23:59:59 liegen.
- Offset-Zeitzone — (Optional) Die Zeitzone für den Offset. Wenn sie nicht angegeben ist, ist die standardmäßige Offset-Zeitzone die koordinierte Weltzeit (UTC).

Unterstützte Zeitzonen

  - (UTC+ 00:00) Koordinierte Weltzeit
  - (UTC+ 01:00) Europäische Zentralzeit
  - (UTC+ 02:00) Osteuropäische
  - (UTC03+:00) Ostafrikanische Zeit
  - (UTC+ 04:00) Nahöstliche Zeit
  - (UTC+ 05:00) Pakistanische Lahore-Zeit
  - (UTC+ 05:30) Indische Standardzeit
  - (UTC+ 06:00) Normalzeit in Bangladesch
  - (UTC+ 07:00) Vietnamesische Normalzeit
  -
  - (UTC+ 09:00) Japanische Normalzeit
  - (UTC+ 09:30) Australische Zentralzeit
  - (UTC+ 10:00) Australische Ostzeit
  - (UTC+ 11:00) Salomonische Normalzeit
  - (UTC+ 12:00) Neuseeländische Normalzeit
  - (UTC- 11:00) Midway-Inseln-Zeit
  - (UTC- 10:00) Hawaii-Normalzeit
  - (UTC- 09:00) Alaska-Normalzeit
  - (UTC- 08:00) Pazifische Standardzeit
  - (UTC- 07:00) Phoenix-Standardzeit
  - (UTC- 06:00) Zentrale Standardzeit
  - (UTC- 05:00) Östliche Standardzeit

- (UTC- 04:00) Zeit in Puerto Rico und den Amerikanischen Jungferninseln
- (UTC- 03:00) Argentinische Normalzeit
- (UTC- 02:00) Südgeorgische Zeit
- (UTC- 01:00) Zentralafrikanische Zeit

Example benutzerdefiniertes Zeitintervall mit einem Offset (Konsole)

Das folgende Beispiel zeigt Ihnen, wie Sie ein 12-Stunden-Zeitintervall mit einem Offset am 20. Februar 2021 um 18:30:30 Uhr (PST) definieren.

Um ein benutzerdefiniertes Intervall mit einem Offset zu definieren

1. Wählen Sie für Zeitintervall die Option Benutzerdefiniertes Intervall aus.
2. Führen Sie für Zeitintervall einen der folgenden Schritte aus:
   - Geben Sie Stunden ein**`12`**, und wählen Sie dann aus.
   - Geben Sie ein**`720`**, und wählen Sie dann Minuten aus.
   - Geben Sie ein**`43200`**, und wählen Sie dann Sekunden.

   > ⚠ Important
   >
   > Das Zeitintervall muss unabhängig von der Einheit eine Ganzzahl sein.
3. Wählen Sie 2021/02/20 als Offset-Datum aus.
4. Geben Sie für Offsetzeit den Wert ein. **`18:30:30`**
5. Wählen Sie für Offset-Zeitzone (UTC- 08:00) Pacific Standard Time aus.

Wenn Sie die Metrik am 1. Juli 2021 vor oder um 18:30 Uhr (PST) erstellen, erhalten Sie das erste Aggregationsergebnis am 1. Juli 2021 um 18:30 Uhr (PST). Das zweite Aggregationsergebnis wird am 2. Juli 2021 um 06:30:30 Uhr (PST) usw. angezeigt.

Metriken definieren ()AWS CLI

Wenn Sie mit der AWS IoT SiteWise API eine Metrik für ein Asset-Modell definieren, geben Sie die folgenden Parameter an:

- `name`— Der Name der Immobilie.
- `dataType`— Der Datentyp der Metrik, der `DOUBLE` oder sein kann`STRING`.
- `externalId`— (Optional) Dies ist eine benutzerdefinierte ID. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- `expression`— Der metrische Ausdruck. Metrische Ausdrücke können Aggregationsfunktionen verwenden, um Daten aus einer Eigenschaft für alle zugehörigen Anlagen in einer Hierarchie einzugeben. Weitere Informationen finden Sie unter Verwenden von Formelausdrücken.
- `window`— Das Zeitintervall und der Offset für das Taumelfenster der Metrik, wobei jedes Intervall beginnt, wenn das vorherige endet:
  - `interval`— Das Zeitintervall für das Taumelfenster. Das Zeitintervall muss zwischen einer Minute und einer Woche liegen.
  - `offsets`— Der Offset für das Taumelfenster.

  Weitere Informationen finden Sie TumblingWindowin der AWS IoT SiteWise API-Referenz.

  Example benutzerdefiniertes Zeitintervall mit einem Offset (AWS CLI)

  Das folgende Beispiel zeigt Ihnen, wie Sie ein 12-Stunden-Zeitintervall mit einem Offset am 20. Februar 2021 um 18:30:30 Uhr (PST) definieren.

```
{
    "window": {
        "tumbling": {
            "interval": "12h",
            "offset": " 2021-07-23T18:30:30-08"
        }
    }
}
```

  Wenn Sie die Metrik am 1. Juli 2021 vor oder um 18:30 Uhr (PST) erstellen, erhalten Sie das erste Aggregationsergebnis am 1. Juli 2021 um 18:30 Uhr (PST). Das zweite Aggregationsergebnis wird am 2. Juli 2021 um 06:30:30 Uhr (PST) usw. angezeigt.
- `variables`— Die Variablenliste, die die anderen Eigenschaften Ihrer Anlage oder Ihrer untergeordneten Anlagen definiert, die in dem Ausdruck verwendet werden sollen. Jede Variablenstruktur enthält einen einfachen Namen, der in dem Ausdruck verwendet werden

soll, sowie eine `value`-Struktur zur Identifizierung der mit dieser Variablen zu verknüpfenden Eigenschaft. Die `value`-Struktur enthält folgende Informationen:

- `propertyId`— Die ID der Eigenschaft, aus der Werte abgerufen werden sollen. Sie können den Namen der Eigenschaft anstelle der ID verwenden, wenn die Eigenschaft im aktuellen Modell (und nicht in einem Modell aus einer Hierarchie) definiert ist.
- `hierarchyId`— (Optional) Die ID der Hierarchie, aus der untergeordnete Vermögenswerte für die Eigenschaft abgefragt werden sollen. Sie können den Namen der Hierarchiedefinition anstelle der ID verwenden. Wenn Sie diesen Wert weglassen, AWS IoT SiteWise wird die Eigenschaft im aktuellen Modell gesucht.

> **Important**
>
> Bei Metriken kann es sich nur um Eigenschaften vom Typ Integer, Double, Boolean oder Zeichenfolge handeln. Boolesche Werte werden in `0` (falsch) und 1 (wahr) konvertiert. Wenn Sie Metrikeingabevariablen im Ausdruck einer Metrik definieren, muss für diese Eingaben dasselbe Zeitintervall wie für die Ausgabemetrik gelten.
> Formelausdrücke können nur Doppelwerte oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

- `unit`— (Optional) Die wissenschaftliche Einheit für die Eigenschaft, z. B. mm oder Celsius.

Example Beispiel für eine Metrik-Definition

Das folgende Beispiel zeigt eine Metrikeigenschaft, die die Temperaturmessdaten einer Komponente aggregiert, um die maximale Durchschnittstemperatur in Fahrenheit zu berechnen. Dieses Objekt ist ein Beispiel für eine AssetModelEigenschaft, die eine Metrik enthält. Sie können dieses Objekt als Teil der Payload der CreateAssetModel-Anforderung angeben, um eine Metrikeigenschaft zu erstellen. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI).

```
{
      ...
      "assetModelProperties": [
      ...
```

```
      {
        "name": "Max temperature",
        "dataType": "DOUBLE",
        "type": {
          "metric": {
            "expression": "max(temp_f)",
            "variables": [
              {
                "name": "temp_f",
                "value": {
                  "propertyId": "Temperature F"
                }
              }
            ],
            "window": {
              "tumbling": {
                "interval": "1h"
              }
            }
          }
        },
        "unit": "Fahrenheit"
      }
    ],
    ...
}
```

Example Beispiel für eine Metrikdefinition, die Daten aus zugehörigen Assets eingibt

Das folgende Beispiel zeigt eine metrische Eigenschaft, die die durchschnittlichen Leistungsdaten mehrerer Windturbinen aggregiert, um die durchschnittliche Gesamtleistung für einen Windpark zu berechnen. Dieses Objekt ist ein Beispiel für eine AssetModelEigenschaft, die eine Metrik enthält. Sie können dieses Objekt als Teil der Payload der CreateAssetModel-Anforderung angeben, um eine Metrikeigenschaft zu erstellen.

```
{
      ...
      "assetModelProperties": [
      ...
      {
          "name": "Total Average Power",
          "dataType": "DOUBLE",
          "type": {
```

```
            "metric": {
              "expression": "avg(power)",
              "variables": [
                {
                  "name": "power",
                  "value": {
                    "propertyId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
                    "hierarchyId": "Turbine Asset Model"
                  }
                }
              ],
              "window": {
                "tumbling": {
                  "interval": "5m"
                }
              }
            }
          },
          "unit": "kWh"
        }
      ],
      ...
}
```

Verwenden von Formelausdrücken

Mit Formelausdrücken können Sie die mathematischen Funktionen definieren, um Ihre industriellen Rohdaten zu transformieren und zu aggregieren, sodass Sie Einblicke in Ihre Operation gewinnen. Formelausdrücke kombinieren Literale, Operatoren, Funktionen und Variablen, um Daten zu verarbeiten. Weitere Informationen zur Definition von Asset-Eigenschaften, die Formelausdrücke verwenden, finden Sie unter Daten transformieren (transformiert) undAggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken). Transformationen und Metriken sind Formeleigenschaften.

Themen

- Verwenden von Variablen in Formelausdrücken
- Verwendung von Literalen in Formelausdrücken
- Verwendung von Operatoren in Formelausdrücken
- Verwendung von Konstanten in Formelausdrücken
- Verwenden von Funktionen in Formelausdrücken

- Tutorials zu Formelausdrücken

Verwenden von Variablen in Formelausdrücken

Variablen stellen AWS IoT SiteWise Asset-Eigenschaften in Formelausdrücken dar. Verwenden Sie Variablen, um Werte aus anderen Objekteigenschaften in Ihre Ausdrücke einzugeben, sodass Sie Daten aus konstanten Eigenschaften (Attributen), Rohdatenströmen (Messungen) und anderen Formeleigenschaften verarbeiten können.

Variablen können Asset-Eigenschaften aus demselben Asset-Modell oder aus zugehörigen untergeordneten Asset-Modellen darstellen. Nur metrische Formeln können Variablen aus untergeordneten Vermögensmodellen eingeben.

Sie identifizieren Variablen in der Konsole und in der API mit unterschiedlichen Namen.

- AWS IoT SiteWise Konsole — Verwenden Sie die Namen von Asset-Eigenschaften als Variablen in Ihren Ausdrücken.
- AWS IoT SiteWise API (AWS CLI, AWS SDKs) — Definieren Sie Variablen mit der ExpressionVariableStruktur, die einen Variablennamen und einen Verweis auf eine Asset-Eigenschaft erfordert. Der Variablenname kann Kleinbuchstaben, Zahlen und Unterstriche enthalten. Verwenden Sie dann Variablennamen, um in Ihren Ausdrücken auf Asset-Eigenschaften zu verweisen.

Bei Variablennamen wird zwischen Groß- und Kleinschreibung unterschieden.

Weitere Informationen finden Sie unter Transformationen definieren und Metriken definieren.

Verwenden von Variablen zum Verweisen auf Eigenschaften

Der Wert einer Variablen definiert die Eigenschaft, auf die sie verweist. AWS IoT SiteWise bietet verschiedene Möglichkeiten, dies zu tun.

- Nach Eigenschafts-ID: Sie können die eindeutige ID (UUID) der Immobilie angeben, um sie zu identifizieren.
- Nach Namen: Wenn sich die Immobilie auf demselben Objektmodell befindet, können Sie ihren Namen im Feld für die Eigenschafts-ID angeben.
- Nach Pfad: Ein Variablenwert kann anhand seines Pfads auf eine Eigenschaft verweisen. Weitere Informationen finden Sie unter Verwenden von Pfaden zum Verweisen auf benutzerdefinierte Eigenschaften von Verbundmodellen.

> **Note**
>
> Variablen werden von der AWS IoT SiteWise Konsole nicht unterstützt. Sie werden von der AWS IoT SiteWise API (einschließlich der AWS Command Line Interface AWS CLI) und AWS SDKs verwendet.

Eine Variable, von der Sie in einer Antwort erhalten, AWS IoT SiteWise enthält vollständige Informationen über den Wert, einschließlich der ID und des Pfads.

Wenn Sie jedoch eine Variable an übergeben AWS IoT SiteWise (z. B. bei einem „create“ - oder „update“ -Aufruf), müssen Sie nur eine dieser Variablen angeben. Wenn Sie beispielsweise den Pfad angeben, müssen Sie die ID nicht angeben.

Verwendung von Literalen in Formelausdrücken

Sie können Zahlen- und Zeichenkettenliterale in Formelausdrücken definieren.

- Zahlen

  Verwenden Sie Zahlen und wissenschaftliche Schreibweise, um ganze Zahlen und Doppelzahlen zu definieren. Sie können die E-Notation verwenden, um Zahlen in wissenschaftlicher Schreibweise auszudrücken.

  Beispiele: `12.0`, `.9`, `-23.1`, `7.89e3`, `3.4E-5`

- Zeichenfolgen

  Verwenden Sie die Zeichen `'` (Anführungszeichen) und `''` (doppelte Anführungszeichen), um Zeichenketten zu definieren. Der Zitattyp für Anfang und Ende muss übereinstimmen. Um ein Anführungszeichen zu maskieren, das dem entspricht, das Sie zur Deklaration einer Zeichenfolge verwenden, fügen Sie dieses Anführungszeichen zweimal ein. Dies ist das einzige Escape-Zeichen in AWS IoT SiteWise Zeichenketten.

  Beispiele: `'active'`, `"inactive"`, `'{"temp": 52}'`, `"{""temp"": ""high""}"`

Verwendung von Operatoren in Formelausdrücken

Sie können die folgenden gängigen Operatoren in Formelausdrücken verwenden.

Operator	Beschreibung
+	Wenn beide Operanden Zahlen sind, addiert dieser Operator den linken und den rechten Operanden. Wenn einer der Operanden eine Zeichenfolge ist, verkettet dieser Operator den linken und den rechten Operanden als Zeichenketten. Der Ausdruck wird beispielsweise zu ausgewert et. `1 + 2 + " is three"` `"3 is three"` Die verkettete Zeichenfolge kann bis zu 1024 Zeichen enthalten. Wenn die Zeichenfolge 1024 Zeichen überschreitet, wird AWS IoT SiteWise kein Datenpunkt für diese Berechnun g ausgegeben.
-	Subtrahiert den rechten Operanden vom linken Operanden Sie können diesen Operator nur mit numerisch en Operanden verwenden.
/	Dividiert den linken Operanden durch den rechten Operanden Sie können diesen Operator nur mit numerisch en Operanden verwenden.
*	Multipliziert die linken und rechten Operanden. Sie können diesen Operator nur mit numerisch en Operanden verwenden.
^	Hebt den linken Operanden auf die Potenz des rechten Operanden (Exponentiation). Sie können diesen Operator nur mit numerisch en Operanden verwenden.

Operator	Beschreibung
`%`	Gibt den Rest zurück, der beim Dividieren des linken Operanden durch den rechten Operanden entsteht. Das Ergebnis hat das gleiche Zeichen wie der linke Operand. Dieses Verhalten unterscheidet sich von der Modulo-Operation. Sie können diesen Operator nur mit numerischen Operanden verwenden.
`x < y`	Gibt zurück`1`, wenn kleiner als `x` ist`y`, andernfalls`0`.
`x > y`	Gibt zurück`1`, wenn größer als `x` ist`y`, andernfalls`0`.
`x <= y`	Gibt zurück`1`, ob kleiner als oder gleich `x` ist`y`, andernfalls`0`.
`x >= y`	Gibt zurück`1`, ob größer als oder gleich `x` ist`y`, andernfalls`0`.
`x == y`	Gibt zurück`1`, ob gleich `x` ist`y`, andernfalls`0`.
`x != y`	Gibt zurück`1`, wenn nicht gleich `x` ist`y`, andernfalls`0`.

Operator	Beschreibung
`!` x	Gibt zurück`1`, ob als `0` (falsch) ausgewertet x wird, andernfalls`0`. xwird als falsch bewertet, wenn: • xist ein numerischer Operand und wird als ausgewertet. `0` • xwird als leere Zeichenfolge ausgewertet. • xwird als leeres Array ausgewertet. • xwird als ausgewertet`None`.
`x and y`	Gibt zurück`0`, ob als `0` (falsch) ausgewertet x wird. Andernfalls wird das ausgewertete Ergebnis von zurückgegebeny. xoder y wird als falsch bewertet, wenn: • xoder y ist ein numerischer Operand und wird als ausgewertet. `0` • xoder y wird als leere Zeichenfolge ausgewertet. • xoder y wird als leeres Array ausgewertet. • xoder y wird als ausgewertet`None`.

Operator	Beschreibung
`x or y`	Gibt zurück`1`, ob als 1 (wahr) ausgewertet `x` wird. Andernfalls wird das ausgewertete Ergebnis von zurückgegeben`y`. `x`oder `y` wird als falsch bewertet, wenn: • `x`oder `y` ist ein numerischer Operand und wird als ausgewertet. `0` • `x`oder `y` wird als leere Zeichenfolge ausgewertet. • `x`oder `y` wird als leeres Array ausgewertet. • `x`oder `y` wird als ausgewertet`None`.
`not x`	Gibt zurück`1`, ob als `0` (falsch) ausgewertet `x` wird, andernfalls`0`. `x`wird als falsch bewertet, wenn: • `x`ist ein numerischer Operand und wird als ausgewertet. `0` • `x`wird als leere Zeichenfolge ausgewertet. • `x`wird als leeres Array ausgewertet. • `x`wird als ausgewertet`None`.

`[]`
 	
`s[index]`
	Gibt das Zeichen an einem Index `index` der Zeichenfolge zurück`s`. Dies entspricht der Indexsyntax in Python.
	
	Example Beispiele
	
	• `"Hello!"[1]` gibt `e` zurück.
	• `"Hello!"[-2]` gibt `o` zurück.

Operator	Beschreibung

`[]`
 	
`s[start:end:step]`
	Gibt einen Teil der Zeichenfolge zurück`s`. Dies entspricht der Slice-Syntax in Python. Dieser Operator hat die folgenden Argumente:
	
	• `start`— (Optional) Der inklusive Startindex des Slice. Standardeinstellung: `0`.
	• `end`— (Optional) Der exklusive Endindex des Slice. Standardmäßig wird die Länge der Zeichenfolge verwendet.
	• `step`— (Optional) Die Zahl, die für jeden Schritt im Slice erhöht werden soll. Sie können beispielsweise angeben`2`, dass ein Segment mit jedem zweiten Zeichen zurückgegeben werden soll, oder Sie können angeben, `-1` dass das Segment umgekehrt werden soll. Standardeinstellung: `1`.
	
	Sie können das `step` Argument weglassen, um seinen Standardwert zu verwenden. Beispiel: `s[1:4:1]` ist gleichbedeutend mit `s[1:4]`.
	
	Bei den Argumenten muss es sich um ganze Zahlen oder um die Konstante None handeln. Wenn Sie angeben`none`, AWS IoT SiteWise wird der Standardwert für dieses Argument verwendet.
	
	Example Beispiele
	
	• `"Hello!"[1:4]` gibt `"ell"` zurück.
	• `"Hello!"[:2]` gibt `"He"` zurück.
	• `"Hello!"[3:]` gibt `"lo!"` zurück.
	• `"Hello!"[:-4]` gibt `"He"` zurück.
	• `"Hello!"[::2]` gibt `"Hlo"` zurück.

Operator	Beschreibung
	• `"Hello!"[::-1]` gibt `"!olleH"` zurück.

Verwendung von Konstanten in Formelausdrücken

Sie können die folgenden allgemeinen mathematischen Konstanten in Ihren Ausdrücken verwenden. Bei allen Konstanten wird nicht zwischen Groß- und Kleinschreibung unterschieden.

> **Note**
>
> Wenn Sie eine Variable mit demselben Namen wie eine Konstante definieren, überschreibt die Variable die Konstante.

Konstante	Beschreibung
`pi`	Die Zahl pi (π): `3.141592653589793`
`e`	Die Zahl e: `2.718281828459045`
`true`	Entspricht der Zahl 1. In werden AWS IoT SiteWise Boolesche Werte in ihre Zahlenäqu ivalente umgewandelt.
`false`	Entspricht der Zahl 0. In werden AWS IoT SiteWise Boolesche Werte in ihre Zahlenäqu ivalente umgewandelt.
`none`	Entspricht keinem Wert. Sie können diese Konstante verwenden, um nichts als Ergebnis eines bedingten Ausdrucks auszugeben.

Verwenden von Funktionen in Formelausdrücken

Sie können die folgenden Funktionen verwenden, um mit Daten in Ihren Formelausdrücken zu arbeiten.

Transformationen und Metriken unterstützen verschiedene Funktionen. Die folgende Tabelle zeigt, welche Funktionstypen mit den einzelnen Typen von Formeleigenschaften kompatibel sind.

> **Note**
>
> Sie können maximal 10 Funktionen in einen Formelausdruck aufnehmen.

Typ der Funktion	Transformationen	Metriken
Verwenden gängiger Funktionen in Formelausdrücken	 Ja	 Ja
Verwenden von Vergleichsfunktionen in Formelausdrücken	 Ja	 Ja
Verwenden von bedingten Funktionen in Formelausdrücken	 Ja	 Ja
Verwenden von Zeichenkettenfunktionen in Formelausdrücken	 Ja	 Ja
Verwenden von Aggregationsfunktionen in Formelausdrücken	 Nein	 Ja

Typ der Funktion	Transformationen	Metriken
Verwendung von temporalen Funktionen in Formelausdrücken	 Ja	 Ja
Verwenden von Datums- und Uhrzeitfunktionen in Formelausdrücken	 Ja	 Ja

Syntax der Funktion

Sie können die folgende Syntax verwenden, um Funktionen zu erstellen:

Reguläre Syntax

Bei der regulären Syntax folgen auf den Funktionsnamen Klammern mit null oder mehr Argumenten.

function_name(*argument1, argument2, argument3, ...*). Funktionen mit der regulären Syntax könnten beispielsweise wie `log(x)` und aussehen`contains(s, substring)`.

Einheitliche Syntax für Funktionsaufrufe (UFCS)

Mit UFCS können Sie Funktionen mithilfe der Syntax für Methodenaufrufen in der objektorientierten Programmierung aufrufen. Bei UFCS folgt auf das erste Argument Punkt (`.`), dann der Funktionsname und die verbleibenden Argumente (falls vorhanden) in Klammern.

argument1.*function_name*(*argument2, argument3, ...*). Funktionen mit UFCS könnten beispielsweise wie `x.log()` und `s.contains(substring)` aussehen.

Sie können UFCS auch verwenden, um nachfolgende Funktionen zu verketten. AWS IoT SiteWise verwendet das Auswertungsergebnis der aktuellen Funktion als erstes Argument für die nächste Funktion.

Sie können beispielsweise `message.jp('$.status').lower().contains('fail')` anstelle von verwenden`contains(lower(jp(message, '$.status')),'fail')`.

Weitere Informationen finden Sie auf der Website der Programmiersprache D.

> **Note**
>
> Sie können UFCS für alle AWS IoT SiteWise Funktionen verwenden.
> AWS IoT SiteWise Bei Funktionen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Beispielsweise können Sie `lower(s)` und `Lower(s)` synonym verwenden.

Verwenden gängiger Funktionen in Formelausdrücken

In Transformationen und Metriken können Sie die folgenden Funktionen verwenden, um allgemeine mathematische Funktionen in Transformationen und Metriken zu berechnen.

Funktion	Beschreibung
`abs(x)`	Gibt den absoluten Wert von x zurück.
`acos(x)`	Gibt den Arkuskosinus von x zurück.
`asin(x)`	Gibt den Arkussinus von x zurück.
`atan(x)`	Gibt den Arkustangens von x zurück.
`cbrt(x)`	Gibt die Kubikwurzel von x zurück.
`ceil(x)`	Gibt die nächste Ganzzahl zurück, die größer als x ist.
`cos(x)`	Gibt den Kosinus von x zurück.
`cosh(x)`	Gibt den hyperbolischen Kosinus von x zurück.
`cot(x)`	Gibt den Kotangens von zurück. x
`exp(x)`	Gibt e hoch x zurück.

Funktion	Beschreibung
`expm1(x)`	Gibt `exp(x) - 1` zurück. Verwenden Sie diese Funktion, um kleinere Werte von genauer `exp(x) - 1` zu berechnen. `x`
`floor(x)`	Gibt die nächste ganze Zahl zurück, die kleiner als `x` ist.
`log(x)`	Gibt $\log_e$ (Basis `e`) von `x` zurück.
`log10(x)`	Gibt $\log_{10}$ (Basis `10`) von `x` zurück.
`log1p(x)`	Gibt `log(1 + x)` zurück. Verwenden Sie diese Funktion, um `log(1 + x)` für kleine Werte von genauer zu berechnen`x`.
`log2(x)`	Gibt $\log_2$ (Basis `2`) von `x` zurück.
`pow(x, y)`	Gibt `x` hoch `y` zurück. Das entspricht`x ^ y`.
`signum(x)`	Gibt das Vorzeichen von `x` (`-1` für negative Eingaben, `0` für Nulleingaben, `+1` für positive Eingaben) zurück.
`sin(x)`	Gibt den Sinus von `x` zurück.
`sinh(x)`	Gibt den hyperbolischen Sinus von `x` zurück.
`sqrt(x)`	Gibt die Quadratwurzel von `x` zurück.
`tan(x)`	Gibt den Tangens von `x` zurück.
`tanh(x)`	Gibt den hyperbolischen Tangens von `x` zurück.

Verwenden von Vergleichsfunktionen in Formelausdrücken

In Transformationen und Metriken können Sie die folgenden Vergleichsfunktionen verwenden, um zwei Werte zu vergleichen und 1 (wahr) oder `0` (falsch) auszugeben. AWS IoT SiteWise vergleicht Zeichenketten in lexikografischer Reihenfolge.

Funktion	Beschreibung
`gt(x, y)`	Gibt 1 zurück, wenn `x` größer als `y` ist, andernfalls `0` (`x > y`). Diese Funktion gibt keinen Wert zurück, wenn `x` es sich um inkompatible Typen `y` handelt, z. B. eine Zahl und eine Zeichenfolge.
`gte(x, y)`	Gibt 1 zurück, wenn `x` größer oder gleich `y` ist, andernfalls `0` (`x ≥ y`). AWS IoT SiteWise betrachtet die Argumente als gleich, wenn sie innerhalb einer relativen Toleranz von liegen`1E-9`. Dies verhält sich ähnlich wie die Funktion isclose in Python. Diese Funktion gibt keinen Wert zurück, wenn `x` es sich um inkompatible Typen `y` handelt, z. B. eine Zahl und eine Zeichenfolge.
`eq(x, y)`	Gibt 1 zurück, wenn `x` gleich `y` ist, andernfalls `0` (`x == y`). AWS IoT SiteWise betrachtet die Argumente als gleich, wenn sie innerhalb einer relativen Toleranz von liegen`1E-9`. Dies verhält sich ähnlich wie die Funktion isclose in Python. Diese Funktion gibt keinen Wert zurück, wenn `x` es sich um inkompatible Typen `y` handelt, z. B. eine Zahl und eine Zeichenfolge.

Funktion	Beschreibung
`lt(x, y)`	Gibt 1 zurück, wenn x kleiner als y ist, andernfalls `0` (`x < y`). Diese Funktion gibt keinen Wert zurück, wenn x es sich um inkompatible Typen y handelt, z. B. eine Zahl und eine Zeichenfolge.
`lte(x, y)`	Gibt 1 zurück, wenn x kleiner oder gleich y ist, andernfalls `0` (`x ≤ y`). AWS IoT SiteWise betrachtet die Argumente als gleich, wenn sie innerhalb einer relativen Toleranz von liegen`1E-9`. Dies verhält sich ähnlich wie die Funktion isclose in Python. Diese Funktion gibt keinen Wert zurück, wenn x es sich um inkompatible Typen y handelt, z. B. eine Zahl und eine Zeichenfolge.
`isnan(x)`	Gibt zurück`1`, ob gleich x ist`NaN`, andernfalls`0`. Diese Funktion gibt keinen Wert zurück, wenn x es sich um eine Zeichenfolge handelt.

Verwenden von bedingten Funktionen in Formelausdrücken

In Transformationen und Metriken können Sie die folgende Funktion verwenden, um eine Bedingung zu überprüfen und unterschiedliche Ergebnisse zurückzugeben, unabhängig davon, ob die Bedingung als wahr oder falsch ausgewertet wird.

Funktion	Beschreibung
`if(condition, result_if_true, result_if_false)`	Wertet das aus `condition` und gibt zurück, `result_if_true` ob die Bedingung als wahr ausgewertet wird oder `result_if_false`

Funktion	Beschreibung
	ob die Bedingung als wahr ausgewertet wird. `false` `condition` muss eine Zahl sein. Diese Funktion betrachtet `0` eine leere Zeichenfolge als `false` und alles andere (einschließlich`NaN`) als`true`. Boolesche Werte werden in `0` (falsch) und `1` (wahr) umgewandelt. Sie können die Konstante none aus dieser Funktion zurückgeben, um die Ausgabe für eine bestimmte Bedingung zu verwerfen. Das bedeutet, dass Sie Datenpunkte herausfiltern können, die eine Bedingung nicht erfüllen. Weitere Informationen finden Sie unter Datenpunkte filtern. Example Beispiele • `if(0, x, y)`gibt die Variable zurück`y`. • `if(5, x, y)`gibt die Variable zurück`x`. • `if(gt(temp, 300), x, y)` gibt die Variable zurück`x`, wenn die Variable größer als `temp` ist`300`. • `if(gt(temp, 300), temp, none)` gibt die Variable zurück, `temp` wenn sie größer oder gleich ist`300`, oder `none` (kein Wert), wenn sie kleiner als `temp` ist`300`. Es wird empfohlen, UFCS für verschachtelte bedingte Funktionen zu verwenden, bei denen es sich bei einem oder mehreren Argumenten um bedingte Funktionen handelt. Sie können `if(condition, result_if_true)` es verwenden, um eine Bedingung

Funktion	Beschreibung
	und zusätzliche Bedingungen `elif(condition, result_if_true, result_if_false)` auszuwerten. Sie können beispielsweise `if(condition1, result1_if_true).elif(condition2, result2_if_true, result2_if_false)` anstelle von verwenden `if(condition1, result1_if_true, if(condition2, result2_if_true, result2_if_false))` . Sie können auch zusätzliche bedingte Zwischenfunktionen verketten. Sie können beispielsweise mehrere `if` Anweisungen verwenden, `if(condition1, result1_if_true).elif(condition2, result2_if_true).elif(condition3, result3_if_true, result3_if_false)` anstatt sie zu verschachteln, wie `if(condition1, result1_if_true, if(condition2, result2_if_true, if(condition3, result3_if_true result3_if_false)))` z. **Important** Sie müssen es `elif(condition, result_if_true, result_if_false)` mit UFCS verwenden.

Verwenden von Zeichenkettenfunktionen in Formelausdrücken

In Transformationen und Metriken können Sie die folgenden Funktionen verwenden, um mit Zeichenketten zu arbeiten. Weitere Informationen finden Sie unter Verwenden von Zeichenketten in Formeln.

> **Important**
>
> Formelausdrücke können nur Doppel- oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

Funktion	Beschreibung
`len(s)`	Gibt die Länge der Zeichenfolge zurück. `s`
`find(s, substring)`	Gibt den Index der Zeichenfolge `substring` in der Zeichenfolge zurück`s`.
`contains(s, substring)`	Gibt zurück`1`, ob die Zeichenfolge die Zeichenfolge `s` enthält`substring` , andernfalls`0`.
`upper(s)`	Gibt die Zeichenfolge `s` in Großbuchstaben zurück.
`lower(s)`	Gibt die Zeichenfolge `s` in Kleinbuchstaben zurück.
`jp(s, json_path)`	Wertet die Zeichenfolge `s` mit dem JsonPathAusdruck aus `json_path` und gibt das Ergebnis zurück. Verwenden Sie diese Funktion, um Folgendes zu tun:

Funktion	Beschreibung
	• Extrahieren Sie einen Wert, ein Array oder ein Objekt aus einer serialisierten JSON-Struktur. • Konvertiert eine Zeichenfolge in eine Zahl. Die Formel `jp('111', '$')` gibt `111` beispielsweise eine Zahl zurück. Um einen Zeichenkettenwert aus einer JSON-Struktur zu extrahieren und ihn als Zahl zurückzugeben, müssen Sie mehrere verschachtelte `jp` Funktionen verwenden. Die äußere `jp` Funktion extrahiert die Zeichenfolge aus der JSON-Struktur, und die innere `jp` Funktion konvertiert die Zeichenfolge in eine Zahl. Die Zeichenfolge `json_path` muss ein Zeichenfolgenliteral enthalten. Das bedeutet, dass es `json_path` sich nicht um einen Ausdruck handeln kann, der zu einer Zeichenfolge ausgewertet wird. Example Beispiele • `jp('{"status":"active","value":15}', '$.value')` gibt 15 zurück. • `jp('{"measurement":{"reading":25,"confidence":0.95}}', '$.measurement.reading')` gibt 25 zurück. • `jp('[2,8,23]', '$[2]')` gibt 23 zurück. • `jp('{"values":[3,6,7]}', '$.values[1]')` gibt 6 zurück.

Funktion	Beschreibung
	• `jp('111', '$')` gibt `111` zurück. • `jp(jp('{"measurement":{"reading":25,"confidence":"0.95"}}', '$.measurement.confidence'), '$')` gibt `0.95` zurück.
`join(s0, s1, s2, s3, ...)`	Gibt eine verkettete Zeichenfolge mit einem Trennzeichen zurück. Diese Funktion verwendet die erste Eingabezeichenfolge als Trennzeichen und verbindet die verbleibenden Eingabezeichenfolgen miteinander. Dies verhält sich ähnlich wie die Funktion join (CharSequence delimiter, CharSequence... elements) in Java. Example Beispiele • `join("-", "aa", "bb", "cc")`gibt zurück `aa-bb-cc`

Funktion	Beschreibung
`format(expression: "format")` oder `format("format", expression)`	Gibt eine Zeichenfolge im angegebenen Format zurück. Diese Funktion ergibt `expression` einen Wert und gibt den Wert dann im angegebenen Format zurück. Dies verhält sich ähnlich wie die Funktion format (String-Format, Object... args) in Java. Weitere Informationen zu unterstützten Formaten finden Sie unter Konvertierungen unter Class Formatter in der API-Spezifikation für Java Platform, Standard Edition 7. Example Beispiele • `format(100+1: "d")` gibt eine Zeichenfolge zurück,`101`. • `format("The result is %d", 100+1)`gibt eine Zeichenfolge zurück,`The result is 101`.

Funktion	Beschreibung
`f'expression'`	Gibt eine verkettete Zeichenfolge zurück. Mit dieser formatierten Funktion können Sie einen einfachen Ausdruck verwenden, um Zeichenketten zu verketten und zu formatier en. Diese Funktionen können verschachtelte Ausdrücke enthalten. Sie können `{}` (geschwei fte Klammern) verwenden, um Ausdrücke zu interpolieren. Dies verhält sich ähnlich wie die formatierten Zeichenkettenliterale in Python. Example Beispiele • `f'abc{1+2: "f"}d'` gibt `abc3.0000 00d` zurück. Gehen Sie wie folgt vor, um diesen Beispielausdruck auszuwerten: 1. `format(1+2: "f")` gibt eine Fließkommazahl zurück,`3.000000`. 2. `join('', "abc", 1+2, 'd')`gibt eine Zeichenfolge zurück,`abc3.000000d` . Sie können den Ausdruck auch auf folgende Weise schreiben:`join('', "abc", format(1+2: "f"), 'd')` .

Verwenden von Aggregationsfunktionen in Formelausdrücken

Nur in Metriken können Sie die folgenden Funktionen verwenden, um Eingabewerte für jedes Zeitintervall zu aggregieren und einen einzelnen Ausgabewert zu berechnen. Einige Aggregationsfunktionen können keine Daten aus zugeordneten Komponenten aggregieren.

Bei den Argumenten von Aggregationsfunktionen kann es sich um Variablen, Zahlenliterale, zeitliche Funktionen, verschachtelte Ausdrücke oder Aggregationsfunktionen handeln. Die Formel `max(latest(x), latest(y), latest(z))` verwendet eine Aggregationsfunktion als Argument und gibt den größten aktuellen Wert der x Eigenschaften, und zurück. y z

Sie können verschachtelte Ausdrücke in Aggregationsfunktionen verwenden. Wenn Sie verschachtelte Ausdrücke verwenden, gelten die folgenden Regeln:

- Jedes Argument kann nur eine Variable haben.

  Example

  Zum Beispiel `avg(x*(x-1))` und `sum(x/2 )/avg(y^2 )` werden unterstützt.

  Wird beispielsweise `min(x/y)` nicht unterstützt.
- Jedes Argument kann verschachtelte Ausdrücke mit mehreren Ebenen haben.

  Example

  Wird beispielsweise unterstützt`sum(avg(x^2 )/2)`.
- Verschiedene Argumente können unterschiedliche Variablen haben.

  Example

  Zum Beispiel `sum(x/2, y*2)` wird unterstützt.

> **Note**
>
> - Wenn Ihre Ausdrücke Messungen enthalten, AWS IoT SiteWise verwendet die letzten Werte im aktuellen Zeitintervall für die Messungen, um Aggregate zu berechnen.
> - Wenn Ihre Ausdrücke Attribute enthalten, AWS IoT SiteWise verwendet die neuesten Werte für die Attribute, um Aggregate zu berechnen.

Funktion	Beschreibung
`avg(`x_0`, ..., `x_n`)`	Gibt den Mittelwert der angegebenen Variablen werte über das aktuelle Zeitintervall zurück. Diese Funktion gibt nur dann einen Datenpunk t aus, wenn die angegebenen Variablen im aktuellen Zeitintervall mindestens einen Datenpunkt haben.

Funktion	Beschreibung
`sum(x0, ..., xn)`	Gibt die Summe der angegebenen Variablen werte über das aktuelle Zeitintervall zurück. Diese Funktion gibt nur dann einen Datenpunk t aus, wenn die angegebenen Variablen im aktuellen Zeitintervall mindestens einen Datenpunkt haben.
`min(x0, ..., xn)`	Gibt den Mindestwert der angegebenen Variablenwerte über das aktuelle Zeitintervall zurück. Diese Funktion gibt nur dann einen Datenpunk t aus, wenn die angegebenen Variablen im aktuellen Zeitintervall mindestens einen Datenpunkt haben.
`max(x0, ..., xn)`	Gibt den Höchstwert der angegebenen Variablenwerte über das aktuelle Zeitintervall zurück. Diese Funktion gibt nur dann einen Datenpunk t aus, wenn die angegebenen Variablen im aktuellen Zeitintervall mindestens einen Datenpunkt haben.
`count(x0, ..., xn)`	Gibt die Gesamtanzahl der Datenpunkte für die angegebenen Variablen über das aktuelle Zeitintervall zurück. Weitere Informationen zum Zählen der Datenpunkte, die eine Bedingung erfüllen, finden Sie unter Zählen von Datenpunk ten, die einer Bedingung entsprechen. Diese Funktion berechnet einen Datenpunkt für jedes Zeitintervall.

Funktion	Beschreibung
`stdev(`x_0`, ..., `x_n`)`	Gibt die Standardabweichung der Werte der angegebenen Variablen über das aktuelle Zeitintervall zurück. Diese Funktion gibt nur dann einen Datenpunkt aus, wenn die angegebenen Variablen im aktuellen Zeitintervall mindestens einen Datenpunkt haben.

Verwendung von temporalen Funktionen in Formelausdrücken

Verwenden Sie temporale Funktionen, um Werte zurückzugeben, die auf Zeitstempeln von Datenpunkten basieren.

Verwendung temporaler Funktionen in Metriken

Nur in Metriken können Sie die folgenden Funktionen verwenden, die Werte auf der Grundlage von Zeitstempeln von Datenpunkten zurückgeben.

Bei den Argumenten für temporale Funktionen muss es sich um Eigenschaften aus dem lokalen Objektmodell oder um verschachtelte Ausdrücke handeln. Das bedeutet, dass Sie keine Eigenschaften aus untergeordneten Vermögensmodellen in temporalen Funktionen verwenden können.

Sie können verschachtelte Ausdrücke in zeitlichen Funktionen verwenden. Wenn Sie verschachtelte Ausdrücke verwenden, gelten die folgenden Regeln:

- Jedes Argument kann nur eine Variable haben.

  Zum Beispiel `latest( t*9/5 + 32 )` wird unterstützt.
- Argumente können keine Aggregationsfunktionen sein.

  Wird beispielsweise `first( sum(x) )` nicht unterstützt.

Funktion	Beschreibung
`first(x)`	Gibt den Wert der angegebenen Variablen mit dem frühesten Zeitstempel über das aktuelle Zeitintervall hinweg zurück.
`last(x)`	Gibt den Wert der angegebenen Variablen mit dem spätesten Zeitstempel über das aktuelle Zeitintervall hinweg zurück.
`earliest(x)`	Gibt den letzten Wert der angegebenen Variablen vor dem Beginn des aktuellen Zeitintervalls zurück. Diese Funktion berechnet einen Datenpunkt für jedes Zeitintervall, wenn die Eingabeeigenschaft mindestens einen Datenpunkt im Verlauf hat. Details dazu finden Sie unter time-range-defintion.
`latest(x)`	Gibt den letzten Wert der angegebenen Variablen mit dem letzten Zeitstempel vor dem Ende des aktuellen Zeitintervalls zurück. Diese Funktion berechnet einen Datenpunkt für jedes Zeitintervall, wenn die Eingabeeigenschaft mindestens einen Datenpunkt im Verlauf hat. Details dazu finden Sie unter time-range-defintion.
`statetime(x)`	Gibt die Zeitspanne in Sekunden zurück, in der die angegebenen Variablen im aktuellen Zeitintervall positiv sind. Sie können die Vergleichsfunktionen verwenden, um eine Transformationseigenschaft zu erstellen, die von der `statetime` Funktion verwendet werden soll.

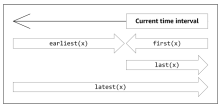
Funktion	Beschreibung
	Wenn Sie beispielsweise eine `Idle`-Eigenschaft haben, für die `0` oder `1` gilt, können Sie die Leerlaufzeit pro Zeitintervall mit diesem Ausdruck berechnen: `IdleTime = statetime(Idle)` . Weitere Informationen finden Sie im Beispielzustandszeitszenario. Diese Funktion unterstützt keine Metrikeigenschaften als Eingabevariablen. Diese Funktion berechnet einen Datenpunkt für jedes Zeitintervall, wenn die Eingabeeigenschaft mindestens einen Datenpunkt im Verlauf hat.

Funktion	Beschreibung
`TimeWeightedAvg(x, [interpolation])`	Gibt den Durchschnitt der Eingabedaten zurück, gewichtet mit Zeitintervallen zwischen Punkten. Einzelheiten zur Berechnung und zu den Intervallen finden Sie unter Parameter für zeitgewichtete Funktionen. Das optionale Argument `interpolaton` muss eine Zeichenkettenkonstante sein: • `locf`— Dies ist die Standardeinstellung. Bei der Berechnung wird der Berechnungsalgorithmus Last Observed Carry Forward für Intervalle zwischen Datenpunkten verwendet. Bei diesem Ansatz wird der Datenpunkt als letzter beobachteter Wert bis zum Zeitstempel des nächsten Eingabedatenpunkts berechnet. Der Wert nach einem guten Datenpunkt wird als Wert bis zum nächsten Datenpunkt-Zeitstempel extrapoliert. • `linear`— Die Berechnung verwendet den Berechnungsalgorithmus der linearen Interpolation für Intervalle zwischen Datenpunkten. Der Wert zwischen zwei guten Datenpunkten wird als lineare Interpolation zwischen den Werten dieser Datenpunkte extrapoliert. Der Wert zwischen guten und schlechten Datenpunkten oder der Wert nach dem letzten guten Datenpunkt wird als guter Datenpunkt extrapoliert.

Funktion	Beschreibung
`TimeWeightedStDev(x, [algo])`	Gibt die Standardabweichung der Eingabeda ten zurück, gewichtet mit Zeitintervallen zwischen Punkten. Einzelheiten zur Berechnung und zu den Intervallen finden Sie unter Parameter für zeitgewichtete Funktionen. Bei der Berechnung wird der Berechnun gsalgorithmus Last Observed Carry Forward für Intervalle zwischen Datenpunkten verwendet . Bei diesem Ansatz wird der Datenpunkt als letzter beobachteter Wert bis zum Zeitstempel des nächsten Eingabedatenpunkts berechnet . Die Gewichtung wird als Zeitintervall in Sekunden zwischen Datenpunkten oder Fenstergrenzen berechnet. Das optionale Argument `algo` muss eine Zeichenkettenkonstante sein: • `f`— Dies ist die Standardeinstellung. Sie gibt eine unvoreingenommene gewichtet e Stichprobenvarianz mit Frequenzg ewichten zurück, die in Sekunden berechnet TimeWeight wird. Dieser Algorithmus wird in der Regel unter Berücksichtigung der Standardabweichung angenommen und wird bei gewichteten Stichproben als Bessel-Ko rrektur der Standardabweichung bezeichnet. • p— Gibt die verzerrte gewichtete Stichprob envarianz zurück, die auch als Populatio nsvarianz bezeichnet wird.

Funktion	Beschreibung
	Die folgenden Formeln werden für Berechnungen verwendet, wobei: • S_p = Standardabweichung der Population • S_f = Frequenzstandardabweichung • X_i = eingehende Daten • ω_i = Gewicht, das dem Zeitintervall in Sekunden entspricht • μ* = ein gewichteter Mittelwert der eingehenden Daten Gleichung für die Standardabweichung der Grundgesamtheit: $$S_p^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i}$$ Gleichung für die Frequenzstandardabweichung: $$S_f^2 = \frac{\sum_{i=1}^{N} \omega_i (x_i - \mu^*)^2}{\sum_{i=1}^{N} \omega_i - 1}$$

Das folgende Diagramm zeigt, wie die zeitlichen Funktionen`first`,, und `last` `earliest``latest`, relativ zum aktuellen Zeitintervall AWS IoT SiteWise berechnet werden.



> **Note**
>
> - Der Zeitraum für`first(x)`, `last(x)` ist (aktueller Fensterstart, aktuelles Fensterende].
> - Der Zeitraum für `latest(x)` ist [Beginn der Zeit, Ende des aktuellen Fensters].
> - Der Zeitraum für `earliest(x)` ist [Beginn der Zeit, Ende des vorherigen Fensters].

Parameter für zeitgewichtete Funktionen

Bei den für das Aggregatfenster berechneten zeitgewichteten Funktionen wird Folgendes berücksichtigt:

- Datenpunkte innerhalb des Fensters
- Zeitintervalle zwischen Datenpunkten
- Letzter Datenpunkt vor dem Fenster
- Erster Datenpunkt nach dem Fenster (für einige Algorithmen)

Bedingungen:

- Schlechter Datenpunkt — Jeder Datenpunkt mit nicht guter Qualität oder schlechtem Zahlenwert. Dies wird bei der Berechnung der Fensterergebnisse nicht berücksichtigt.
- Fehlerhaftes Intervall — Das Intervall nach einem fehlerhaften Datenpunkt. Das Intervall vor dem ersten bekannten Datenpunkt wird ebenfalls als schlechtes Intervall angesehen.
- Guter Datenpunkt — Jeder Datenpunkt mit guter Qualität und numerischem Wert.

> **Note**
>
> - AWS IoT SiteWise verbraucht nur `GOOD` hochwertige Daten, wenn es Transformationen und Metriken berechnet. Es ignoriert alle Datenpunkte. `UNCERTAIN` `BAD`
> - Das Intervall vor dem ersten bekannten Datenpunkt wird als schlechtes Intervall angesehen. Weitere Informationen finden Sie unter the section called “Tutorials zu Formelausdrücken”.

Das Intervall nach dem letzten bekannten Datenpunkt dauert unbegrenzt und wirkt sich auf alle folgenden Fenster aus. Wenn ein neuer Datenpunkt eintrifft, berechnet die Funktion das Intervall neu.

Gemäß den obigen Regeln wird das aggregierte Fensterergebnis berechnet und auf Fenstergrenzen beschränkt. Standardmäßig sendet die Funktion das Fensterergebnis nur, wenn das gesamte Fenster ein gutes Intervall aufweist.

Wenn das Intervall für den Fensterwert kleiner als die Fensterlänge ist, sendet die Funktion das Fenster nicht.

Wenn sich die Datenpunkte, die das Fensterergebnis beeinflussen, ändern, berechnet die Funktion das Fenster neu, auch wenn sich die Datenpunkte außerhalb des Fensters befinden.

Wenn die Eingabeeigenschaft mindestens einen Datenpunkt in ihrer Historie hat und eine Berechnung eingeleitet wurde, berechnet die Funktion die zeitgewichteten Aggregatfunktionen für jedes Zeitintervall.

Example Beispielzustandszeitszenario

Betrachten Sie ein Beispiel mit einer Komponente mit den folgenden Eigenschaften:

- `Idle`— Eine Messung, die oder ist. `0` `1` Wenn der Wert „1“ ist, befindet sich die Maschine im Leerlauf.
- `Idle Time`— Eine Metrik, die anhand der Formel `statetime(Idle)` die Zeit in Sekunden berechnet, in der sich die Maschine im Leerlauf befindet, pro 1-Minuten-Intervall.

Die `Idle`-Eigenschaft verfügt über die folgenden Datenpunkte.

Zeitstempel	14:00:00 Uhr	14:00:30 Uhr	14:01:15 Uhr	14:02:45 Uhr	14:04:00 Uhr
Idle	0	1	1	0	0

AWS IoT SiteWise berechnet die `Idle Time` Eigenschaft jede Minute aus den Werten von`Idle`. Nach Abschluss dieser Berechnung verfügt die `Idle Time`-Eigenschaft über die folgenden Datenpunkte.

Zeitstempel	14:00:00 Uhr	14:01:00 Uhr	14:02:00 Uhr	14:03:00 Uhr	14:04:00 Uhr

Idle Time	N/A	30	60	45	0

AWS IoT SiteWise führt am Ende jeder Minute die folgenden Berechnungen durch. `Idle Time`

- Um 14:00 Uhr (für 13:59 Uhr bis 14:00 Uhr)
  - Vor 14:00 Uhr liegen keine Daten für `Idle` vor, daher wird kein Datenpunkt berechnet.
- Um 14:01 Uhr (für 14:00 Uhr bis 14:01 Uhr)
  - Um 14:00:00 Uhr ist die Maschine aktiv (`Idle` ist `0`).
  - Um 14:00:30 Uhr befindet sich die Maschine im Leerlauf (`Idle` ist `1`).
  - `Idle` ändert sich vor dem Ende des Intervalls um 14:01:00 Uhr nicht mehr, `Idle Time` ist also 30 Sekunden.
- Um 14:02 Uhr (für 14:01 bis 14:02 Uhr)
  - Um 14:01:00 Uhr befindet sich die Maschine im Leerlauf (entsprechend des letzten Datenpunkts um 14:00:30 Uhr).
  - Um 14:01:15 Uhr befindet sich die Maschine noch im Leerlauf.
  - `Idle` ändert sich vor dem Ende des Intervalls um 14:02:00 Uhr nicht mehr, `Idle Time` ist also 60 Sekunden.
- Um 14:03 Uhr (für 14:02 Uhr bis 14:03 Uhr)
  - Um 14:02:00 Uhr befindet sich die Maschine im Leerlauf (entsprechend des letzten Datenpunkts um 14:01:15 Uhr).
  - Um 14:02:45 Uhr ist die Maschine aktiv.
  - `Idle` ändert sich vor dem Ende des Intervalls um 14:03:00 Uhr nicht mehr, `Idle Time` ist also 45 Sekunden.
- Um 14:04 Uhr (für 14:03 Uhr bis 14:04 Uhr)
  - Um 14:03:00 Uhr ist die Maschine aktiv (entsprechend des letzten Datenpunkts um 14:02:45 Uhr).
  - `Idle` ändert sich vor dem Ende des Intervalls um 14:04:00 Uhr nicht mehr, `Idle Time` ist also 0 Sekunden.

Example Beispiel TimeWeightedAvg und TimeWeightedStDev Szenario

Die folgenden Tabellen enthalten Beispieleingaben und -ausgaben für diese einminütigen Fenstermetriken:`Avg(x)`, `TimeWeightedAvg(x)`, `TimeWeightedAvg(x, "linear")`, `stDev(x)`, `timeWeightedStDev(x)`, `timeWeightedStDev(x, 'p')`.

Beispieleingabe für ein einminütiges Aggregatfenster:

> **Note**
>
> Diese Datenpunkte sind alle `GOOD` qualitativ hochwertig.

03:00:00	4,0
03:01:00	2.0
03:01:10	8.0
03:01:50	20.0
03:02:00	14,0
03:02:05	10.0
03:02:10	3.0
03:02:30	20.0
03:03:30	0.0

Ausgabe aggregierter Ergebnisse:

> **Note**
>
> Keine — Für dieses Fenster wurde kein Ergebnis erzeugt.

Zeit	`Avg(x)`	`TimeWeighted Avg(x)`	`TimeWeighted Avg(X, "linear")`	`stDev(X)`	`timeWeighted StDev(x)`	`timeWeighted StDev(x, 'p')`
3:00:00	4	Keine	None	0	Keine	None
3:01:00	2	4	3	0	0	0
3:02:00	14	9	13	6	5,430610041581775	5,385164807134504
3:03:00	11	13	12,875	8,54400374531753	7,724054437220943	7,659416862050705
3:04:00	0	10	2.5	0	10,084389681792215	10
3:05:00	None	0	0	None	0	0

Verwendung temporaler Funktionen in Transformationen

Nur bei Transformationen können Sie die `pretrigger()` Funktion verwenden, um den `GOOD` Qualitätswert für eine Variable vor der Eigenschaftenaktualisierung abzurufen, die die aktuelle Transformationsberechnung ausgelöst hat.

Stellen Sie sich ein Beispiel vor AWS IoT SiteWise , bei dem ein Hersteller den Status einer Maschine überwacht. Der Hersteller verwendet die folgenden Messungen und Transformationen, um den Prozess darzustellen:

- Eine Messung`current_state`, die 0 oder 1 sein kann.
  - Wenn sich die Maschine im Reinigungszustand befindet, `current_state` entspricht dies 1.
  - Wenn sich die Maschine im Fertigungszustand befindet, `current_state` entspricht 0.
- Eine Transformation`cleaning_state_duration`, das entsprichtif`(pretrigger(current_state) == 1, timestamp(current_state) - timestamp(pretrigger(current_state)), none)`. Diese Transformation gibt im Unix-Epochenformat in Sekunden zurück, wie lange sich die Maschine im Reinigungszustand

befunden hat. Weitere Informationen finden Sie unter Verwenden von bedingten Funktionen in Formelausdrücken und zur Funktion timestamp ().

Bleibt das Gerät länger als erwartet im Reinigungszustand, überprüft der Hersteller das Gerät möglicherweise.

Sie können die `pretrigger()` Funktion auch in multivariaten Transformationen verwenden. Sie haben beispielsweise zwei Messungen mit dem Namen `x` und und `y` eine Transformation`z`, die entspricht. `x + y + pretrigger(y)` Die folgende Tabelle zeigt die Werte für `x`y, und `z` von 9:00 Uhr bis 9:15 Uhr.

> **Note**
>
> - In diesem Beispiel wird davon ausgegangen, dass die Werte für die Messungen chronologisch eintreffen. Beispielsweise kommt der Wert `x` für 09:00 Uhr vor dem Wert `x` für 09:05 Uhr an.
> - Wenn die Datenpunkte für 9:05 Uhr vor den Datenpunkten für 9:00 Uhr ankommen, wird um 9:05 Uhr `z` nicht berechnet.
> - Wenn der Wert `x` für 9:05 Uhr vor dem Wert für 09:00 Uhr eintrifft und die Werte `x` für chronologisch `y` eintreffen, `z` entspricht `22 = 20 + 1 + 1` dies um 9:05 Uhr.

	09:00 UHR	09:05 UHR	09:10 UHR	09:15 UHR
`x`	10	20		30
`y`	1	2	3	
`z = x + y + pretrigger(y)`	yempfängt vor 09:00 Uhr keinen Datenpunkt. Wird daher `z` nicht um 09:00 Uhr berechnet.	23 = 20 + 2 + 1 `pretrigger(y)` entspricht 1.	25 = 20 + 3 + 2 `x`empfängt keinen neuen Datenpunkt. `pretrigger(y)` entspricht 2.	36 = 30 + 3 + 3 yempfängt keinen neuen Datenpunkt. Entspricht `pretrigger(y)` also 3 um 09:15 Uhr.

Verwenden von Datums- und Uhrzeitfunktionen in Formelausdrücken

In Transformationen und Metriken können Sie die Datums- und Uhrzeitfunktionen auf folgende Weise verwenden:

- Ruft den aktuellen Zeitstempel eines Datenpunkts in UTC oder in der lokalen Zeitzone ab.
- Konstruieren Sie Zeitstempel mit Argumenten wie `yearmonth`, und. `day_of_month`
- Extrahieren Sie mit dem `unix_time` Argument einen Zeitraum, z. B. ein Jahr oder einen Monat.

Funktion	Beschreibung
`now()`	Gibt das aktuelle Datum und die aktuelle Uhrzeit in Sekunden im Unix-Epochenformat zurück.
`timestamp()`	• Bei Transformationen gibt die Funktion den Zeitstempel der Eingabenachricht in Sekunden im Unix-Epochenformat zurück. Nur bei Transformationen können Sie einen der folgenden Schritte ausführen: • Geben Sie eine Variable als Argument für die Funktion an. Die `timestamp ( variable-name )` Funktion gibt den Zeitstempel des letzten `GOOD` Qualitäts werts für die angegebene Variable in Sekunden im Unix-Epochenformat zurück. Wenn Ihr Asset beispielsweise eine Transformationseigenschaft mit dem Namen hat, die die `9/5 * Temperature_C` Formel verwendet`Temperature_F` , um jeden Temperaturdatenpunkt von Celsius in Fahrenheit umzurechnen, können Sie die `timestamp(Temperature_F)` Funktion verwenden, um den Zeitstempel des neuesten `GOOD` Qualitäts

Funktion	Beschreibung
	werts für die Eigenschaft abzurufen. `Temperature_F` • Verwenden Sie die `pretrigge r()` Funktion als Argument für die Funktion. Die `timestamp(pretrigg er(` *`variable-name`* `))` Funktion gibt den Zeitstempel des `GOOD` Qualitäts werts für die angegebene Variable vor der Eigenschaftenaktualisierung, die die aktuelle Transformationsberechnung ausgelöst hat, in Sekunden im Unix-Epoc henformat zurück. Weitere Informationen finden Sie unter Verwendung temporaler Funktionen in Transformationen. • Bei Metriken gibt die Funktion den am Ende des aktuellen Fensters abgerufen en Zeitstempel in Sekunden im Unix-Epoc henformat zurück.

Funktion	Beschreibung
`mktime(time_zone, year, month, day_of_month, hour, minute, second)`	Gibt die Eingabezeit in Sekunden im Unix-Epoc henformat zurück. Für die Verwendung dieser Funktion gelten die folgenden Anforderungen: • Das Zeitzonenargument muss eine Zeichenfo lge (`'UTC'`) in Anführungszeichen sein. Wenn nicht angegeben, ist die Standardz eitzone UTC. Das Zeitzonenargument kann das erste oder letzte Argument sein. • Die Argumente Jahr, Monat, Tag des Monats, Stunde, Minute und Sekunde müssen in der richtigen Reihenfolge angegeben werden. • Die Argumente Jahr, Monat und Datum sind erforderlich. Für die Verwendung dieser Funktion gelten die folgenden Einschränkungen: • `year`- Gültige Werte liegen zwischen 1970 und 2250. • `month`- Gültige Werte liegen zwischen 1 und 12. • `day-of-month` - Gültige Werte liegen zwischen 1 und 31. • `hour`- Gültige Werte liegen zwischen 0 und 23. • `minute`- Gültige Werte liegen zwischen 0 und 59.

Funktion	Beschreibung
	• `second`- Gültige Werte liegen zwischen 0 und 60. Es kann sich um eine Fließkomm azahl handeln. Beispiele: • `mktime(2020, 2, 29)` • `mktime('UTC+3', 2021, 12, 31, 22)` • `mktime(2022, 10, 13, 2, 55, 13.68, 'PST')`

Funktion	Beschreibung
`localtime(unix_time, time_zone)`	Gibt das Jahr, den Tag des Monats, den Wochentag, den Tag des Jahres, die Stunde, die Minute oder die Sekunde in der angegeben en Zeitzone aus der Unix-Zeit zurück. Für die Verwendung dieser Funktion gelten die folgenden Anforderungen: • Das Zeitzonenargument muss eine Zeichenfo lge (`'UTC'`) in Anführungszeichen sein. Wenn nicht angegeben, ist die Standardz eitzone UTC. • Das Unix-Zeitargument ist die Zeit in Sekunden im Unix-Epochenformat. Der gültige Bereich liegt zwischen 1-3155688 9864403199. Es kann eine Fließkommazahl sein. Beispiel für eine Antwort: `2007-12-0 3T10:15:30+01:00[Europe/Paris]` `localtime(unix_time, time_zone ) ` ist keine eigenständige Funktion. Die `sec()` Funktionen `year() mon()mday,wday(),yday(),hour(),minute()`, und nehmen `localtime(unix_time, time_zone)` als Argument an. Beispiele: • `year(localtime('GMT', 160589860 8.8113723))` • `now().localtime().year()` • `timestamp().localtime('PST' ).year()`

Funktion	Beschreibung
	• `localtime(1605289736, 'Europe/London').year()`
`year(localtime(unix_time, time_zone)`	Gibt das Jahr von zurück`localtime(unix_time, time_zone)` .
`mon(localtime(unix_time, time_zone))`	Gibt den Monat von zurück`localtime(unix_time, time_zone)` .
`mday(localtime(unix_time, time_zone))`	Gibt den Tag des Monats von zurück`localtime(unix_time, time_zone)` .
`wday(localtime(unix_time, time_zone))`	Gibt den Wochentag von zurück`localtime(unix_time, time_zone)` .
`yday(localtime(unix_time, time_zone))`	Gibt den Tag des Jahres von zurück`localtime(unix_time, time_zone)` .
`hour(localtime(unix_time, time_zone))`	Gibt die Stunde von zurück`localtime(unix_time, time_zone)` .
`minute(localtime(unix_time, time_zone))`	Gibt die Minute von zurück`localtime(unix_time, time_zone)` .
`sec(localtime(unix_time, time_zone))`	Gibt die Sekunde von zurück`localtime(unix_time, time_zone)` .

Unterstützte Zeitzonenformate

Sie können das Zeitzonenargument auf folgende Weise angeben:

- Zeitzonen-Offset — Geben Sie `'Z'` UTC oder einen Offset (`'+2'`oder`'-5'`) an.
- Offset-IDs — Kombinieren Sie eine Abkürzung für eine Zeitzone und einen Offset. Beispiel: `'GMT+2'` und `'UTC-01:00'`. Die Abkürzung für die Zeitzone darf nur drei Buchstaben enthalten.
- Regionsbasierte IDs — Zum Beispiel `'Etc/GMT+12'` und`'Pacific/Pago_Pago'`.

Unterstützte Abkürzungen für Zeitzonen

Die Datums- und Uhrzeitfunktionen unterstützen die folgenden aus drei Buchstaben bestehenden Abkürzungen für Zeitzonen:

- AM BESTEN - 05:00 UHR
- DONNERSTAG - - 10:00
- MST - - 07:00
- ACT - Australien/Darwin
- AET - Australien/Sydney
- AGT - Amerika/Argentinien/Buenos_Aires
- KUNST - Afrika/Kairo
- AST - Amerika/Anchorage
- BET - Amerika/Sao_Paulo
- BST - Asien/Dhaka
- CAT - Afrika/Harare
- MEZ - Europa/Paris
- CNT - Amerika/St_Johns
- CST - Amerika/Chicago
- CTT - Asien/Shanghai
- ESSEN - Afrika/Addis_Abeba
- IET - Amerika/Indiana/Indianapolis
- IST - Asien/Kalkutta
- JST - Asien/Tokio
- MIT - Pazifik/Apia
- NET - Asien/Eriwan
- NST - Pazifik/Auckland
- PLT - Asien/Karatschi
- PRT - Amerika/Puerto_Rico
- PST - Amerika/Los_Angeles

- SST - Pazifik/Guadalcanal
- VST - Asien/Ho_Chi_Minh

Unterstützte regionsbasierte IDs

Die Datums- und Uhrzeitfunktionen unterstützen die folgenden regionsbasierten IDs, geordnet nach ihrer Beziehung zu UTC+ 00:00:

- ETC/GMT+12 (UTC-12:00)
- Pazifik/Pago_Pago (UTC- 11:00)
- Pazifik/Samoa (UTC- 11:00)
- Pazifik/Niue (UTC- 11:00)
- USA/Samoa (UTC- 11:00)
- ETC/GMT+11 (UTC-11:00)
- Pazifik/Midway (UTC- 11:00)
- Pazifik/Honolulu (UTC- 10:00)
- Pazifik/Rarotonga (UTC- 10:00)
- Pazifik/Tahiti (UTC- 10:00)
- Pazifik/Johnston (UTC- 10:00)
- USA/Hawaii (UTC- 10:00)
- System V/HST10 (UTC- 10:00)
- ETC/GMT+10 (UTC-10:00)
- Pazifik/Marquesas (UTC- 09:30)
- ETC/GMT+9 (UTC-09:00)
- Pazifik/Gambier (UTC- 09:00)
- Amerika/Atka (UTC- 09:00)
- System V/YST9 (UTC- 09:00)
- Amerika/Adak (UTC- 09:00)
- USA/Aleuten (UTC- 09:00)
- ETC/GMT+8 (UTC-08:00)

- USA/Alaska (UTC- 08:00)
- Amerika/Juneau (UTC- 08:00)
- Amerika/Metlakatla (UTC- 08:00)
- Amerika/Yakutat (UTC- 08:00)
- Pazifik/Pitcairninseln (UTC- 08:00)
- Amerika/Sitka (UTC- 08:00)
- Amerika/Anchorage (UTC- 08:00)
- SystemV/PST8 (UTC- 08:00)
- Amerika/Nome (UTC- 08:00)
- System V/YST9YDT (UTC- 08:00)
- Kanada/Yukon (UTC- 07:00)
- USA/Pazifik-Neu (UTC- 07:00)
- ETC/GMT+7 (UTC-07:00)
- Vereinigte Staaten von Amerika und Arizona (UTC- 07:00)
- Amerika/Dawson_Creek (UTC- 07:00)
- Kanada/Pazifik (UTC- 07:00)
- PST8PDT (UTC-07:00)
- System V/MST7 (UTC- 07:00)
- Amerika/Dawson (UTC- 07:00)
- Mexiko/ (UTC BajaNorte - 07:00)
- Amerika/Tijuana (UTC- 07:00)
- Amerika/Creston (UTC- 07:00)
- Amerika/Hermosillo (UTC- 07:00)
- Amerika/Santa_Isabel (UTC- 07:00)
- Amerika/Vancouver (UTC- 07:00)
- Amerika/Ensenada (UTC- 07:00)
- Amerika/Phoenix (UTC- 07:00)
- Amerika/Whitehorse (UTC- 07:00)

- Amerika/Fort_Nelson (UTC- 07:00)
- SystemV/PST8PDT (UTC- 07:00)
- Amerika/Los_Angeles (UTC- 07:00)
- USA/Pazifik (UTC- 07:00)
- Amerika/El_Salvador (UTC- 06:00)
- Amerika/Guatemala (UTC- 06:00)
- Amerika/Belize (UTC- 06:00)
- Amerika/Managua (UTC- 06:00)
- Amerika/Tegucigalpa (UTC- 06:00)
- ETC/GMT+6 (UTC-06:00)
- Pazifik/Ostern (UTC- 06:00)
- Mexiko/ (UTC- 06:00BajaSur)
- Amerika/Regina (UTC- 06:00)
- Amerika/Denver (UTC- 06:00)
- Pazifik/Galapagos (UTC- 06:00)
- Amerika/Yellowknife (UTC- 06:00)
- Amerika/Swift_Current (UTC- 06:00)
- Amerika/Inuvik (UTC- 06:00)
- Amerika/Mazatlan (UTC- 06:00)
- Amerika/Boise (UTC- 06:00)
- Amerika/Costa_Rica (UTC- 06:00)
- MST7MDT (UTC-06:00)
- SystemV/CST6 (UTC- 06:00)
- Amerika/Chihuahua (UTC- 06:00)
- Amerika/Ojinaga (UTC- 06:00)
- Chile/ EasterIsland (UTC- 06:00)
- USA/Berg (UTC- 06:00)
- Amerika/Edmonton (UTC- 06:00)
- Kanada/Berg (UTC- 06:00)

- Amerika/Cambridge_Bay (UTC- 06:00)
- Navajo (UTC-06:00)
- SystemV/MST7MDT (UTC- 06:00)
- Kanada/Saskatchewan (UTC- 06:00)
- Amerika/Shiprock (UTC- 06:00)
- Amerika/Panama (UTC- 05:00)
- Amerika/Chicago (UTC- 05:00)
- Amerika/Eirunepe (UTC- 05:00)
- ETC/GMT+5 (UTC-05:00)
- Mexiko/Allgemein (UTC- 05:00)
- Amerika/Porto_Acre (UTC- 05:00)
- Amerika/Guayaquil (UTC- 05:00)
- Amerika/Rankin_Inlet (UTC- 05:00)
- USA/Zentral (UTC- 05:00)
- Amerika/Rainy_River (UTC- 05:00)
- Amerika/Indiana/Knox (UTC- 05:00)
- Amerika/North_Dakota/Beulah (UTC- 05:00)
- Amerika/Monterrey (UTC- 05:00)
- Amerika/Jamaika (UTC- 05:00)
- Amerika/Atikokan (UTC- 05:00)
- Amerika/Coral_Harbour (UTC- 05:00)
- Amerika/North_Dakota/Center (UTC- 05:00)
- Amerika/Cayman (UTC- 05:00)
- Amerika/Indiana/Tell_City (UTC- 05:00)
- Amerika/Mexico_City (UTC- 05:00)
- Amerika/Matamoros (UTC- 05:00)
- CST6CDT (UTC-05:00)
- Amerika/Knox_IN (UTC- 05:00)
- Amerika/Bogota (UTC- 05:00)

- Amerika/Menominee (UTC- 05:00)
- Amerika/Resolute (UTC- 05:00)
- System V/EST5 (UTC- 05:00)
- Kanada/Zentral (UTC- 05:00)
- Brasilien/Acre (UTC- 05:00)
- Amerika/Cancun (UTC- 05:00)
- Amerika/Lima (UTC- 05:00)
- Amerika/Bahia_Banderas (UTC- 05:00)
- Vereinigte Staaten von Amerika und Indien (UTC- 05:00)
- Amerika/Rio_Branco (UTC- 05:00)
- SystemV/CST6CDT (UTC- 05:00)
- Jamaika (UTC- 05:00)
- Amerika/Mérida (UTC- 05:00)
- Amerika/North_Dakota/New_Salem (UTC- 05:00)
- Amerika/Winnipeg (UTC- 05:00)
- Amerika/Cuiaba (UTC- 04:00)
- Amerika/Marigot (UTC- 04:00)
- Amerika/Indiana/Petersburg (UTC- 04:00)
- Chile/Kontinental (UTC- 04:00)
- Amerika/Grand_Turk (UTC- 04:00)
- Kuba (UTC- 04:00)
- ETC/GMT+4 (UTC-04:00)
- Amerika/Manaus (UTC- 04:00)
- Amerika/Fort_Wayne (UTC- 04:00)
- Amerika/St_Thomas (UTC- 04:00)
- Amerika/Anguilla (UTC- 04:00)
- Amerika/Havanna (UTC- 04:00)
- USA/Michigan (UTC- 04:00)
- Amerika/Barbados (UTC- 04:00)

- Amerika/Louisville (UTC- 04:00)
- Amerika/Curacao (UTC- 04:00)
- Amerika/Guyana (UTC- 04:00)
- Amerika/Martinique (UTC- 04:00)
- Amerika/Puerto_Rico (UTC- 04:00)
- Amerika/Port_of_Spain (UTC- 04:00)
- SystemV/AST4 (UTC- 04:00)
- Amerika/Indiana/Vevay (UTC- 04:00)
- Amerika/Indiana/Vincennes (UTC- 04:00)
- Amerika/Kralendijk (UTC- 04:00)
- Amerika/Antigua (UTC- 04:00)
- Amerika/Indianapolis (UTC- 04:00)
- Amerika/Iqaluit (UTC- 04:00)
- Amerika/St_Vincent (UTC- 04:00)
- Amerika/Kentucky/Louisville (UTC- 04:00)
- Amerika/Dominica (UTC- 04:00)
- Amerika/Asuncion (UTC- 04:00)
- SAMSTAG 5 EDT (UTC-04:00)
- Amerika/Nassau (UTC- 04:00)
- Amerika/Kentucky/Monticello (UTC- 04:00)
- Brasilien/West (UTC- 04:00)
- Amerika/Aruba (UTC- 04:00)
- Amerika/Indiana/Indianapolis (UTC- 04:00)
- Amerika/Santiago (UTC- 04:00)
- Amerika/La_Paz (UTC- 04:00)
- Amerika/Thunder_Bay (UTC- 04:00)
- Amerika/Indiana/Marengo (UTC- 04:00)
- Amerika/Blanc-Sablon (UTC- 04:00)
- Amerika/Santo_Domingo (UTC- 04:00)

- USA/Ost (UTC- 04:00)
- Kanada/Ost (UTC- 04:00)
- Amerika/Port-au-Prince (UTC- 04:00)
- Amerika/St_Barthelemy (UTC- 04:00)
- Amerika/Nipigon (UTC- 04:00)
- USA/Ost-Indiana (UTC- 04:00)
- Amerika/St_Lucia (UTC- 04:00)
- Amerika/Montserrat (UTC- 04:00)
- Amerika/Lower_Princes (UTC- 04:00)
- Amerika/Detroit (UTC- 04:00)
- Amerika/Tortola (UTC- 04:00)
- Amerika/Porto_Velho (UTC- 04:00)
- Amerika/Campo_Grande (UTC- 04:00)
- Amerika/Virgin (UTC- 04:00)
- Amerika/Pangnirtung (UTC- 04:00)
- Amerika/Montreal (UTC- 04:00)
- Amerika/Indiana/Winamac (UTC- 04:00)
- Amerika/Boa_Vista (UTC- 04:00)
- Amerika/Grenada (UTC- 04:00)
- Amerika/New_York (UTC- 04:00)
- Amerika/St_Kitts (UTC- 04:00)
- Amerika/Caracas (UTC- 04:00)
- Amerika/Guadeloupe (UTC- 04:00)
- Amerika/Toronto (UTC- 04:00)
- SystemV/EST5EDT (UTC- 04:00)
- Amerika/Argentinien/Catamarca (UTC- 03:00)
- Kanada/Atlantik (UTC- 03:00)
- Amerika/Argentinien/Cordoba (UTC- 03:00)

- Amerika/Araguaina (UTC- 03:00)
- Amerika/Argentinien/Salta (UTC- 03:00)
- ETC/GMT+3 (UTC-03:00)
- Amerika/Montevideo (UTC- 03:00)
- Brasilien/Ost (UTC- 03:00)
- Amerika/Argentinien/Mendoza (UTC- 03:00)
- Amerika/Argentinien/Rio_Gallegos (UTC- 03:00)
- Amerika/Catamarca (UTC- 03:00)
- Amerika/Cordoba (UTC- 03:00)
- Amerika/Sao_Paulo (UTC- 03:00)
- Amerika/Argentinien/Jujuy (UTC- 03:00)
- Amerika/Cayenne (UTC- 03:00)
- Amerika/Recife (UTC- 03:00)
- Amerika/Buenos_Aires (UTC- 03:00)
- Amerika/Paramaribo (UTC- 03:00)
- Amerika/Moncton (UTC- 03:00)
- Amerika/Mendoza (UTC- 03:00)
- Amerika/Santarem (UTC- 03:00)
- Atlantik/Bermuda (UTC- 03:00)
- Amerika/Maceio (UTC- 03:00)
- Atlantik/Stanley (UTC- 03:00)
- Amerika/Halifax (UTC- 03:00)
- Antarktis/Rothera (UTC- 03:00)
- Amerika/Argentinien/San_Luis (UTC- 03:00)
- Amerika/Argentinien/Ushuaia (UTC- 03:00)
- Antarktis/Palmer (UTC- 03:00)
- Amerika/Punta_Arenas (UTC- 03:00)
- Amerika/Glace_Bay (UTC- 03:00)

- Amerika/Fortaleza (UTC- 03:00)
- Amerika/Thule (UTC- 03:00)
- Amerika/Argentinien/La_Rioja (UTC- 03:00)
- Amerika/Belem (UTC- 03:00)
- Amerika/Jujuy (UTC- 03:00)
- Amerika/Bahia (UTC- 03:00)
- Amerika/Goose_Bay (UTC- 03:00)
- Amerika/Argentinien/San_Juan (UTC- 03:00)
- Amerika/Argentinien/ ComodRivadavia (UTC- 03:00)
- Amerika/Argentinien/Tucuman (UTC- 03:00)
- Amerika/Rosario (UTC- 03:00)
- SystemV/AST4ADT (UTC- 03:00)
- Amerika/Argentinien/Buenos_Aires (UTC- 03:00)
- Amerika/St_Johns (UTC- 02:30)
- Kanada/Neufundland (UTC- 02:30)
- Amerika/Miquelon (UTC- 02:00)
- ETC/GMT+2 (UTC-02:00)
- Amerika/Godthab (UTC- 02:00)
- Amerika/Noronha (UTC- 02:00)
- DeNoronha Brasilien/ (UTC- 02:00)
- Atlantik/Südgeorgien (UTC- 02:00)
- ETC/GMT+1 (UTC-01:00)
- Atlantik/Kap Verde (UTC- 01:00)
- Pazifik/Kiritimati (UTC+ 14:00)
- ETC/GMT-14 (UTC+ 14:00)
- Pazifik/Fakaofo (UTC+ 13:00)
- Pazifik/Enderbury (UTC+ 13:00)
- Pazifik/Apia (UTC+ 13:00)
- Pazifik/Tongatapu (UTC+ 13:00)

- ETC/GMT-13 (UTC+ 13:00)
- NZ-CHAT (UTC+ 12:45)
- Pazifik/Chatham (UTC+ 12:45)
- Pazifik/Kwajalein (UTC+ 12:00)
- Antarktis/ McMurdo (UTC+ 12:00)
- Pazifik/Wallis (UTC+ 12:00)
- Pazifik/Fidschi (UTC+ 12:00)
- Pazifik/Funafuti (UTC+ 12:00)
- Pazifik/Nauru (UTC+ 12:00)
- Kwajalein (UTC+ 12:00)
- NEUSEELAND (UTC+ 12:00)
- Pazifik/Wake (UTC+ 12:00)
- Antarktis/Südpol (UTC+ 12:00)
- Pazifik/Tarawa (UTC+ 12:00)
- Pazifik/Auckland (UTC+ 12:00)
- Asien/Kamtschatka (UTC+ 12:00)
- ETC/GMT-12 (UTC+ 12:00)
- Asien/Anadyr (UTC+ 12:00)
- Pazifik/Majuro (UTC+ 12:00)
- Pazifik/Ponape (UTC+ 11:00)
- Pazifik/Bougainville (UTC+ 11:00)
- Antarktis/Macquarie (UTC+ 11:00)
- Pazifik/Pohnpei (UTC+ 11:00)
- Pazifik/Efate (UTC+ 11:00)
- Pazifik/Norfolk (UTC+ 11:00)
- Asien/Magadan (UTC+ 11:00)
- Pazifik/Kosrae (UTC+ 11:00)
- Asien/Sachalin (UTC+ 11:00)
- Pazifik/Noumea (UTC+ 11:00)

- ETC/GMT-11 (UTC+ 11:00)
- Asien/Srednekolymsk (UTC+ 11:00)
- Pazifik/Guadalcanal (UTC+ 11:00)
- Australien/Lord_Howe (UTC+ 10:30)
- Australien/LHI (UTC+ 10:30)
- Australien/Hobart (UTC+ 10:00)
- Pazifik/Yap (UTC+ 10:00)
- Australien/Tasmanien (UTC+ 10:00)
- Pazifik/Port_Moresby (UTC+ 10:00)
- Australien/ACT (UTC+ 10:00)
- Australien/Victoria (UTC+ 10:00)
- Pazifik/Chuuk (UTC+ 10:00)
- Australien/Queensland (UTC+ 10:00)
- Australien/Canberra (UTC+ 10:00)
- Australien/Currie (UTC+ 10:00)
- Pazifik/Guam (UTC+ 10:00)
- Pazifik/Truk (UTC+ 10:00)
- Australien/NSW (UTC+ 10:00)
- Asien/Wladiwostok (UTC+ 10:00)
- Pazifik/Saipan (UTC+ 10:00)
- Antarktis/Dumont-Durville (UTC+ 10:00)
- Australien/Sydney (UTC+ 10:00)
- Australien/Brisbane (UTC+ 10:00)
- ETC/GMT-10 (UTC+ 10:00)
- Asien/Ust-Nera (UTC+ 10:00)
- Australien/Melbourne (UTC+ 10:00)
- Australien/Lindeman (UTC+ 10:00)
- Australien/Norden (UTC+ 09:30)
- Australien/Yancowinna (UTC+ 09:30)

- Australien/Adelaide (UTC+ 09:30)
- Australien/Broken_Hill (UTC+ 09:30)
- Australien/Süden (UTC+ 09:30)
- Australien/Darwin (UTC+ 09:30)
- ETC/GMT-9 (UTC+ 09:00)
- Pazifik/Palau (UTC+ 09:00)
- Asien/Chita (UTC+ 09:00)
- Asien/Dili (UTC+ 09:00)
- Asien/Jayapura (UTC+ 09:00)
- Asien/Jakutsk (UTC+ 09:00)
- Asien/Pjöngjang (UTC+ 09:00)
- ROCK (UTC+ 09:00)
- Asien/Seoul (UTC+ 09:00)
- Asien/Khandyga (UTC+ 09:00)
- Japan (UTC+ 09:00)
- Asien/Tokio (UTC+ 09:00)
- Australien/Eucla (UTC+ 08:45)
- Asien/Kuching (UTC+ 08:00)
- Asien/Chungking (UTC+ 08:00)
- ETC/GMT-8 (UTC+ 08:00)
- Australien/Perth (UTC+ 08:00)
- Asien/Macau (UTC+ 08:00)
- Asien/Macau (UTC+ 08:00)
- Asien/Choibalsan (UTC+ 08:00)
- Asien/Shanghai (UTC+ 08:00)
- Antarktis/Casey (UTC+ 08:00)
- Asien/Ulan_Bator (UTC+ 08:00)
- Asien/Chongqing (UTC+ 08:00)
- Asien/Ulaanbaatar (UTC+ 08:00)

- Asien/Taipeh (UTC+ 08:00)
- Asien/Manila (UTC+ 08:00)
- PRC (UTC+ 08:00)
- Asien/Ujung_Pandang (UTC+ 08:00)
- Asien/Harbin (UTC+ 08:00)
- Singapur (UTC+ 08:00)
- Asien/Brunei (UTC+ 08:00)
- Australien/West (UTC+ 08:00)
- Asien/Hong_Kong (UTC+ 08:00)
- Asien/Makassar (UTC+ 08:00)
- Hongkong (UTC+ 08:00)
- Asien/Kuala_Lumpur (UTC+ 08:00)
- Asien/Irkutsk (UTC+ 08:00)
- Asien/Singapur (UTC+ 08:00)
- Asien/Pontianak (UTC+ 07:00)
- ETC/GMT-7 (UTC+ 07:00)
- Asien/Phnom_Penh (UTC+ 07:00)
- Asien/Nowosibirsk (UTC+ 07:00)
- Antarktis/Davis (UTC+ 07:00)
- Asien/Tomsk (UTC+ 07:00)
- Asien/Jakarta (UTC+ 07:00)
- Asien/Barnaul (UTC+ 07:00)
- Indisch/Weihnachten (UTC+ 07:00)
- Asien/Ho_Chi_Minh (UTC+ 07:00)
- Asien/Hovd (UTC+ 07:00)
- Asien/Bangkok (UTC+ 07:00)
- Asien/Vientiane (UTC+ 07:00)
- Asien/Nowokusnezk (UTC+ 07:00)
- Asien/Krasnojarsk (UTC+ 07:00)

- Asien/Saigon (UTC+ 07:00)
- Asien/Rangun (UTC+ 06:30)
- Asien/Rangun (UTC+ 06:30)
- Indisch/Cocos (UTC+ 06:30)
- Asien/Kashgar (UTC+ 06:00)
- ETC/GMT-6 (UTC+ 06:00)
- Asien/Almaty (UTC+ 06:00)
- Asien/Dacca (UTC+ 06:00)
- Asien/Omsk (UTC+ 06:00)
- Asien/Dhaka (UTC+ 06:00)
- Indisch/Chagos (UTC+ 06:00)
- Asien/Qyzylorda (UTC+ 06:00)
- Asien/Bischkek (UTC+ 06:00)
- Antarktis/Wostok (UTC+ 06:00)
- Asien/Urumqi (UTC+ 06:00)
- Asien/Thimbu (UTC+ 06:00)
- Asien/Thimphu (UTC+ 06:00)
- Asien/Kathmandu (UTC+ 05:45)
- Asien/Katmandu (UTC+ 05:45)
- Asien/Kalkutta (UTC+ 05:30)
- Asien/Colombo (UTC+ 05:30)
- Asien/Kalkutta (UTC+ 05:30)
- Asien/Aktau (UTC+ 05:00)
- ETC/GMT-5 (UTC+ 05:00)
- Asien/Samarkand (UTC+ 05:00)
- Asien/Karatschi (UTC+ 05:00)
- Asien/Jekaterinburg (UTC+ 05:00)
- Asien/Duschanbe (UTC+ 05:00)
- Indien/Malediven (UTC+ 05:00)

- Asien/Oral (UTC+ 05:00)
- Asien/Taschkent (UTC+ 05:00)
- Antarktis/Mawson (UTC+ 05:00)
- Asien/Aktobe (UTC+ 05:00)
- Asien/Ashkhabad (UTC+ 05:00)
- Asien/Aschgabat (UTC+ 05:00)
- Asien/Atyrau (UTC+ 05:00)
- Indisch/Kerguelen (UTC+ 05:00)
- Iran (UTC+ 04:30)
- Asien/Teheran (UTC+ 04:30)
- Asien/Kabul (UTC+ 04:30)
- Asien/Eriwan (UTC+ 04:00)
- ETC/GMT-4 (UTC+ 04:00)
- ETC/GMT-4 (UTC+ 04:00)
- Asien/Dubai (UTC+ 04:00)
- Indisch/Reunion (UTC+ 04:00)
- Europa/Saratow (UTC+ 04:00)
- Europa/Samara (UTC+ 04:00)
- Indisch/Mahe (UTC+ 04:00)
- Asien/Baku (UTC+ 04:00)
- Asien/Muscat (UTC+ 04:00)
- Europa/Wolgograd (UTC+ 04:00)
- Europa/Astrachan (UTC+ 04:00)
- Asien/Tiflis (UTC+ 04:00)
- Europa/Uljanowsk (UTC+ 04:00)
- Asien/Aden (UTC+ 03:00)
- Afrika/Nairobi (UTC+ 03:00)
- Europa/Istanbul (UTC+ 03:00)
- ETC/GMT-3 (UTC+ 03:00)

- Europa/Zaporozhye (UTC+ 03:00)
- Israel (UTC+ 03:00)
- Indisch/Komoren (UTC+ 03:00)
- Antarktis/Syowa (UTC+ 03:00)
- Afrika/Mogadischu (UTC+ 03:00)
- Europa/Bukarest (UTC+ 03:00)
- Afrika/Asmera (UTC+ 03:00)
- Europa/Mariehamn (UTC+ 03:00)
- Asien/Istanbul (UTC+ 03:00)
- Europa/Tiraspol (UTC+ 03:00)
- Europa/Moskau (UTC+ 03:00)
- Europa/Chisinau (UTC+ 03:00)
- Europa/Helsinki (UTC+ 03:00)
- Asien/Beirut (UTC+ 03:00)
- Asien/Tel_Aviv (UTC+ 03:00)
- Afrika/Dschibuti (UTC+ 03:00)
- Europa/Simferopol (UTC+ 03:00)
- Europa/Sofia (UTC+ 03:00)
- Asien/Gaza (UTC+ 03:00)
- Afrika/Asmara (UTC+ 03:00)
- Europa/Riga (UTC+ 03:00)
- Asien/Bagdad (UTC+ 03:00)
- Asien/Damaskus (UTC+ 03:00)
- Afrika/Dar_es_Salaam (UTC+ 03:00)
- Afrika/Addis_Abeba (UTC+ 03:00)
- Europa/Uzhgorod (UTC+ 03:00)
- Asien/Jerusalem (UTC+ 03:00)
- Asien/Riad (UTC+ 03:00)
- Asien/Kuwait (UTC+ 03:00)

- Europa/Kirow (UTC+ 03:00)
- Afrika/Kampala (UTC+ 03:00)
- Europa/Minsk (UTC+ 03:00)
- Asien/Katar (UTC+ 03:00)
- Europa/Kiew (UTC+ 03:00)
- Asien/Bahrain (UTC+ 03:00)
- Europa/Vilnius (UTC+ 03:00)
- Indien/Antananarivo (UTC+ 03:00)
- Indien/Mayotte (UTC+ 03:00)
- Europa/Tallinn (UTC+ 03:00)
- Türkei (UTC+ 03:00)
- Afrika/Juba (UTC+ 03:00)
- Asien/Nikosia (UTC+ 03:00)
- Asien/Famagusta (UTC+ 03:00)
- J-SO (UTC+ 03:00)
- FÜSSE (UTC+ 03:00)
- Asien/Hebron (UTC+ 03:00)
- Asien/Amman (UTC+ 03:00)
- Europa/Nikosia (UTC+ 03:00)
- Europa/Athen (UTC+ 03:00)
- Afrika/Kairo (UTC+ 02:00)
- Afrika/Mbabane (UTC+ 02:00)
- Europa/Brüssel (UTC+ 02:00)
- Europa/Warschau (UTC+ 02:00)
- MEZ (UTC+ 02:00)
- Europa/Luxemburg (UTC+ 02:00)
- ETC/GMT-2 (UTC+ 02:00)
- Libyen (UTC+ 02:00)
- Afrika/Kigali (UTC+ 02:00)

- Afrika/Tripolis (UTC+ 02:00)
- Europa/Kaliningrad (UTC+ 02:00)
- Afrika/Windhoek (UTC+ 02:00)
- Europa/Malta (UTC+ 02:00)
- Europa/Busingen (UTC+ 02:00)
-
- Europa/Skopje (UTC+ 02:00)
- Europa/Sarajevo (UTC+ 02:00)
- Europa/Rom (UTC+ 02:00)
- Europa/Zürich (UTC+ 02:00)
- Europa/Gibraltar (UTC+ 02:00)
- Afrika/Lubumbashi (UTC+ 02:00)
- Europa/Vaduz (UTC+ 02:00)
- Europa/Ljubljana (UTC+ 02:00)
- Europa/Berlin (UTC+ 02:00)
- Europa/Stockholm (UTC+ 02:00)
- Europa/Budapest (UTC+ 02:00)
- Europa/Zagreb (UTC+ 02:00)
- Europa/Paris (UTC+ 02:00)
- Afrika/Ceuta (UTC+ 02:00)
- Europa/Prag (UTC+ 02:00)
- Antarktis/Troll (UTC+ 02:00)
- Afrika/Gaborone (UTC+ 02:00)
- Europa/Kopenhagen (UTC+ 02:00)
- Europa/Wien (UTC+ 02:00)
- Europa/Tirane (UTC+ 02:00)
- GETROFFEN (UTC+ 02:00)
- Europa/Amsterdam (UTC+ 02:00)
- Afrika/Maputo (UTC+ 02:00)

- Europa/San_Marino (UTC+ 02:00)
- Polen (UTC+ 02:00)
- Europa/Andorra (UTC+ 02:00)
- Europa/Oslo (UTC+ 02:00)
- Europa/Podgorica (UTC+ 02:00)
- Afrika/Bujumbura (UTC+ 02:00)
- Atlantik/Jan_Mayen (UTC+ 02:00)
- Afrika/Maseru (UTC+ 02:00)
- Europa/Madrid (UTC+ 02:00)
- Afrika/Blantyre (UTC+ 02:00)
- Afrika/Lusaka (UTC+ 02:00)
- Afrika/Harare (UTC+ 02:00)
- Afrika/Khartum (UTC+ 02:00)
- Afrika/Johannesburg (UTC+ 02:00)
- Europa/Belgrad (UTC+ 02:00)
- Europa/Bratislava (UTC+ 02:00)
- Arktis/Longyearbyen (UTC+ 02:00)
- Ägypten (UTC+ 02:00)
- Europa/Vatikan (UTC+ 02:00)
- Europa/Monaco (UTC+ 02:00)
- Europa/London (UTC+ 01:00)
- ETC/GMT-1 (UTC+ 01:00)
- Europa/Jersey (UTC+ 01:00)
- Europa/Guernsey (UTC+ 01:00)
- Europa/Isle_of_Man (UTC+ 01:00)
- Afrika/Tunis (UTC+ 01:00)
- Afrika/Malabo (UTC+ 01:00)
- Großbritannien (UTC+ 01:00)
- Afrika/Lagos (UTC+ 01:00)

- Afrika/Algier (UTC+ 01:00)
- GB (UTC+ 01:00)
- Portugal (UTC+ 01:00)
- Afrika/Sao_Tome (UTC+ 01:00)
- Afrika/Ndjamena (UTC+ 01:00)
- Atlantik/Färöer (UTC+ 01:00)
- Irland (UTC+ 01:00)
- Atlantik/Färöer (UTC+ 01:00)
- Europa/Dublin (UTC+ 01:00)
- Afrika/Libreville (UTC+ 01:00)
- Afrika/El_Aaiun (UTC+ 01:00)
- Afrika/El_Aaiun (UTC+ 01:00)
- Afrika/Douala (UTC+ 01:00)
- Afrika/Brazzaville (UTC+ 01:00)
- Afrika/Porto Novo (UTC+ 01:00)
- Atlantik/Madeira (UTC+ 01:00)
- Europa/Lissabon (UTC+ 01:00)
- Atlantik/Kanarische Inseln (UTC+ 01:00)
- Afrika/Casablanca (UTC+ 01:00)
- Europa/Belfast (UTC+ 01:00)
- Afrika/Luanda (UTC+ 01:00)
- Afrika/Kinshasa (UTC+ 01:00)
- Afrika/Bangui (UTC+ 01:00)
- NASS (UTC+ 01:00)
- Afrika/Niamey (UTC+ 01:00)
- GMT (UTC+ 00:00)
- ETC/GMT-0 (UTC+ 00:00)
- Atlantik/St_Helena (UTC+ 00:00)
- ETC/GMT+0 (UTC+ 00:00)

- Afrika/Banjul (UTC+ 00:00)
- ETC/GMT (UTC+ 00:00)
- Afrika/Freetown (UTC+ 00:00)
- Afrika/Bamako (UTC+ 00:00)
- Afrika/Conakry (UTC+ 00:00)
- Universell (UTC+ 00:00)
- Afrika/Nouakchott (UTC+ 00:00)
- UTC (UTC+ 00:00)
- /etc/Universell (UTC+ 00:00)
- Atlantik/Azoren (UTC+ 00:00)
- Afrika/Abidjan (UTC+ 00:00)
- Afrika/Accra (UTC+ 00:00)
- ETC/UTC (UTC+ 00:00)
- GMT0 (UTC+ 00:00)
- Zulu (UTC+ 00:00) Zulu (UTC+ 00:00)
- Afrika/Ouagadougou (UTC+ 00:00)
- Atlantik/Reykjavik (UTC+ 00:00)
- etC/Zulu (UTC+ 00:00)
- Island (UTC+ 00:00)
- Afrika/Lome (UTC+ 00:00)
- Greenwich (UTC+ 00:00)
- ETC/GMT0 (UTC+ 00:00)
- Amerika/Danmarkshavn (UTC+ 00:00)
- Afrika/Dakar (UTC+ 00:00)
- Afrika/Bissau (UTC+ 00:00)
- ETC/Greenwich (UTC+ 00:00)
- Afrika/Timbuktu (UTC+ 00:00)
- UTC (UTC+ 00:00)
- Afrika/Monrovia (UTC+ 00:00)

- ETC/UTC (UTC+ 00:00)

Tutorials zu Formelausdrücken

Sie können diesen Anleitungen folgen, um Formelausdrücke in zu verwenden. AWS IoT SiteWise

Themen

- Verwenden von Zeichenketten in Formeln
- Datenpunkte filtern
- Zählen von Datenpunkten, die einer Bedingung entsprechen
- Späte Daten in Formeln
- Datenqualität in Formeln
- Undefinierte, unendliche und Überlaufwerte

Verwenden von Zeichenketten in Formeln

Sie können mit Zeichenketten in Ihren Formelausdrücken arbeiten. Sie können auch Zeichenketten aus Variablen eingeben, die auf Attribut- und Messeigenschaften verweisen.

> **Important**
>
> Formelausdrücke können nur Doppel- oder Zeichenkettenwerte ausgeben. Verschachtelte Ausdrücke können andere Datentypen ausgeben, z. B. Zeichenfolgen, aber die Formel als Ganzes muss eine Zahl oder Zeichenfolge ergeben. Sie können die Funktion jp verwenden, um eine Zeichenfolge in eine Zahl umzuwandeln. Der boolesche Wert muss 1 (wahr) oder 0 (falsch) sein. Weitere Informationen finden Sie unter Undefinierte, unendliche und Überlaufwerte.

AWS IoT SiteWise stellt die folgenden Funktionen für Formelausdrücke bereit, mit denen Sie Zeichenfolgen bearbeiten können:

- Zeichenkettenliterale
- Der Indexoperator () `s[index]`
- Der Slice-Operator (`s[start:end:step]`)

- Vergleichsfunktionen, mit denen Sie Zeichenketten in lexikografischer Reihenfolge vergleichen können
- Zeichenkettenfunktionen, zu denen auch die `jp` Funktion gehört, die serialisierte JSON-Objekte analysieren und Zeichenketten in Zahlen konvertieren kann

Datenpunkte filtern

Sie können die if-Funktion verwenden, um Datenpunkte herauszufiltern, die eine Bedingung nicht erfüllen. Die `if` Funktion wertet eine Bedingung aus und gibt unterschiedliche Werte `true` und `false` Ergebnisse zurück. Sie können die Konstante none als Ausgabe für einen Fall einer `if` Funktion verwenden, um den Datenpunkt für diesen Fall zu verwerfen.

Um Datenpunkte herauszufiltern, die einer Bedingung entsprechen

- Erstellen Sie eine Transformation, die die `if` Funktion verwendet, um eine Bedingung zu definieren, die prüft, ob eine Bedingung erfüllt ist, und entweder den `result_if_false` Wert `result_if_true` oder zurückgibt`none`.

Example Beispiel: Filtert Datenpunkte heraus, an denen das Wasser nicht kocht

Stellen Sie sich ein Szenario vor, in dem Sie eine Messung durchführen`temp_c`, die die Temperatur (in Celsius) des Wassers in einer Maschine angibt. Sie können die folgende Transformation definieren, um Datenpunkte herauszufiltern, an denen das Wasser nicht kocht:

- Transformation: `boiling_temps = if(gte(temp_c, 100), temp_c, none)` — Gibt die Temperatur zurück, wenn sie größer oder gleich 100 Grad Celsius ist, andernfalls wird kein Datenpunkt zurückgegeben.

Zählen von Datenpunkten, die einer Bedingung entsprechen

Sie können Vergleichsfunktionen und sum () verwenden, um die Anzahl der Datenpunkte zu zählen, für die eine Bedingung zutrifft.

Um Datenpunkte zu zählen, die einer Bedingung entsprechen

1. Erstellen Sie eine Transformation, die eine Vergleichsfunktion verwendet, um eine Filterbedingung für eine andere Eigenschaft zu definieren.
2. Erstellen Sie eine Metrik, die die Datenpunkte summiert, für die diese Bedingung erfüllt ist.

Example Beispiel: Zählen Sie die Anzahl der Datenpunkte, bei denen Wasser kocht

Stellen Sie sich ein Szenario vor, in dem Sie über eine Messung verfügen`temp_c`, die die Temperatur (in Celsius) des Wassers in einer Maschine angibt. Sie können die folgenden Transformations- und Metrikeigenschaften definieren, um die Anzahl der Datenpunkte zu zählen, bei denen das Wasser kocht:

- Transformation: `is_boiling = gte(temp_c, 100)` — Gibt zurück, 1 ob die Temperatur größer oder gleich 100 Grad Celsius ist, andernfalls wird zurückgegeben`0`.
- Metrisch: `boiling_count = sum(is_boiling)` — Gibt die Anzahl der Datenpunkte zurück, an denen Wasser kocht.

Späte Daten in Formeln

AWS IoT SiteWise unterstützt die späte Datenaufnahme von Daten, die bis zu 7 Tage alt sind. Wenn verspätete Daten AWS IoT SiteWise empfangen werden, werden vorhandene Werte für jede Metrik neu berechnet, die die verspäteten Daten in einem vergangenen Fenster eingibt. Diese Neuberechnungen führen zu Gebühren für die Datenverarbeitung.

> **Note**
>
> Bei der AWS IoT SiteWise Berechnung von Eigenschaften, die verspätete Daten eingeben, wird der aktuelle Formelausdruck jeder Eigenschaft verwendet.

Nachdem ein vergangenes Fenster für eine Metrik AWS IoT SiteWise neu berechnet wurde, ersetzt es den vorherigen Wert für dieses Fenster. Wenn Sie Benachrichtigungen für diese Metrik aktiviert haben, wird AWS IoT SiteWise auch eine Benachrichtigung über den Eigenschaftswert ausgegeben. Dies bedeutet, dass Sie eine neue Benachrichtigung zum Aktualisieren von Eigenschaftswerten für dieselbe Eigenschaft und denselben Zeitstempel erhalten können, für die Sie zuvor bereits eine Benachrichtigung erhalten haben. Wenn Ihre Anwendungen oder Data Lakes Eigenschaftswertbenachrichtigungen verwenden, müssen Sie den vorherigen Wert mit dem neuen Wert aktualisieren, damit die Daten weiterhin korrekt sind.

Datenqualität in Formeln

AWS IoT SiteWise In hat jeder Datenpunkt einen Qualitätscode, der einer der folgenden sein kann:

- `GOOD`— Die Daten sind von keinen Problemen betroffen.

- `BAD`— Die Daten sind von einem Problem wie einem Sensorausfall betroffen.
- `UNCERTAIN`— Die Daten sind von einem Problem wie einer Sensorungenauigkeit betroffen.

AWS IoT SiteWise verbraucht bei der Berechnung von Transformationen und Metriken nur `GOOD` hochwertige Daten. AWS IoT SiteWise gibt nur `GOOD` Qualitätsdaten für erfolgreiche Berechnungen aus. Wenn eine Berechnung nicht erfolgreich ist, wird AWS IoT SiteWise kein Datenpunkt für diese Berechnung ausgegeben. Dies kann auftreten, wenn eine Berechnung zu einem undefinierten, unendlichen oder Überlaufwert führt.

Weitere Informationen zum Abfragen von Daten und zum Filtern nach Datenqualität finden Sie unter Daten abfragen von AWS IoT SiteWise.

Undefinierte, unendliche und Überlaufwerte

Einige Formelausdrücke (wie `x / 0`sqrt(-1), oderlog(0)) berechnen Werte, die in einem reellen Zahlensystem undefiniert, unendlich oder außerhalb des von unterstützten Bereichs liegen. AWS IoT SiteWise Wenn der Ausdruck einer Anlageneigenschaft einen undefinierten, unendlichen Wert oder einen Überlaufwert berechnet, wird AWS IoT SiteWise kein Datenpunkt für diese Berechnung ausgegeben.

AWS IoT SiteWise gibt auch keinen Datenpunkt aus, wenn ein nicht numerischer Wert als Ergebnis eines Formelausdrucks berechnet wird. Das bedeutet, dass, wenn Sie eine Formel definieren, die eine Zeichenfolge, ein Array oder die Konstante none berechnet, AWS IoT SiteWise kein Datenpunkt für diese Berechnung ausgegeben wird.

Example Beispiele

Jeder der folgenden Formelausdrücke führt zu einem Wert, der nicht als Zahl dargestellt AWS IoT SiteWise werden kann. AWS IoT SiteWise gibt bei der Berechnung dieser Formelausdrücke keinen Datenpunkt aus.

- `x / 0`ist undefiniert.
- `log(0)`ist undefiniert.
- `sqrt(-1)`ist in einem reellen Zahlensystem undefiniert.
- `"hello" + " world"`ist eine Zeichenfolge.
- `jp('{"values":[3,6,7]}', '$.values')`ist ein Array.
- `if(gte(temp, 300), temp, none)`ist none wann `temp` ist weniger als`300`.

Erstellen von benutzerdefinierten Verbundmodellen (Komponenten)

Benutzerdefinierte Verbundmodelle oder Komponenten, wenn Sie die Konsole verwenden, bieten eine weitere Organisationsebene für Ihre Asset- und Komponentenmodelle. Sie können sie verwenden, um Ihre Modelle zu strukturieren, indem Sie Eigenschaften gruppieren oder auf andere Modelle verweisen. Weitere Informationen zum Arbeiten mit benutzerdefinierten Verbundmodellen finden Sie unter. Benutzerdefinierte zusammengesetzte Modelle (Komponenten)

Sie erstellen ein benutzerdefiniertes Verbundmodell innerhalb eines vorhandenen Objekt- oder Komponentenmodells. Es gibt zwei Arten von benutzerdefinierten Verbundmodellen. Um verwandte Eigenschaften innerhalb eines Modells zu gruppieren, können Sie ein benutzerdefiniertes Verbundmodell erstellen. Um in Ihrem Objekt- oder Komponentenmodell auf ein Komponentenmodell zu verweisen, können Sie ein auf einem Komponentenmodell basierendes benutzerdefiniertes Verbundmodell erstellen.

In den folgenden Abschnitten wird beschrieben, wie Sie mithilfe der AWS IoT SiteWise API benutzerdefinierte Verbundmodelle erstellen.

Themen

Erstellen einer Inline-Komponente (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um eine Inline-Komponente zu erstellen, die ihre eigenen Eigenschaften definiert.

> **Note**
>
> Da es sich um eine Inline-Komponente handelt, gelten diese Eigenschaften nur für das aktuelle Asset-Modell und werden nirgendwo anders gemeinsam genutzt.
> Wenn Sie ein wiederverwendbares Modell erstellen müssen (z. B. um mehrere Objektmodelle gemeinsam zu nutzen oder um mehrere Instanzen in ein Objektmodell einzubeziehen), sollten Sie stattdessen eine Komponente erstellen, die auf einem Komponentenmodell basiert. Einzelheiten finden Sie im folgenden Abschnitt.

Um eine Komponente (Konsole) zu erstellen

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das Asset-Modell aus, zu dem Sie eine Komponente hinzufügen möchten.
4. Wählen Sie auf der Registerkarte Eigenschaften die Option Komponenten aus.
5. Wählen Sie Komponente erstellen.
6. Gehen Sie auf der Seite Komponente erstellen wie folgt vor:

    a. Geben Sie einen Namen für die Komponente ein, z. B. **`ServoMotor`** oder**`ServoMotor Model`**. Dieser Name muss für alle Komponenten in Ihrem Konto in dieser Region eindeutig sein.

    b. (Optional) Fügen Sie Attributdefinitionen für das Modell hinzu. Attribute stellen Informationen dar, die sich selten ändern. Weitere Informationen finden Sie unter Definition statischer Daten (Attribute).

    c. (Optional) Fügen Sie Messungsdefinitionen für das Modell hinzu. Messungen stellen Datenströme von Ihren Geräten dar. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).

    d. (Optional) Fügen Sie Transformationsdefinitionen für das Modell hinzu. Transformationen sind Formeln, die Daten von einem Formular auf ein anderes abbilden. Weitere Informationen finden Sie unter Daten transformieren (transformiert).

    e. (Optional) Fügen Sie Metrik-Definitionen für das Modell hinzu. Metriken sind Formeln, die Daten über Zeitintervalle aggregieren. Mit Metriken können Daten aus zugehörigen Anlagen eingegeben werden, sodass Sie Werte berechnen können, die Ihren Betrieb oder einen Teil Ihres Betriebs repräsentieren. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

    f. Wählen Sie Komponente erstellen.

Erstellen eines benutzerdefinierten Inline-Verbundmodells (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein benutzerdefiniertes Inline-Verbundmodell zu erstellen, das seine eigenen Eigenschaften definiert.

Verwenden Sie die Operation CreateAssetModelCompositeModel, um ein Inline-Modell mit Eigenschaften zu erstellen. Diese Operation erwartet eine Nutzlast mit der folgenden Struktur.

> **Note**
>
> Da es sich um ein zusammengesetztes Inline-Modell handelt, gelten diese Eigenschaften nur für das aktuelle Anlagenmodell und werden nirgendwo anders verwendet. Was es „inline“ macht, ist, dass es keinen Wert für das `composedAssetModelId` Feld bereitstellt.
> Wenn Sie ein wiederverwendbares Modell erstellen müssen (z. B. um es von mehreren Asset-Modellen gemeinsam zu nutzen oder um mehrere Instanzen in ein Asset-Modell einzubeziehen), sollten Sie stattdessen ein auf einem Komponentenmodell basierendes Verbundmodell erstellen. Einzelheiten finden Sie im folgenden Abschnitt.

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "assetModelCompositeModelProperties": [
        {
            "dataType": "DOUBLE",
            "name": "Servo Motor Temperature",
            "type": {
            "measurement": {}
            },
            "unit": "Celsius"
        },
        {
            "dataType": "DOUBLE",
            "name": "Spindle speed",
            "type": {
            "measurement": {}
            },
            "unit": "rpm"
        }
    ]
}
```

Eine component-model-based Komponente (Konsole) erstellen

Sie können die AWS IoT SiteWise Konsole verwenden, um eine Komponente zu erstellen, die auf einem Komponentenmodell basiert.

Um eine component-model-based Komponente (Konsole) zu erstellen

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das Asset-Modell aus, zu dem Sie eine Komponente hinzufügen möchten.
4. Wählen Sie auf der Registerkarte Eigenschaften die Option Komponenten aus.
5. Wählen Sie Komponente erstellen.
6. Gehen Sie auf der Seite Komponente erstellen wie folgt vor:

   a. Wählen Sie das Komponentenmodell aus, auf dem die Komponente basieren soll.

   b. Geben Sie einen Namen für die Komponente ein, z. B. **`ServoMotor`** oder**`ServoMotor Model`**. Dieser Name muss für alle Komponenten in Ihrem Konto in dieser Region eindeutig sein.

   c. Wählen Sie Komponente erstellen aus.

Erstellen eines component-model-based benutzerdefinierten Verbundmodells (AWS CLI)

Sie können das verwenden AWS CLI , um ein component-model-based benutzerdefiniertes Verbundmodell innerhalb Ihres Asset-Modells zu erstellen. Ein component-model-based benutzerdefiniertes Verbundmodell ist ein Verweis auf ein Komponentenmodell, das Sie bereits an anderer Stelle definiert haben.

Verwenden Sie die Operation CreateAssetModelCompositeModell, um ein component-model-based benutzerdefiniertes Verbundmodell zu erstellen. Diese Operation erwartet eine Nutzlast mit der folgenden Struktur.

> **Note**
>
> In diesem Beispiel `composedAssetModelId` ist der Wert von die Objektmodell-ID oder die externe ID eines vorhandenen Komponentenmodells. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch. Ein Beispiel für die Erstellung eines Komponentenmodells finden Sie unterErstellen eines Komponentenmodells (AWS CLI).

```
{
    "assetModelCompositeModelName": "CNCLathe_ServoMotorA",
    "assetModelCompositeModelType": "CUSTOM",
    "composedAssetModelId": component model ID
]
```

Da es sich nur um eine Referenz handelt, hat ein component-model-based benutzerdefiniertes Verbundmodell außer einem Namen keine eigenen Eigenschaften.

Wenn Sie Ihrem Objektmodell mehrere Exemplare derselben Komponente hinzufügen möchten (z. B. eine CNC-Maschine mit mehreren Servomotoren), können Sie mehrere component-model-based benutzerdefinierte Verbundmodelle hinzufügen, die jeweils einen eigenen Namen haben, aber alle auf denselben Namen verweisen`composedAssetModelId`.

Sie können Komponenten innerhalb anderer Komponenten verschachteln. Dazu können Sie einem Ihrer Komponentenmodelle ein component-model-based zusammengesetztes Modell hinzufügen, wie in diesem Beispiel gezeigt.

Erstellen von Komponenten

Sie können eine Komponente aus einem Komponentenmodell erstellen. Sie müssen über ein Komponentenmodell verfügen, bevor Sie eine Komponente erstellen können. Wenn Sie noch kein Komponentenmodell erstellt haben, beachten Sie die Informationen im Abschnitt Erstellen von Komponentenmodellen.

> **Note**
>
> Sie können nur Komponenten anhand von Modellen mit dem Status `ACTIVE` erstellen. Wenn der Status Ihres Modells nicht `ACTIVE` lautet, müssen Sie möglicherweise einige Minuten warten, bevor Sie Komponenten von diesem Modell ausgehend erstellen können. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Themen

- Erstellen einer Komponente (Konsole)
- Ein Asset erstellen (AWS CLI)
- Konfigurieren einer neuen Komponente

Erstellen einer Komponente (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um eine Anlage zu erstellen.

So erstellen Sie eine Komponente (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie dann Create asset (Komponente erstellen) aus.
4. Gehen Sie auf der Seite Komponente erstellen wie folgt vor:

   a. Wählen Sie unter Modell das Komponentenmodell aus, aus dem eine Komponente erstellt werden soll.

   > **Note**
   >
   > Wenn Ihr Modell nicht AKTIV, ist, müssen Sie warten, bis es aktiv ist, oder Probleme beheben, wenn es FEHLGESCHLAGEN ist.

   b. Geben Sie unter Name einen Namen für Ihre Komponente ein.

   c. (Optional) Fügen Sie Tags für Ihre Komponente hinzu. Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.

   d. Wählen Sie dann Create asset (Komponente erstellen) aus.

   Wenn Sie ein Asset erstellen, navigiert die AWS IoT SiteWise Konsole zur Seite des neuen Assets. Auf dieser Seite sehen Sie den Status der Komponente, der anfänglich WIRD ERSTELLT lautet. Diese Seite wird automatisch aktualisiert. Sie können daher einfach abwarten, bis der Status der Komponente aktualisiert wird.

   > **Note**
   >
   > Die Komponentenerstellung kann bis zu einer Minute dauern. Wenn der Status AKTIV ist, können Sie Aktualisierungsvorgänge für Ihr Asset durchführen. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Nachdem Sie eine Komponente erstellt haben, finden Sie weitere Informationen unter Konfigurieren einer neuen Komponente.

Ein Asset erstellen (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um eine Anlage aus einem Anlagenmodell zu erstellen.

Sie müssen über eine `assetModelId` verfügen, um eine Komponente zu erstellen. Wenn Sie ein Asset-Modell erstellt haben, es aber nicht kennen`assetModelId`, verwenden Sie die ListAsset Models-API, um all Ihre Asset-Modelle anzuzeigen.

Verwenden Sie die CreateAssetAPI mit den folgenden Parametern, um ein Asset aus einem Asset-Modell zu erstellen:

- `assetName`— Der Name des neuen Assets. Geben Sie Ihrem Asset einen Namen, damit Sie es leichter identifizieren können.
- `assetModelId`— Die ID des Vermögenswerts. Dies ist die tatsächliche ID im UUID-Format, oder die, `externalId:myExternalId` falls sie eine hat. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Um ein Asset zu erstellen ()AWS CLI

- Führen Sie den folgenden Befehl aus, um eine Komponente zu erstellen. Ersetzen Sie *`Asset-Name`* durch einen Namen für das Asset und *`Asset-Model-ID durch die ID`* oder die externe ID des Asset-Modells.

  ```
  aws iotsitewise create-asset \
    --asset-name asset-name \
    --asset-model-id asset-model-id
  ```

  Die Operation gibt eine Antwort zurück, in der die Angaben und der Status der neuen Komponente im folgenden Format enthalten sind.

  ```
  {
    "assetId": "String",
    "assetArn": "String",
    "assetStatus": {
      "state": "String",
  ```

```
    "error": {
      "code": "String",
      "message": "String"
    }
  }
}
```

Der `state` der Komponente ist `CREATING`, bis die Komponente erstellt wird.

> **Note**
>
> Die Komponentenerstellung kann bis zu einer Minute dauern. Um den Status Ihres Assets zu überprüfen, verwenden Sie den DescribeAssetVorgang mit der ID Ihres Assets als Parameter. `assetId` Sobald das Asset fertig `state` ist`ACTIVE`, können Sie Aktualisierungsvorgänge an Ihrem Asset durchführen. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Nachdem Sie eine Komponente erstellt haben, finden Sie weitere Informationen unter Konfigurieren einer neuen Komponente.

Konfigurieren einer neuen Komponente

Beenden Sie die Konfiguration Ihrer Komponente mit den folgenden optionalen Aktionen:

- Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften, wenn Ihre Komponente über Messeigenschaften verfügt.
- Aktualisieren von Attributwerten, wenn Ihre Komponente über eindeutige Attributwerte verfügt.
- Zuordnen und Aufheben der Zuordnung von Komponenten, wenn Ihre Komponente eine übergeordnete Komponente ist.

Nach Anlagen suchen

Verwenden Sie die AWS-IoT-SiteWise-Konsole Suchfunktion, um Objekte anhand von Metadaten und Echtzeitfiltern für Eigenschaftswerte zu finden.

Voraussetzungen

AWS IoT SiteWise erfordert Genehmigungen für die Integration von Industriedaten AWS IoT TwinMaker , um sie besser organisieren und modellieren zu können. Wenn Sie Berechtigungen dafür erteilt haben AWS IoT SiteWise, verwenden Sie die ExecuteQueryAPI. Wenn Sie noch keine Berechtigungen erteilt haben und Hilfe bei den AWS IoT SiteWise ersten Schritten benötigen, finden Sie weitere Informationen unterIntegration von AWS IoT SiteWise und AWS IoT TwinMaker.

Erweiterte Suche auf AWS-IoT-SiteWise-Konsole

Suche nach Metadaten

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich unter Assets die Option Erweiterte Suche aus.
3. Wählen Sie unter Erweiterte Suche die Option Metadatensuche aus.
4. Füllen Sie die Parameter aus. Füllen Sie für eine effiziente Suche so viele Felder wie möglich aus.

    a. Assetname — Geben Sie einen vollständigen Asset-Namen oder einen Teil des Namens für eine umfassende Suche ein.

    b. Eigenschaftsname — Geben Sie einen vollständigen oder einen Teil des Namens für eine umfassende Suche ein.

    c. Operator — Wählen Sie einen Operator aus:

    - **=**
    - **<**
    - **>**
    - **<=**
    - **>=**

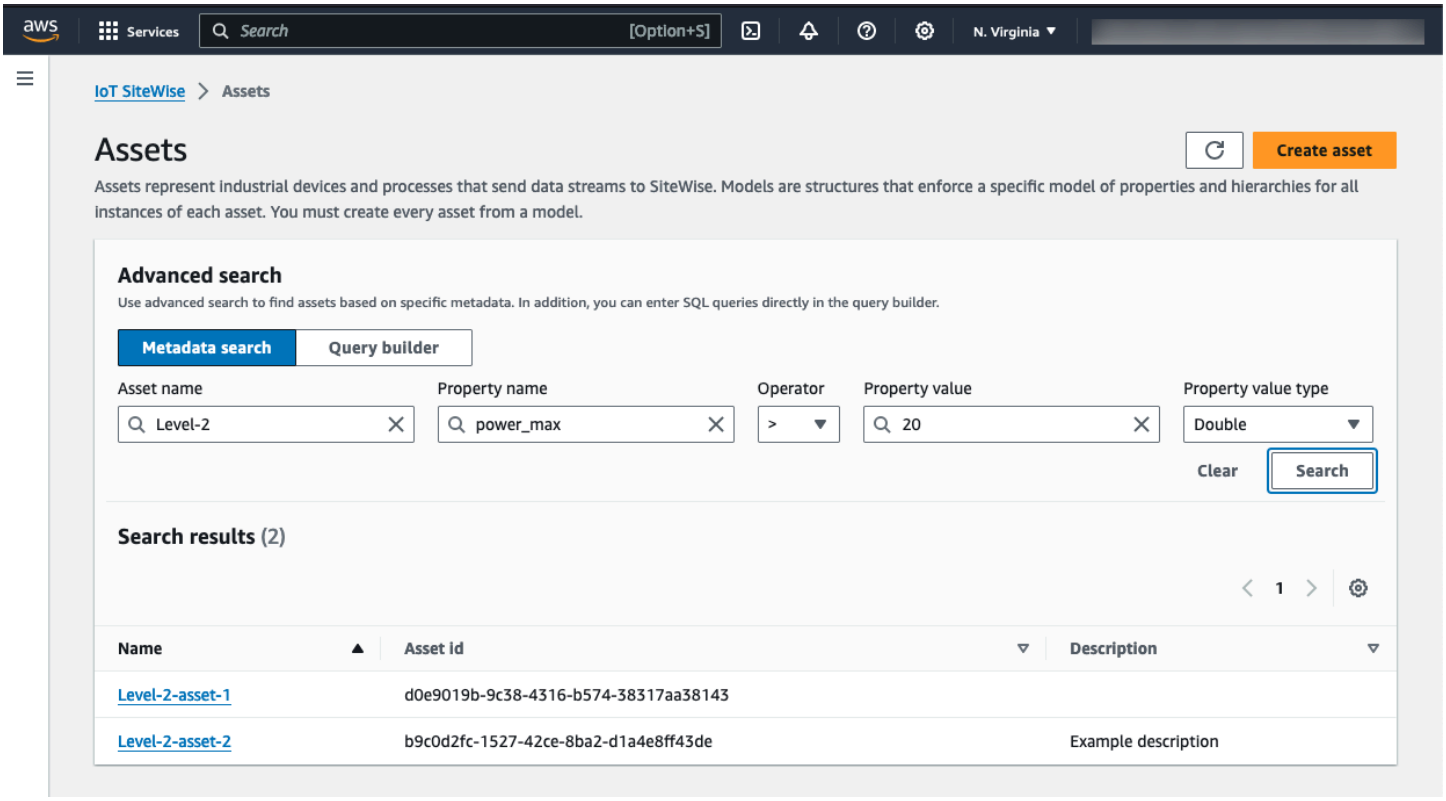
    d. Immobilienwert — Dieser Wert wird mit dem aktuellen Wert der Immobilie verglichen.

    e. Eigenschaftswerttyp — Der Datentyp der Eigenschaft. Wählen Sie eine der folgenden Optionen aus:

    - Doppelt
    - Ganzzahl
    - Zeichenfolge

- Boolesch

5. Wählen Sie Search (Suchen) aus.
6. Wählen Sie in der Tabelle mit den Suchergebnissen das Asset aus der Spalte Name aus. Dadurch gelangen Sie zur detaillierten Asset-Seite für dieses Asset.



Partial search (Partielle Suche)

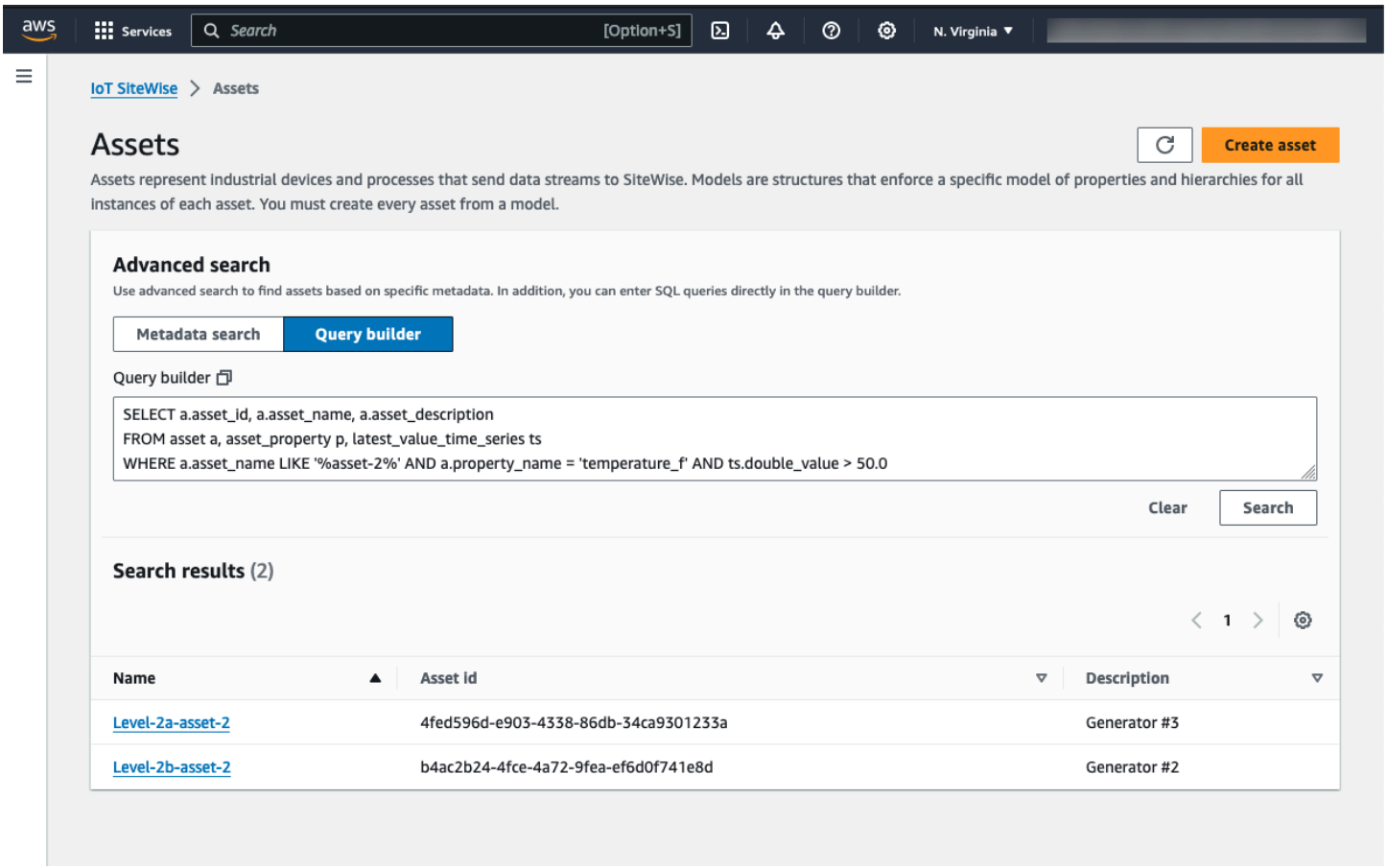
Für eine Asset-Suche müssen nicht alle Parameter angegeben werden. Hier sind einige Beispiele für partielle Suchen mit der Metadatensuchoption:

- Finden Sie Assets anhand ihres Namens:
  - Geben Sie einen Wert nur in das Feld Assetname ein.
  - Die Felder Eigenschaftsname und Eigenschaftswert sind leer.
- Suchen Sie nach Assets, die Eigenschaften mit einem bestimmten Namen enthalten:
  - Geben Sie einen Wert nur in das Feld Eigenschaftsname ein.
  - Die Felder „Assetname“ und „Eigenschaftswert“ sind leer.
- Finden Sie Vermögenswerte anhand der neuesten Werte ihrer Eigenschaften:

- Geben Sie Werte in die Felder Eigenschaftsname und Eigenschaftswert ein.
- Wählen Sie einen Operator und einen Eigenschaftswerttyp aus.

Suche im Query Builder

1. Navigieren Sie zur AWS-IoT-SiteWise-Konsole.
2. Wählen Sie im Navigationsbereich unter Assets die Option Erweiterte Suche aus.
3. Wählen Sie unter Erweiterte Suche die Option Query Builder aus.
4. Schreiben Sie im Bereich Query Builder Ihre SQL-Abfrage, um ein`asset_name`, `asset_id` und abzurufen`asset_description`.
5. Wählen Sie Search (Suchen) aus.
6. Wählen Sie in der Tabelle mit den Suchergebnissen das Asset aus der Spalte Name aus. Dadurch gelangen Sie zur detaillierten Asset-Seite für dieses Asset.



Note

- Die `SELECT` Klausel in der SQL-Abfrage muss die `asset_id` Felder `asset_name` und enthalten, um sicherzustellen, dass die Tabelle mit den Suchergebnissen ein gültiges Asset enthält.
- Der Abfrage-Generator zeigt in der Ergebnistabelle nur den Namen, die Asset-ID und die Beschreibung an. Durch das Hinzufügen weiterer Felder zur `SELECT` Klausel werden der Ergebnistabelle keine weiteren Spalten hinzugefügt

Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften

Sie können einen Eigenschaftsalias für eine Anlageeigenschaft definieren. Auf diese Weise können Sie eine Anlageneigenschaft identifizieren, wenn Sie Anlagendaten aufnehmen oder abrufen. Wenn Ihr Asset über Messeigenschaften verfügt, können Sie die Eigenschaftsaliase definieren, um Ihre Datenströme diesen Messeigenschaften zuzuordnen.

Für diesen Vorgang müssen Sie den Aliasnamen Ihrer Immobilie kennen.

- Wenn Sie Daten von OPC-UA-Servern mithilfe einer OPC-UA-Datenquelle in einem SiteWise Edge-Gateway aufnehmen, ist Ihr Eigenschaftsalias der Pfad zu einer Variablen unter dem Objektknoten, beginnend mit. `/`

  Example

  Wenn der Pfad zu Ihrer Variablen lautet, dann ist Ihr `company/windfarm/3/turbine/7/temperature` Eigenschaftsalias. `/company/windfarm/3/turbine/7/temperature`

  Weitere Informationen zur OPC-UA-Informationsarchitektur finden Sie unter Informationsmodell und Zuordnung von Adressabständen in der OPC UA Online Reference.

  Hinweise

  - Wenn Sie ein Datenstrompräfix für Ihre OPC-UA-Quelle konfigurieren, müssen Sie dieses Präfix in den Eigenschaftenalias für alle Datenströme aus dieser Quelle aufnehmen.

Example

Wenn `/RentonWA` es ein Präfix ist, dann ist es der vorherige Alias. `/RentonWA/company/windfarm/3/turbine/7/temperature`

- Eigenschaftsaliase können bis zu 1.000 Byte enthalten. OPC-UA-Variablenpfade können bis zu 4.096 Byte enthalten. Unterstützt derzeit AWS IoT SiteWise nicht das Einlesen von Daten aus OPC-UA-Variablen mit langen Pfaden.

- Wenn Sie Daten von Modbus-Servern mithilfe einer Modbus-TCP-Datenquelle in einem SiteWise Edge-Gateway aufnehmen, lautet Ihr Eigenschaftsalias:

  Modbus `register set tag name`

  Verwenden Sie diesen Wert, um Daten aus diesem Registersatz an eine Anlageneigenschaft zu senden.

- Wenn Sie Daten aus anderen Quellen aufnehmen, z. B. mithilfe von AWS IoT Regeln oder der API, müssen Sie Ihre Eigenschafts-Aliase definieren. Sie können ein Benennungssystem für Eigenschaftenalias definieren, das auf Ihre Gerätekonfiguration anwendbar ist. Wenn Sie beispielsweise Daten aus AWS IoT -Dingen aufnehmen, können Sie den Namen der Sache in Eigenschaftenaliasnamen aufnehmen, um Datenströme eindeutig zu identifizieren. Weitere Informationen zu diesem Beispiel finden Sie im Tutorial Daten aus AWS IoT Dingen aufnehmen.

Aliase für Immobilien müssen innerhalb einer Region und AWS eines Kontos eindeutig sein. AWS IoT SiteWise gibt einen Fehler zurück, wenn Sie als Eigenschaftsalias einen Alias angeben, der bereits in einer anderen Vermögenseigenschaft vorhanden ist.

Wenn Sie über mehrere OPC-UA-Quellen mit identischen Datenstream-Pfaden verfügen, fügen Sie den Pfaden jeder Quelle ein Präfix hinzu, um eindeutige Aliase zu bilden. Weitere Informationen finden Sie unter Konfigurieren von Datenquellen.

> **Note**
>
> In diesem Abschnitt wird beschrieben, wie Eigenschaftsaliase für Messeigenschaften festgelegt werden. Weitere Informationen zum Festlegen von Eigenschaftsaliasnamen für externe Alarmstatuseigenschaften finden Sie unter. Zuordnung externer Alarmzustandsströme

Themen

Festlegen eines Eigenschaftenalias (Konsole)

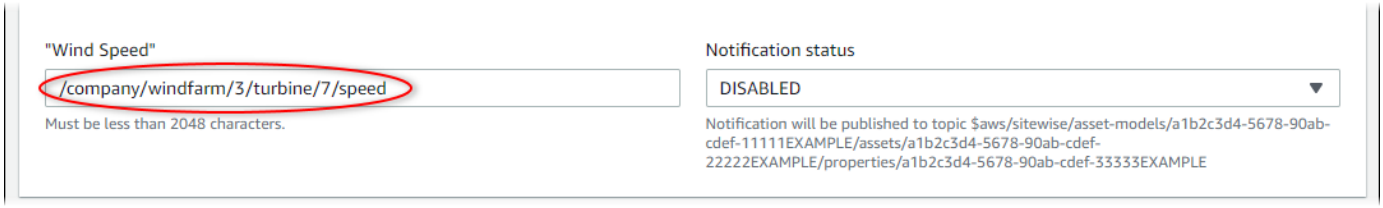
Sie können die AWS IoT SiteWise Konsole verwenden, um einen Alias für eine Anlageneigenschaft festzulegen.

So legen Sie einen Eigenschaftenalias fest (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die Komponente aus, für die Sie einen Eigenschaftenalias festlegen möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Suchen Sie die Eigenschaft, für die Sie einen Alias festlegen möchten, und geben Sie dann den Eigenschaftenalias ein.



6. Wählen Sie Speichern.

Einen Eigenschaftsalias einrichten (AWS CLI)

Verwenden Sie AWS Command Line Interface (AWS CLI), um einen Alias für eine Anlageneigenschaft festzulegen.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie

ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

Verwenden Sie die Operation „UpdateAssetImmobilien“, um der Immobilie Ihrer Anlage einen Datenstrom zuzuordnen. Geben Sie die folgenden Parameter an:

- `assetId`— Die ID oder externe ID des Assets. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- `propertyId`— Die ID oder externe ID der Asset-Immobilie.
- `propertyAlias`— Der Pfad des Datenstroms zum Alias für die Eigenschaft.
- `propertyNotificationState`— Status der Benachrichtigung über den Eigenschaftswert: `ENABLED` oder`DISABLED`. Geben Sie den vorhandenen Benachrichtigungsstatus der Eigenschaft an, wenn Sie den Eigenschaftenalias aktualisieren. Sie können den vorhandenen Benachrichtigungsstatus mit der Operation „DescribeAssetEigenschaft“ abrufen.

  Wenn Sie diesen Parameter auslassen, ist der neue Benachrichtigungsstatus `DISABLED`. Weitere Informationen zu Eigenschaftenbenachrichtigungen finden Sie unter Interaktion mit anderen AWS Diensten.

Um einen Eigenschaftsalias (AWS CLI) festzulegen

1. Führen Sie den folgenden Befehl aus, um den aktuellen Benachrichtigungsstatus der Eigenschaft abzurufen. Ersetzen Sie *`asset-id`* und *`property-id`* durch die IDs der Komponenteneigenschaft.

   ```
   aws iotsitewise describe-asset-property \
     --asset-id asset-id \
     --property-id property-id
   ```

   Die Operation gibt eine Antwort zurück, die Informationen zur Komponenteneigenschaft im folgenden Format enthält. Der Benachrichtigungsstatus der Eigenschaft befindet sich in `assetProperty.notification.state` im JSON-Objekt.

   ```
   {
     "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
     "assetName": "Wind Turbine 7",
     "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
   ```

```
  "assetProperty": {
    "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "name": "Wind Speed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "ENABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

2. Führen Sie den folgenden Befehl aus, um den Alias der Komponenteneigenschaft festzulegen. Ersetzen Sie *property-alias* durch den Eigenschaftenalias und *notification-state* durch den Benachrichtigungsstatus, oder lassen Sie `--property-notification-state` weg, um Benachrichtigungen zu deaktivieren. Sie können optional die Einheit des Assets mit einer neuen *Einheit* und aktualisieren`--property-unit`.

```
aws iotsitewise update-asset-property \
  --asset-id asset-id \
  --property-id property-id \
  --property-alias property-alias \
  --property-notification-state notification-state \
  --property-unit unit
```

3. Um zu überprüfen, ob der Alias festgelegt wurde, führen Sie den folgenden Befehl aus, um die Details der Immobilie abzurufen. Ersetzen Sie *asset-id* und *property-id* durch die IDs der Komponenteneigenschaft.

```
aws iotsitewise describe-asset-property \
  --asset-id asset-id \
  --property-id property-id
```

   Die Operation gibt eine Antwort zurück, die Informationen zur Komponenteneigenschaft im folgenden Format enthält. Der Eigenschaftsalias befindet sich `assetProperty.alias` im JSON-Objekt und ist `myAlias` in diesem Beispiel auf festgelegt.

```
{
  "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
  "assetName": "Wind Turbine 7",
  "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
  "assetProperty": {
    "alias": "myAlias",
    "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
    "name": "Wind Speed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "ENABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

Aktualisieren von Attributwerten

Komponenten übernehmen die Attribute ihres Komponentenmodells, einschließlich des Standardwerts des Attributs. In bestimmten Fällen möchten Sie u. U. das Standardattribut des Komponentenmodells beibehalten, z. B. für die Eigenschaft des Komponentenherstellers. In anderen Fällen möchten Sie u. U. das übernommene Attribut aktualisieren, beispielsweise für den Breiten- und Längengrad einer Komponente.

Updating an attribute value (console)

Sie können die AWS IoT SiteWise Konsole verwenden, um den Wert einer Attribut-Asset-Eigenschaft zu aktualisieren.

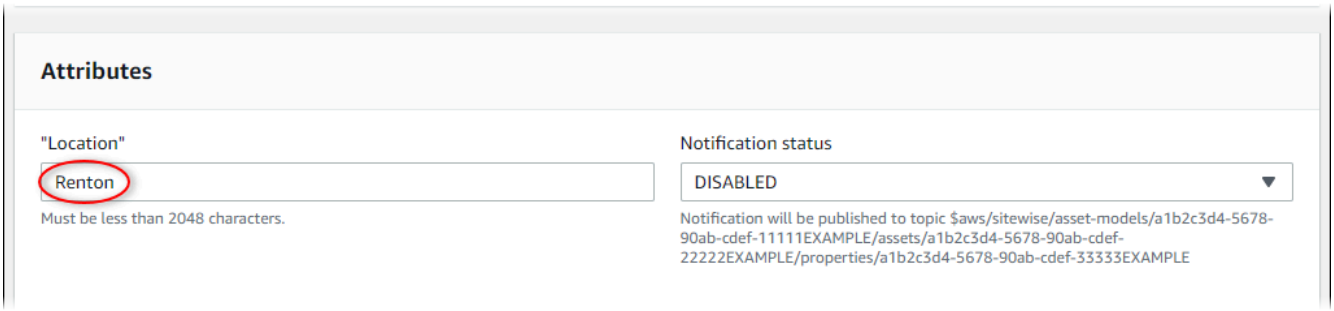
So aktualisieren Sie den Wert eines Attributs (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.

3. Wählen Sie die Komponente aus, für die Sie ein Attribut aktualisieren möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Suchen Sie das zu aktualisierende Attribut und geben Sie dann den neuen Wert ein.



6. Wählen Sie Speichern.

Updating an attribute value (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um einen Attributwert zu aktualisieren.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

Verwenden Sie die Operation „BatchPutAssetPropertyWert“, um Ihrem Objekt Attributwerte zuzuweisen. Mit dieser Operation können Sie mehrere Attribute gleichzeitig festlegen. Die Nutzlast dieser Operation enthält eine Liste von Einträgen, jeweils mit der Komponenten-ID, der Eigenschafts-ID und dem Attributwert.

Um den Wert eines Attributs zu aktualisieren (AWS CLI)

1. Erstellen Sie eine Datei namens `batch-put-payload.json` und kopieren Sie das folgende JSON-Objekt in die Datei. In diesem Nutzlast-Beispiel wird veranschaulicht, wie der Breiten-

und Längengrad einer Windturbine festgelegt wird. Aktualisieren Sie die IDs, Werte und Zeitstempel, um die Nutzlast für Ihren Anwendungsfall zu ändern.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

- Jeder Eintrag in der Nutzlast enthält eine `entryId`, die Sie als eindeutige Zeichenfolge definieren können. Bei fehlgeschlagenen Anforderungseinträgen enthält jeder Fehler die `entryId` der entsprechenden Anforderung, woran Sie erkennen können, welche Anforderungen zu wiederholen sind.

- Um einen Attributwert festzulegen, können Sie `propertyValues` für jede Attributeigenschaft eine timestamp-quality-value (TQV-) Struktur in die Liste aufnehmen. Diese Struktur muss den neuen `value` und den aktuellen `timestamp` enthalten.
  - `value`— Eine Struktur, die je nach Typ der festzulegenden Eigenschaft eines der folgenden Felder enthält:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Eine Struktur, die die aktuelle Unix-Epoche in Sekunden enthält,`timeInSeconds`. AWS IoT SiteWise lehnt alle Datenpunkte mit Zeitstempeln ab, die länger als 7 Tage in der Vergangenheit oder neuer als 5 Minuten in der future existierten.

Weitere Hinweise zur Vorbereitung einer Payload für BatchPutAssetPropertyValue finden Sie unter. Daten mithilfe der AWS IoT SiteWise API aufnehmen

2. Führen Sie den folgenden Befehl aus, um die Attributwerte an zu AWS IoT SiteWise senden:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-
put-payload.json
```

Zuordnen und Aufheben der Zuordnung von Komponenten

Wenn das Modell Ihrer Komponente Hierarchien für untergeordnete Komponentenmodelle definiert, können Sie Ihrer Komponente untergeordnete Komponenten zuordnen. Übergeordnete Komponenten können von zugehörigen Komponenten aus auf Daten zugreifen und diese aggregieren. Weitere Informationen zu hierarchischen Komponentenmodellen finden Sie unter Definition von Hierarchien für Anlagenmodelle.

Themen

- Zuordnen und Aufheben der Zuordnung von Komponenten (Konsole)
- Elemente zuordnen und deren Zuordnung aufheben ()AWS CLI

Zuordnen und Aufheben der Zuordnung von Komponenten (Konsole)

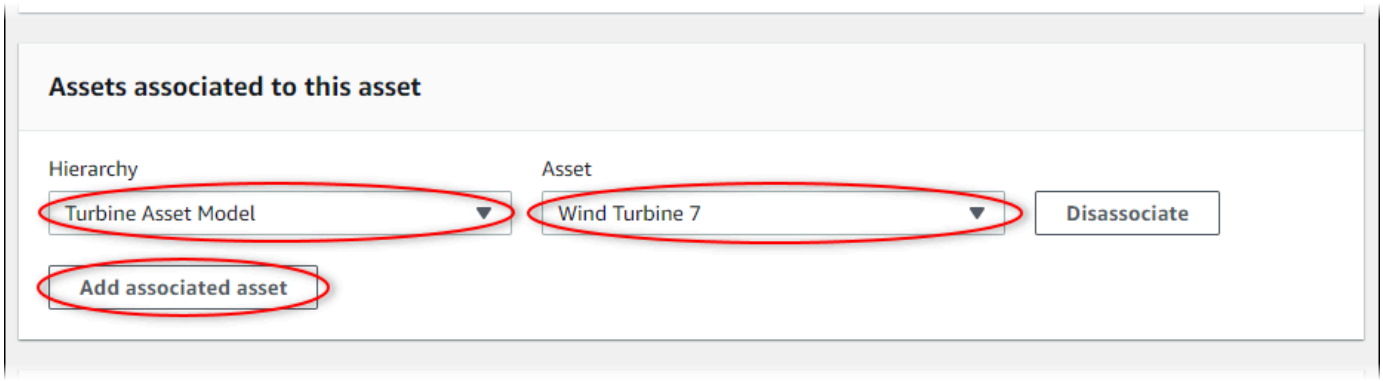
Sie können die AWS IoT SiteWise Konsole verwenden, um Anlagen zuzuordnen und die Zuordnung aufzuheben.

So ordnen Sie eine Komponente zu (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die übergeordnete Komponente aus, der Sie eine untergeordnete Komponente zuordnen möchten.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Wählen Sie unter Mit dieser Komponente verknüpfte Komponente die Option Zugehörige Komponente hinzufügen aus.



6. Wählen Sie für Hierarchie die Hierarchie aus, durch die die Beziehung zwischen der übergeordneten Komponente und der untergeordneten Komponente definiert wird.
7. Wählen Sie unter Komponente die untergeordnete Komponente aus, die zugeordnet werden soll.
8. Wählen Sie Speichern.

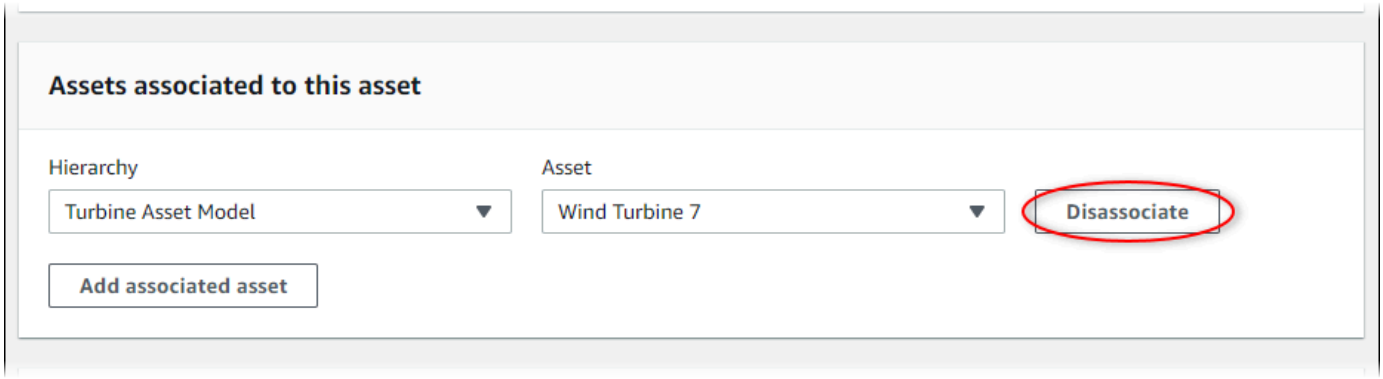
So heben Sie die Zuordnung einer Komponente auf (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.

2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die übergeordnete Komponente aus, für die Sie die Zuordnung einer untergeordneten Komponente aufheben möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Wählen Sie unter Mit dieser Komponente verknüpfte Komponenten für die Komponente die Option Zuordnung aufheben aus.



6. Wählen Sie Speichern.

Elemente zuordnen und deren Zuordnung aufheben ()AWS CLI

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um Anlagen zuzuordnen oder zu trennen.

Für dieses Verfahren müssen Sie die ID der Hierarchie (`hierarchyId`) im übergeordneten Komponentenmodell kennen, durch die die Beziehung zum untergeordneten Komponentenmodell definiert wird. Verwenden Sie die DescribeAssetOperation, um die Hierarchie-ID in der Antwort zu finden.

So suchen Sie eine Hierarchie-ID

- Führen Sie den folgenden Befehl aus, um das übergeordnete Komponente zu beschreiben. Ersetzen Sie *`parent-asset-id durch die ID`* oder externe ID des übergeordneten Assets.

```
aws iotsitewise describe-asset --asset-id parent-asset-id
```

Die Operation gibt eine Antwort zurück, die Details der Komponente enthält. Die Antwort enthält eine `assetHierarchies` Liste mit der folgenden Struktur:

```
{
  ...
  "assetHierarchies": [
    {
      "id": "String",
      "name": "String"
    }
  ],
  ...
}
```

Die Hierarchie-ID ist der `id`-Wert für eine Hierarchie in der Liste der Komponentenhierarchien.

Wenn Sie über die Hierarchie-ID verfügen, können Sie eine Komponente dieser Hierarchie zuordnen oder ihre Zuordnung zu dieser Hierarchie aufheben.

Verwenden Sie die AssociateAssetsOperation, um eine untergeordnete Anlage einer übergeordneten Anlage zuzuordnen. Verwenden Sie die DisassociateAssetsOperation, um eine untergeordnete Anlage von einer übergeordneten Anlage zu trennen. Geben Sie die folgenden Parameter an, die für beide Operationen identisch sind:

- `assetId`— Die ID oder externe ID der übergeordneten Anlage.
- `hierarchyId`— Die Hierarchie-ID oder externe ID im übergeordneten Asset.
- `childAssetId`— Die ID oder externe ID der untergeordneten Anlage.

Um ein Asset zuzuordnen (AWS CLI)

- Führen Sie den folgenden Befehl aus, um eine untergeordnete Komponente einer übergeordneten Komponente zuzuordnen. *Ersetzen Sie parent-asset-id, hierarchy-id und child-asset-id durch die entsprechenden IDs:*

```
aws iotsitewise associate-assets \
```

```
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Um die Zuordnung zu einem Asset AWS CLI() aufzuheben

- Führen Sie den folgenden Befehl aus, um die Zuordnung einer untergeordneten Komponente zu einer übergeordneten Komponente aufzuheben. *Ersetzen Sie parent-asset-id, hierarchy-id und child-asset-id durch die entsprechenden IDs:*

```
aws iotsitewise disassociate-assets \
  --asset-id parent-asset-id \
  --hierarchy-id hierarchy-id \
  --child-asset-id child-asset-id
```

Aktualisieren von Komponenten und Modellen

Sie können Ihre Anlagen, Anlagenmodelle und Komponentenmodelle aktualisieren, AWS IoT SiteWise um deren Namen und Definitionen zu ändern. Diese Aktualisierungsvorgänge sind asynchron und es dauert einige Zeit, bis sie weitergegeben werden. AWS IoT SiteWiseÜberprüfen Sie den Status des Assets oder Modells, bevor Sie weitere Änderungen vornehmen. Sie müssen warten, bis die Änderungen weitergegeben werden, bevor Sie die aktualisierte Komponente oder das aktualisierte Modell weiterhin verwenden können.

Themen

- Aktualisieren von Komponenten
- Aktualisierung von Asset- und Komponentenmodellen
- Aktualisierung benutzerdefinierter Verbundmodelle (Komponenten)

Aktualisieren von Komponenten

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um den Namen einer Anlage zu aktualisieren.

Wenn Sie ein Asset aktualisieren, bleibt der Status des Assets so lange erhalten, `UPDATING` bis die Änderungen übernommen werden. Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Themen

- Aktualisieren einer Komponenten (Konsole)
- Ein Asset aktualisieren (AWS CLI)

Aktualisieren einer Komponenten (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um die Asset-Details zu aktualisieren.

So aktualisieren Sie eine Komponente (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die zu aktualisierende Komponente aus.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Aktualisieren Sie den Eintrag für Name der Komponente.
6. (Optional) Aktualisieren Sie auf dieser Seite andere Informationen für die Komponente. Weitere Informationen finden Sie hier:

   - Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften
   - Aktualisieren von Attributwerten
   - Interaktion mit anderen AWS Diensten
7. Wählen Sie Speichern.

Ein Asset aktualisieren (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um den Namen eines Assets zu aktualisieren.

Verwenden Sie die UpdateAssetOperation, um ein Asset zu aktualisieren. Geben Sie die folgenden Parameter an:

- `assetId`— Die ID des Assets. Dies ist die tatsächliche ID im UUID-Format, oder die, `externalId:myExternalId` falls sie eine hat. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.
- `assetName`— Der neue Name des Assets.

Um den Namen eines Assets zu aktualisieren (AWS CLI)

- Führen Sie den folgenden Befehl aus, um den Namen einer Komponente zu aktualisieren. Ersetzen Sie die *`Asset-ID`* durch die ID oder externe ID des Assets. Aktualisieren Sie den *`Asset-Namen`* mit dem neuen Namen für das Asset.

```
aws iotsitewise update-asset \
  --asset-id asset-id \
  --asset-name asset-name
```

Aktualisierung von Asset- und Komponentenmodellen

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um ein Asset- oder Komponentenmodell zu aktualisieren.

Sie können den Typ oder den Datentyp einer vorhandenen Eigenschaft oder das Fenster einer vorhandenen Metrik nicht ändern. Sie können den Modelltyp auch nicht von einem Asset-Modell zum Komponentenmodell oder umgekehrt ändern.

> **Important**
>
> - Wenn Sie eine Eigenschaft aus einem Asset- oder Komponentenmodell entfernen, AWS IoT SiteWise werden alle vorherigen Daten für diese Eigenschaft gelöscht. Bei Komponentenmodellen wirkt sich dies auf alle Anlagenmodelle aus, die dieses

Komponentenmodell verwenden. Achten Sie also besonders darauf, zu verstehen, wie umfassend Ihre Änderung sein kann.

- Wenn Sie eine Hierarchiedefinition aus einem Anlagenmodell entfernen, AWS IoT SiteWise wird die Zuordnung aller Anlagen in dieser Hierarchie aufgehoben.

Wenn Sie ein Komponentenmodell aktualisieren, spiegelt jede Komponente, die auf diesem Modell basiert, alle Änderungen wider, die Sie am zugrunde liegenden Modell vornehmen. Bis die Änderungen weitergeben werden, hat jede Komponente den Status `UPDATING`. Sie müssen warten, bis diese Komponenten wieder in den Zustand `ACTIVE` zurückkehren, bevor Sie mit ihnen interagieren können. Während dieser Zeit hat das aktualisierte Komponentenmodell den Status `PROPAGATING`.

Wenn Sie ein Komponentenmodell aktualisieren, spiegelt jedes Anlagenmodell, das dieses Komponentenmodell enthält, die Änderungen wider. Bis die Änderungen am Komponentenmodell wirksam werden, hat jedes betroffene Asset-Modell den `UPDATING` Status, gefolgt von `PROPAGATING` der Aktualisierung der zugehörigen Assets, wie im vorherigen Absatz beschrieben. Sie müssen warten, bis diese Asset-Modelle wieder in den gleichen `ACTIVE` Zustand zurückkehren, bevor Sie mit ihnen interagieren. Während dieser Zeit wird der Status des aktualisierten Komponentenmodells beibehalten`PROPAGATING`.

Weitere Informationen finden Sie unter Komponenten- und Modellzustände.

Themen

- Aktualisierung eines Asset- oder Komponentenmodells (Konsole)
- Aktualisierung eines Asset- oder Komponentenmodells (AWS CLI)

Aktualisierung eines Asset- oder Komponentenmodells (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um ein Asset- oder Komponentenmodell zu aktualisieren.

Um ein Asset- oder Komponentenmodell (Konsole) zu aktualisieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das zu aktualisierende Asset- oder Komponentenmodell aus.

4. Wählen Sie Bearbeiten aus.
5. Führen Sie auf der Seite Modell bearbeiten einen der folgenden Schritte aus:
   - Ändern Sie unter Modelldetails die Angabe unter Name für das Modell.
   - Ändern Sie eine der Attributdefinitionen. Sie können den Datentyp vorhandener Attribute nicht ändern. Weitere Informationen finden Sie unter Definition statischer Daten (Attribute).
   - Ändern Sie eine der Messungsdefinitionen. Sie können den Datentyp vorhandener Messungen nicht ändern. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).
   - Ändern Sie eine der Transformationsdefinitionen. Weitere Informationen finden Sie unter Daten transformieren (transformiert).
   - Ändern Sie eine der Metrikdefinitionen. Sie können das Zeitintervall vorhandener Metriken nicht ändern. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).
   - (Nur Asset-Modelle) Ändern Sie eine der Hierarchiedefinitionen. Sie können das Hierarchiemodell vorhandener Hierarchien nicht ändern. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.
6. Wählen Sie Save (Speichern) aus.

Aktualisierung eines Asset- oder Komponentenmodells (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein Asset- oder Komponentenmodell zu aktualisieren.

Verwenden Sie die UpdateAssetModel-API, um den Namen, die Beschreibung und die Eigenschaften eines Asset- oder Komponentenmodells zu aktualisieren. Nur für Asset-Modelle können Sie Hierarchien aktualisieren. Geben Sie die folgenden Parameter an:

- `assetModelId`— Die ID des Assets. Dies ist die tatsächliche ID im UUID-Format, oder die, `externalId:myExternalId` falls sie eine hat. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Geben Sie das aktualisierte Modell in der Payload an. Weitere Informationen zum erwarteten Format eines Asset- oder Komponentenmodells finden Sie unterErstellen von Komponentenmodellen.

> **Warning**
>
> Die UpdateAssetModel-API überschreibt das vorhandene Modell mit dem Modell, das Sie in der Payload angeben. Um zu verhindern, dass die Eigenschaften oder Hierarchien Ihres Modells gelöscht werden, müssen Sie deren IDs und Definitionen in die aktualisierte Modellnutzlast aufnehmen. Informationen zum Abfragen der vorhandenen Struktur Ihres Modells finden Sie unter Operation DescribeAssetModell.

> **Note**
>
> Mit dem folgenden Verfahren können nur zusammengesetzte Modelle des Typs aktualisiert `AWS/ALARM` werden. Wenn Sie `CUSTOM` zusammengesetzte Modelle aktualisieren möchten, verwenden Sie stattdessen UpdateAssetModelCompositeModel. Weitere Informationen finden Sie unter Aktualisierung benutzerdefinierter Verbundmodelle (Komponenten).

Um ein Asset- oder Komponentenmodell zu aktualisieren (AWS CLI)

1. Führen Sie den folgenden Befehl aus, um die vorhandene Modelldefinition abzurufen. Ersetzen Sie *`asset-model-id`* durch die ID oder die externe ID des zu aktualisierenden Asset- oder Komponentenmodells.

   ```
   aws iotsitewise describe-asset-model --asset-model-id asset-model-id
   ```

   Die Operation gibt eine Antwort zurück, die die Details des Modells enthält. Die Antwort weist die folgenden Struktur auf.

   ```
   {
     "assetModelId": "String",
     "assetModelArn": "String",
     "assetModelName": "String",
     "assetModelDescription": "String",
     "assetModelProperties": Array of AssetModelProperty,
     "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
     "assetModelCompositeModels": Array of AssetModelCompositeModel,
     "assetModelCompositeModelSummaries": Array of AssetModelCompositeModelSummary,
     "assetModelCreationDate": "String",
     "assetModelLastUpdateDate": "String",
   ```

```
  "assetModelStatus": {
    "state": "String",
    "error": {
      "code": "String",
      "message": "String"
    },
  "assetModelType": "String"
  }
}
```

Weitere Informationen finden Sie unter der Operation DescribeAssetModell.

2. Erstellen Sie eine Datei namens `update-asset-model.json` und kopieren Sie die Antwort des vorherigen Befehls in die Datei.
3. Entfernen Sie die folgenden Schlüssel-Wert-Paare aus dem JSON-Objekt in `update-asset-model.json`:

   - `assetModelId`
   - `assetModelArn`
   - `assetModelCompositeModelSummaries`
   - `assetModelCreationDate`
   - `assetModelLastUpdateDate`
   - `assetModelStatus`
   - `assetModelType`

   Für die Operation UpdateAssetModel wird eine Nutzlast mit der folgenden Struktur erwartet:

```
{
  "assetModelName": "String",
  "assetModelDescription": "String",
  "assetModelProperties": Array of AssetModelProperty,
  "assetModelHierarchies": Array of AssetModelHierarchyDefinition,
  "assetModelCompositeModels": Array of AssetModelCompositeModel
}
```

4. Führen Sie in `update-asset-model.json` eine der folgenden Aufgaben durch:

   - Ändern des Namens des Komponentenmodells (`assetModelName`).

- Ändern, Hinzufügen oder Entfernen der Beschreibung des Komponentenmodells (`assetModelDescription`).
- Ändern, Hinzufügen oder Entfernen der Eigenschaften des Komponentenmodells (`assetModelProperties`). Sie können den `dataType` der vorhandenen Eigenschaften oder das `window` vorhandener Metriken nicht ändern. Weitere Informationen finden Sie unter Definieren von Dateneigenschaften.
- Ändern, Hinzufügen oder Entfernen einer der Hierarchien des Komponentenmodells (`assetModelHierarchies`). Sie können die `childAssetModelId` von vorhandenen Hierarchien nicht ändern. Weitere Informationen finden Sie unter Definition von Hierarchien für Anlagenmodelle.
- Sie können eines der zusammengesetzten Modelle des Typs `AWS/ALARM` (`assetModelCompositeModels`) des Asset-Modells ändern, hinzufügen oder entfernen. Alarme überwachen andere Eigenschaften, sodass Sie erkennen können, wann Geräte oder Prozesse besondere Aufmerksamkeit erfordern. Jede Alarmdefinition ist ein zusammengesetztes Modell, das die vom Alarm verwendeten Eigenschaften standardisiert. Weitere Informationen finden Sie unter Daten mit Alarmen überwachen und Definition von Alarmen für Anlagenmodelle.

5. Führen Sie den folgenden Befehl aus, um das Komponentenmodell mit der in `update-asset-model.json` gespeicherten Definition zu aktualisieren. Ersetzen Sie *`asset-model-id durch die ID`* des Asset-Modells:

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://model-payload.json
```

Aktualisierung benutzerdefinierter Verbundmodelle (Komponenten)

Sie können die AWS IoT SiteWise API verwenden, um ein benutzerdefiniertes Verbundmodell zu aktualisieren, oder die AWS IoT SiteWise Konsole, um Komponenten zu aktualisieren.

Themen

- Aktualisierung einer Komponente (Konsole)
- Aktualisieren eines benutzerdefinierten Verbundmodells (AWS CLI)

Aktualisierung einer Komponente (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um eine Komponente zu aktualisieren.

Um eine Komponente (Konsole) zu aktualisieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das Asset-Modell aus, in dem sich die Komponente befindet.
4. Wählen Sie auf der Registerkarte Eigenschaften die Option Komponenten aus.
5. Wählen Sie die Komponente aus, die Sie aktualisieren möchten.
6. Wählen Sie Bearbeiten aus.
7. Führen Sie auf der Seite Komponente bearbeiten einen der folgenden Schritte aus:
   - Ändern Sie unter Modelldetails die Angabe unter Name für das Modell.
   - Ändern Sie eine der Attributdefinitionen. Sie können den Datentyp vorhandener Attribute nicht ändern. Weitere Informationen finden Sie unter Definition statischer Daten (Attribute).
   - Ändern Sie eine der Messungsdefinitionen. Sie können den Datentyp vorhandener Messungen nicht ändern. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen).
   - Ändern Sie eine der Transformationsdefinitionen. Weitere Informationen finden Sie unter Daten transformieren (transformiert).
   - Ändern Sie eine der Metrikdefinitionen. Sie können das Zeitintervall vorhandener Metriken nicht ändern. Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).
8. Wählen Sie Save (Speichern) aus.

Aktualisieren eines benutzerdefinierten Verbundmodells (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein benutzerdefiniertes Verbundmodell zu aktualisieren.

Verwenden Sie die Operation UpdateAssetModelCompositeModel, um den Namen oder die Beschreibung zu aktualisieren. Nur für benutzerdefinierte Verbundwerkstoffmodelle können Sie auch die Eigenschaften aktualisieren. Sie können die Eigenschaften eines component-model-based

benutzerdefinierten Verbundmodells nicht aktualisieren, da das referenzierte Komponentenmodell die zugehörigen Eigenschaften bereitstellt.

> **Important**
>
> Wenn Sie eine Eigenschaft aus einem benutzerdefinierten Verbundmodell entfernen, AWS IoT SiteWise werden alle vorherigen Daten für diese Eigenschaft gelöscht. Sie können den Typ oder den Datentyp einer vorhandenen Eigenschaft nicht ändern.
> Gehen Sie wie folgt vor, um eine vorhandene Eigenschaft eines zusammengesetzten Modells durch eine neue Eigenschaft mit derselben `name` zu ersetzen:
>
> 1. Reichen Sie eine `UpdateAssetModelCompositeModel` Anfrage ein, bei der die gesamte vorhandene Eigenschaft entfernt wurde.
> 2. Reichen Sie eine zweite `UpdateAssetModelCompositeModel` Anfrage ein, die die neue Immobilie umfasst. Die neue Objekteigenschaft hat dieselbe Eigenschaft `name` wie die vorherige und AWS IoT SiteWise generiert ein neues Unikat`id`.

Um ein benutzerdefiniertes Verbundmodell zu aktualisieren (AWS CLI)

1. Führen Sie den folgenden Befehl aus, um die bestehende Definition eines zusammengesetzten Modells abzurufen. Ersetzen Sie *`composite-model-id durch die ID`* oder die externe ID des benutzerdefinierten Verbundmodells, das aktualisiert werden soll, und *`asset-model-id durch das Asset-Modell`*, dem das benutzerdefinierte Verbundmodell zugeordnet ist. Weitere Informationen finden Sie im Benutzerhandbuch.AWS IoT SiteWise

   ```
   aws iotsitewise describe-asset-model-composite-model \
   --asset-model-composite-model-id composite-model-id \
   --asset-model-id asset-model-id
   ```

   Weitere Informationen finden Sie unter „DescribeAssetModelCompositeModellieren“.
2. Erstellen Sie eine Datei mit dem Namen`update-custom-composite-model.json`, und kopieren Sie dann die Antwort des vorherigen Befehls in die Datei.
3. Entfernen Sie alle Schlüssel-Wert-Paare aus dem JSON-Objekt in `update-custom-composite-model.json` mit Ausnahme der folgenden Felder:

   - `assetModelCompositeModelName`
   - `assetModelCompositeModelDescription`(falls vorhanden)

- `assetModelCompositeModelProperties`(falls vorhanden)

4. Führen Sie in `update-custom-composite-model.json` eine der folgenden Aufgaben durch:

   - Ändern Sie den Wert von`assetModelCompositeModelName`.
   - Fügen Sie den Wert hinzu`assetModelCompositeModelDescription`, entfernen Sie ihn oder ändern Sie ihn.
   - Nur für benutzerdefinierte Inline-Verbundmodelle: Ändern, hinzufügen oder entfernen Sie alle Eigenschaften des Asset-Modells in`assetModelCompositeModelProperties`.

   Weitere Informationen zum erforderlichen Format für diese Datei finden Sie in der Anforderungssyntax für UpdateAssetModelCompositeModel.

5. Führen Sie den folgenden Befehl aus, um das benutzerdefinierte Verbundmodell mit der Definition zu aktualisieren, die in gespeichert ist`update-custom-composite-model.json`. Ersetzen Sie *`composite-model-id durch die ID`* des Verbundmodells und *`asset-model-id durch die ID des Asset-Modells`*, in dem es sich befindet.

```
aws iotsitewise update-asset-model-composite-model \
--asset-model-composite-model-id composite-model-id \
--asset-model-id asset-model-id \
--cli-input-json file://update-custom-composite-model.json
```

Löschen von Komponenten und Modellen

Sie können Ihre Anlagen und Modelle löschen AWS IoT SiteWise , sobald Sie mit ihnen fertig sind. Die Löschvorgänge sind asynchron und es dauert einige Zeit, bis sie weitergegeben werden. AWS IoT SiteWise

Themen

- Löschen von Komponenten
- Löschen von Komponentenmodellen

Löschen von Komponenten

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um ein Asset zu löschen.

Bevor Sie eine Komponente löschen können, müssen Sie zunächst die Zuordnung der ihr untergeordneten Komponenten und ihre Zuordnung zu der ihr übergeordneten Komponente aufheben. Weitere Informationen finden Sie unter Zuordnen und Aufheben der Zuordnung von Komponenten. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, können Sie die Operation ListAssociatedAssets verwenden, um die untergeordneten Elemente eines Assets aufzulisten.

Wenn Sie eine Komponente löschen, ist der Status so lange `DELETING`, bis die Änderungen weitergegeben werden. Weitere Informationen finden Sie unter Komponenten- und Modellzustände. Nachdem die Komponente gelöscht wurde, können Sie sie nicht mehr abfragen. Wenn Sie dies versuchen, gibt die API eine HTTP-404-Antwort zurück.

> **Important**
>
> AWS IoT SiteWise löscht alle Eigenschaftsdaten für gelöschte Objekte.

Themen

- Löschen einer Komponente (Konsole)
- Löschen eines Assets (AWS CLI)

Löschen einer Komponente (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um ein Asset zu löschen.

So löschen Sie ein Asset (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die zu löschende Komponente aus.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wenn die Komponente über Zugehörige Komponenten verfügt, löschen Sie jede Komponente. Sie können den Namen einer Komponente auswählen, um zu ihrer Seite zu navigieren, auf der Sie sie löschen können.
5. Wählen Sie auf der Seite der Komponente Löschen aus.
6. Gehen Sie im Dialogfeld „Asset löschen“ wie folgt vor:

   a. Geben Sie **`Delete`** ein, um den Löschvorgang zu bestätigen.

   b. Wählen Sie Löschen aus.

Löschen eines Assets (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein Asset zu löschen.

Verwenden Sie die DeleteAssetOperation, um ein Asset zu löschen. Geben Sie den folgenden Parameter an:

- `assetId`— Die ID des Assets. Dies ist die tatsächliche ID im UUID-Format, oder die, `externalId:myExternalId` falls sie eine hat. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Um ein Asset zu löschen ()AWS CLI

1. Führen Sie den folgenden Befehl aus, um die Hierarchien der Komponente aufzulisten. Ersetzen Sie die *`Asset-ID`* durch die ID oder die externe ID des Assets:

   ```
   aws iotsitewise describe-asset --asset-id asset-id
   ```

   Die Operation gibt eine Antwort zurück, die Details der Komponente enthält. Die Antwort enthält eine `assetHierarchies` Liste mit der folgenden Struktur:

   ```
   {
     ...
     "assetHierarchies": [
       {
         "id": "String",
         "name": "String"
       }
     ],
   ```

```
  ...
}
```

Weitere Informationen finden Sie in der DescribeAssetOperation.

2. Führen Sie für jede Hierarchie den folgenden Befehl aus, um die untergeordneten Komponenten der Komponente aufzulisten, die dieser Hierarchie zugeordnet sind. Ersetzen Sie *Asset-ID* durch die ID oder externe ID des Assets und *Hierarchy-ID durch die ID* oder externe ID der Hierarchie.

```
aws iotsitewise list-associated-assets \
  --asset-id asset-id \
  --hierarchy-id hierarchy-id
```

Weitere Informationen finden Sie unter dem Vorgang „Assets“. ListAssociated

3. Führen Sie den folgenden Befehl aus, um jede zugeordnete Komponente zu löschen und dann die Komponente zu löschen. Ersetzen Sie die *Asset-ID* durch die ID oder externe ID des Assets.

```
aws iotsitewise delete-asset --asset-id asset-id
```

Löschen von Komponentenmodellen

Sie können die AWS IoT SiteWise Konsole oder API verwenden, um ein Asset-Modell zu löschen.

Bevor Sie ein Asset-Modell löschen können, müssen Sie zunächst alle Assets löschen, die anhand des Asset-Modells erstellt wurden.

Wenn Sie ein Komponentemodell löschen, ist der Status so lange `DELETING`, bis die Änderungen weitergegeben werden. Weitere Informationen finden Sie unter Komponenten- und Modellzustände. Nachdem das Komponentenmodell gelöscht wurde, können Sie es nicht mehr abfragen. Wenn Sie dies versuchen, gibt die API eine HTTP-404-Antwort zurück.

Themen

- Löschen eines Komponentenmodells (Konsole)
- Löschen eines Objektmodells (AWS CLI)

Löschen eines Komponentenmodells (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um ein Asset-Modell zu löschen.

So löschen Sie ein Komponentenmodell (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das zu löschende Komponentenmodell aus.
4. Wenn das Modell über Komponenten verfügt, löschen Sie jede Komponente. Wählen Sie den Namen einer Komponente aus, um zu ihrer Seite zu navigieren, auf der Sie sie löschen können. Weitere Informationen finden Sie unter Löschen einer Komponente (Konsole).
5. Wählen Sie auf der Seite des Modells die Option Löschen aus.
6. Gehen Sie im Dialogfeld Modell löschen wie folgt vor:

   a. Geben Sie **`Delete`** ein, um den Löschvorgang zu bestätigen.

   b. Wählen Sie Löschen aus.

Löschen eines Objektmodells (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um ein Asset-Modell zu löschen.

Verwenden Sie die DeleteAssetModel-Operation, um ein Asset-Modell zu löschen. Geben Sie den folgenden Parameter an:

- `assetModelId`— Die ID des Assets. Dies ist die tatsächliche ID im UUID-Format, oder die, `externalId:myExternalId` falls sie eine hat. Weitere Informationen finden Sie unter Objekte mit externen IDs referenzieren im AWS IoT SiteWise -Benutzerhandbuch.

Um ein Asset-Modell zu löschen ()AWS CLI

1. Führen Sie den folgenden Befehl aus, um alle Komponenten aufzulisten, die aus dem Modell erstellt wurden. Ersetzen Sie *`asset-model-id durch die ID`* oder die externe ID des Asset-Modells.

   ```
   aws iotsitewise list-assets --asset-model-id asset-model-id
   ```

Weitere Informationen finden Sie in der Operation. ListAssets

2. Wenn der vorherige Befehl Komponenten aus dem Modell zurückgibt, löschen Sie jede Komponente. Weitere Informationen finden Sie unter Löschen eines Assets (AWS CLI).
3. Führen Sie den folgenden Befehl zum Löschen des Komponentenmodells aus. Ersetzen Sie *asset-model-id durch die ID* oder externe ID des Asset-Modells.

```
aws iotsitewise delete-asset-model --asset-model-id asset-model-id
```

Massenoperationen mit Assets und Modellen

Wenn Sie mit einer großen Anzahl von Anlagen oder Anlagenmodellen arbeiten möchten, verwenden Sie Massenoperationen, um Ressourcen massenweise zu importieren und an einen anderen Ort zu exportieren. Sie können beispielsweise eine Datendatei erstellen, die Assets oder Asset-Modelle in einem Amazon S3 S3-Bucket definiert, und diese mithilfe des Massenimports erstellen oder aktualisieren AWS IoT SiteWise. Wenn Sie über eine große Anzahl von Assets oder Asset-Modellen verfügen AWS IoT SiteWise, können Sie diese alternativ nach Amazon S3 exportieren.

> **Note**
>
> Sie führen Massenoperationen durch, AWS IoT SiteWise indem Sie Operationen in der AWS IoT TwinMaker API aufrufen. Sie können dies tun, ohne einen AWS IoT TwinMaker Workspace einzurichten AWS IoT TwinMaker oder zu erstellen. Sie benötigen lediglich einen Amazon S3 S3-Bucket, in dem Sie Ihre AWS IoT SiteWise Inhalte platzieren können.

Themen

- AWS IoT SiteWise Auftragsschema für die Übertragung von Metadaten

Wichtige Konzepte und Terminologie

AWS IoT SiteWise Funktionen für Massenimport und -export basieren auf den folgenden Konzepten und Begriffen:

- Import: Die Aktion, bei der Assets oder Asset-Modelle aus einer Datei in einem Amazon S3 S3-Bucket in verschoben AWS IoT SiteWise werden.
- Export: Die Aktion, bei der Assets oder Asset-Modelle aus AWS IoT SiteWise einem Amazon S3 S3-Bucket verschoben werden.
- Quelle: Der Startort, von dem Sie Inhalte verschieben möchten.

  Ein Amazon S3 S3-Bucket ist beispielsweise eine Importquelle und AWS IoT SiteWise eine Exportquelle.
- Ziel: Der gewünschte Ort, an den Sie Ihre Inhalte verschieben möchten.

  Ein Amazon S3 S3-Bucket ist beispielsweise ein Exportziel und AWS IoT SiteWise ein Importziel.
- AWS IoT SiteWise Schema: Dieses Schema wird verwendet, um Metadaten von zu importieren und zu exportieren AWS IoT SiteWise.
- Ressource der obersten Ebene: Eine AWS IoT SiteWise Ressource, die Sie individuell erstellen oder aktualisieren können, z. B. ein Asset oder ein Asset-Modell.
- Unterressource: Eine verschachtelte AWS IoT SiteWise Ressource innerhalb einer Ressource der obersten Ebene. Beispiele hierfür sind Eigenschaften, Hierarchien und zusammengesetzte Modelle.
- Metadaten: Wichtige Informationen, die für den erfolgreichen Import oder Export von Ressourcen erforderlich sind. Beispiele für Metadaten sind Definitionen von Vermögenswerten und Asset-Modellen.
- Metadaten TransferJob: Das Objekt, das beim Ausführen erstellt wurde`CreateMetadataTransferJob`.

Unterstützte Funktionen

In diesem Thema wird erklärt, was Sie tun können, wenn Sie einen Massenvorgang ausführen. Massenvorgänge unterstützen die folgenden Funktionen:

- Erstellung von Ressourcen auf oberster Ebene: Wenn Sie ein Asset oder ein Asset-Modell importieren, das keine ID definiert oder dessen ID nicht mit der einer vorhandenen ID übereinstimmt, wird es als neue Ressource erstellt.
- Ersetzung von Ressourcen auf oberster Ebene: Wenn Sie ein Asset oder ein Asset-Modell importieren, dessen ID mit einer bereits vorhandenen übereinstimmt, ersetzt es die vorhandene Ressource.
- Erstellen, Ersetzen oder Löschen von Unterressourcen: Wenn Ihr Import eine Ressource der obersten Ebene ersetzt, z. B. eine Anlage oder ein Anlagenmodell, ersetzt die neue Definition alle Unterressourcen wie Eigenschaften, Hierarchien oder zusammengesetzte Modelle.

  Wenn Sie beispielsweise ein Asset-Modell während eines Massenimports aktualisieren und die aktualisierte Version eine Eigenschaft definiert, die im Original nicht vorhanden war, wird eine neue Eigenschaft erstellt. Wenn sie eine Eigenschaft definiert, die bereits vorhanden ist, wird die vorhandene Eigenschaft aktualisiert. Wenn das aktualisierte Objektmodell eine Eigenschaft auslässt, die im Original vorhanden war, wird die Eigenschaft gelöscht.
- Kein Löschen von Ressourcen auf oberster Ebene: Bei Massenvorgängen wird kein Asset oder Asset-Modell gelöscht. Bei Massenvorgängen werden sie nur erstellt oder aktualisiert.

Voraussetzungen für Massenoperationen

In diesem Abschnitt werden die Voraussetzungen für den Massenvorgang erläutert, einschließlich AWS Identity and Access Management (IAM-) Berechtigungen für den Austausch von Ressourcen zwischen AWS-Services und Ihrem lokalen Computer. Bevor Sie einen Massenvorgang starten, müssen Sie die folgenden Voraussetzungen erfüllen:

- Erstellen Sie einen Amazon S3 S3-Bucket zum Speichern von Ressourcen. Weitere Informationen zur Verwendung von Amazon S3 finden Sie unter Was ist Amazon S3?

IAM-Berechtigungen

Um Massenoperationen durchzuführen, müssen Sie eine AWS Identity and Access Management (IAM-) Richtlinie mit Berechtigungen erstellen, die den Austausch von AWS Ressourcen zwischen Amazon S3 und Ihrem lokalen Computer ermöglichen. AWS IoT SiteWise Weitere Informationen zum Erstellen von benutzerdefinierten Richtlinien finden Sie unter IAM-Richtlinien erstellen.

Um Massenoperationen durchzuführen, benötigen Sie die folgenden Richtlinien.

AWS IoT SiteWise Richtlinie

Diese Richtlinie ermöglicht den Zugriff auf die erforderlichen AWS IoT SiteWise API-Aktionen für Massenoperationen:

```
{
    "Sid": "SiteWiseApiAccess",
    "Effect": "Allow",
    "Action": [
        "iotsitewise:CreateAsset",
        "iotsitewise:CreateAssetModel",
        "iotsitewise:UpdateAsset",
        "iotsitewise:UpdateAssetModel",
        "iotsitewise:UpdateAssetProperty",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:AssociateAssets",
        "iotsitewise:DisassociateAssets",
        "iotsitewise:AssociateTimeSeriesToAssetProperty",
        "iotsitewise:DisassociateTimeSeriesFromAssetProperty",
        "iotsitewise:BatchPutAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:CreateAssetModelCompositeModel",
        "iotsitewise:UpdateAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DeleteAssetModelCompositeModel",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:DescribeAssetCompositeModel"
    ],
    "Resource": "*"
}
```

AWS IoT TwinMaker Richtlinie

Diese Richtlinie ermöglicht den Zugriff auf die AWS IoT TwinMaker API-Operationen, die Sie für die Arbeit mit Massenoperationen verwenden:

```
{
    "Sid": "MetadataTransferJobApiAccess",
    "Effect": "Allow",
    "Action": [
        "iottwinmaker:CreateMetadataTransferJob",
        "iottwinmaker:CancelMetadataTransferJob",
        "iottwinmaker:GetMetadataTransferJob",
        "iottwinmaker:ListMetadataTransferJobs"
    ],
    "Resource": "*"
}
```

Amazon S3 S3-Richtlinie

Diese Richtlinie bietet Zugriff auf Amazon S3 S3-Buckets für die Übertragung von Metadaten für Massenoperationen.

For a specific Amazon S3 bucket

Wenn Sie einen bestimmten Bucket für die Arbeit mit Ihren Metadaten für Massenoperationen verwenden, bietet diese Richtlinie Zugriff auf diesen Bucket:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::bucket name",
        "arn:aws:s3:::bucket name/*"
    ]
```

```
}
```

To allow any Amazon S3 bucket

Wenn Sie viele verschiedene Buckets verwenden, um mit Ihren Metadaten für Massenoperationen zu arbeiten, bietet diese Richtlinie Zugriff auf jeden beliebigen Bucket:

```
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": "*"
}
```

Informationen zur Fehlerbehebung bei Import- und Exportvorgängen finden Sie unterFehlerbehebung beim Massenimport und -export.

Einen Massenimportauftrag ausführen

Beim Massenimport werden Metadaten in einen AWS IoT SiteWise Workspace verschoben. Durch den Massenimport können beispielsweise Metadaten aus einer lokalen Datei oder einer Datei in einem Amazon S3 S3-Bucket in einen AWS IoT SiteWise Workspace verschoben werden.

Schritt 1: Bereiten Sie die Datei für den Import vor

Laden Sie die Datei im AWS IoT SiteWise nativen Format herunter, um Assets und Asset-Modelle zu importieren. Weitere Details finden Sie unter AWS IoT SiteWise Auftragsschema für die Übertragung von Metadaten.

Schritt 2: Laden Sie die vorbereitete Datei auf Amazon S3 hoch

Laden Sie die Datei auf Amazon S3 hoch. Weitere Informationen finden Sie unter Hochladen einer Datei auf Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

Metadaten importieren (Konsole)

Sie können den verwenden AWS-IoT-SiteWise-Konsole , um Metadaten massenweise zu importieren. Folgen Sie Schritt 1: Bereiten Sie die Datei für den Import vor und bereiten Schritt 2: Laden Sie die vorbereitete Datei auf Amazon S3 hoch Sie eine Datei vor, die für den Import bereit ist.

Daten von Amazon S3 importieren nach AWS-IoT-SiteWise-Konsole

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich die Option Massenoperationen Neu aus.
3. Wählen Sie Neuer Import, um den Importvorgang zu starten.
4. Gehen Sie auf der Seite Metadaten importieren wie folgt vor:
   - Wählen Sie Amazon S3 durchsuchen, um den Amazon S3 S3-Bucket und die Dateien anzuzeigen.
   - Navigieren Sie zu dem Amazon S3 S3-Bucket, der die vorbereitete Importdatei enthält.
   - Wählen Sie die zu importierende Datei aus.
   - Überprüfen Sie die ausgewählte Datei und wählen Sie „Importieren“.
5. Auf der Seite „Massenvorgänge für SiteWise Metadaten“ von AWS-IoT-SiteWise-Konsole wird der neu erstellte Importauftrag in der Fortschrittstabelle der Jobs angezeigt.

Metadaten importieren (AWS CLI)

Gehen Sie wie folgt vor, um eine Importaktion durchzuführen:

Daten von Amazon S3 importieren nach AWS CLI

1. Erstellen Sie eine Metadatendatei, die die Ressourcen angibt, die Sie importieren möchten, und folgen Sie dabei demAWS IoT SiteWise Auftragsschema für die Übertragung von Metadaten. Speichern Sie diese Datei in Ihrem Amazon S3 S3-Bucket.

   Beispiele für zu importierende Metadatendateien finden Sie unterBeispiele für den Import von Metadaten.
2. Erstellen Sie nun eine JSON-Datei mit dem Hauptteil der Anfrage. Der Anforderungstext gibt die Quelle und das Ziel für den Übertragungsjob an. Diese Datei ist von der Datei aus dem vorherigen Schritt getrennt. Stellen Sie sicher, dass Sie Ihren Amazon S3 S3-Bucket als Quelle und `iotsitewise` als Ziel angeben.

Das folgende Beispiel zeigt den Hauptteil der Anfrage:

```
{
      "metadataTransferJobId": "your-transfer-job-Id",
      "sources": [{
          "type": "s3",
          "s3Configuration": {
              "location": "arn:aws:s3:::your-S3-bucket-name/
your_import_metadata.json"
          }
      }],
      "destination": {
          "type": "iotsitewise"
      }
  }
```

3. Rufen Sie den auf, `CreateMetadataTransferJob` indem Sie den folgenden AWS CLI Befehl ausführen. In diesem Beispiel wird die Anforderungstextdatei aus dem vorherigen Schritt benannt`createMetadataTransferJobExport.json`.

```
aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
  --cli-input-json file://createMetadataTransferJobImport.json
```

Dadurch wird ein Auftrag zur Übertragung von Metadaten erstellt und der Prozess der Übertragung der ausgewählten Ressourcen gestartet.

Einen Massenexportauftrag ausführen

Beim Massenexport werden Metadaten von einem AWS IoT SiteWise Workspace in einen Amazon S3 S3-Bucket verschoben.

Wenn Sie einen Massenexport Ihrer AWS IoT SiteWise Inhalte nach Amazon S3 durchführen, können Sie Filter angeben, um einzuschränken, welche spezifischen Asset-Modelle und Assets Sie exportieren möchten.

Die Filter müssen in einem `iotSiteWiseConfiguration` Abschnitt im Quellenbereich Ihrer JSON-Anfrage angegeben werden.

> **Note**
>
> Sie können mehrere Filter in Ihre Anfrage aufnehmen. Bei der Massenoperation werden Asset-Modelle und Assets exportiert, die einem der Filter entsprechen.
> Wenn Sie keine Filter angeben, exportiert der Massenvorgang alle Ihre Asset-Modelle und Assets.

Example Hauptteil mit Filtern anfordern

```
{
      "metadataTransferJobId": "your-transfer-job-id",
      "sources": [
       {
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
          "filters": [
           {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID"
              }
           },
           {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeAssets": true
              }
           },
           {
              "filterByAssetModel": {
                  "assetModelId": "asset model ID",
                  "includeOffspring": true
               }
            }
          ]
        }
       }
      ],
      "destination": {
         "type": "s3",
         "s3Configuration": {
```

```
            "location": "arn:aws:s3:::your-S3-bucket-location"
          }
      }
}
```

Metadaten exportieren (Konsole)

Das folgende Verfahren erklärt die Exportaktion der Konsole:

Erstellen Sie einen Exportauftrag in der AWS-IoT-SiteWise-Konsole

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich die Option Massenoperationen Neu aus.
3. Wählen Sie Neuer Export, um den Exportvorgang zu starten.
4. Gehen Sie auf der Seite Metadaten exportieren wie folgt vor:

   - Geben Sie einen Namen für den Exportjob ein. Dies ist der Name, der für die exportierte Datei in Ihrem Amazon S3 S3-Bucket verwendet wird.
   - Wählen Sie Ihre zu exportierenden Ressourcen aus, wodurch die Filter für den Job festgelegt werden:
     - Exportieren Sie alle Assets und Asset-Modelle. Verwenden Sie Filter für Assets und Asset-Modelle.
     - Exportieren Sie Vermögenswerte. Filtern Sie nach Ihren Vermögenswerten.
       - Wählen Sie das Asset aus, das für den Exportfilter verwendet werden soll.
       - (Optional) Fügen Sie den Nachwuchs oder das zugehörige Asset-Modell hinzu.
     - Exportieren Sie Asset-Modelle. Filtern Sie nach Ihren Asset-Modellen.
       - Wählen Sie das Asset-Modell aus, das für den Exportfilter verwendet werden soll.
       - (Optional) Fügen Sie den Nachwuchs oder das zugehörige Asset oder beides hinzu.
     - Wählen Sie Weiter aus.
   - Navigieren Sie zum Amazon S3 S3-Bucket:
     - Wählen Sie Amazon S3 durchsuchen, um den Amazon S3 S3-Bucket und die Dateien anzuzeigen.
     - Navigieren Sie zu dem Amazon S3 S3-Bucket, in dem die Datei platziert werden muss.
     - Wählen Sie Weiter aus.
   - Überprüfen Sie den Exportauftrag und wählen Sie Exportieren.

5. Auf der Seite „Massenoperationen für SiteWise Metadaten“ von AWS-IoT-SiteWise-Konsole wird der neu erstellte Importauftrag in der Fortschrittstabelle der Jobs angezeigt.

Informationen zu den verschiedenen Möglichkeiten, Filter beim Exportieren von Metadaten zu verwenden, finden Sie unterBeispiele für den Export von Metadaten.

Metadaten exportieren (AWS CLI)

Das folgende Verfahren erklärt die AWS CLI Exportaktion:

Daten von AWS IoT SiteWise zu Amazon S3 exportieren

1. Erstellen Sie eine JSON-Datei mit Ihrem Anfragetext. Der Anforderungstext gibt die Quelle und das Ziel für den Übertragungsjob an. Das folgende Beispiel zeigt ein Beispiel für einen Anforderungstext:

```
{
    "metadataTransferJobId": "your-transfer-job-Id",
    "sources": [{
        "type": "iotsitewise"
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

   Stellen Sie sicher, dass Sie Ihren Amazon S3 S3-Bucket als Ziel des Metadatentransferjobs angeben.

   > **Note**
   >
   > In diesem Beispiel werden alle Ihre Asset-Modelle und Assets exportiert. Um den Export auf bestimmte Asset-Modelle oder Assets zu beschränken, können Sie Filter in Ihren Anfragetext aufnehmen. Weitere Informationen zum Anwenden von Exportfiltern finden Sie unterBeispiele für den Export von Metadaten.

2. Speichern Sie Ihre Anfragetextdatei, um sie im nächsten Schritt zu verwenden. In diesem Beispiel heißt die Datei `createMetadataTransferJobExport.json`.
3. Rufen Sie die auf, `CreateMetadataTransferJob` indem Sie den folgenden AWS CLI Befehl ausführen:

   ```
   aws iottwinmaker create-metadata-transfer-job --region us-east-1 \
            --cli-input-json file://createMetadataTransferJobExport.json
   ```

   Ersetzen Sie die JSON-Eingabedatei `createMetadataTransferJobExport.json` durch Ihren eigenen Namen der Übertragungsdatei.

Verfolgung des Auftragsfortschritts und Fehlerbehandlung

Die Verarbeitung eines Massenverarbeitungsauftrags nimmt Zeit in Anspruch. Jeder Auftrag wird in der Reihenfolge des AWS IoT SiteWise Eingangs der Anfrage verarbeitet. Es wird one-at-a-time für jedes Konto bearbeitet. Wenn ein Job abgeschlossen ist, beginnt der nächste in der Warteschlange automatisch mit der Verarbeitung. AWS IoT SiteWise löst die Jobs asynchron auf und aktualisiert den Status der einzelnen Jobs im Laufe der Bearbeitung. Jeder Auftrag hat ein Statusfeld, das den Status der Ressource und gegebenenfalls eine Fehlermeldung enthält.

Der Zustand kann einer der folgenden Werte sein:

- `VALIDATING`— Validierung des Jobs einschließlich des übermittelten Dateiformats und seines Inhalts.
- `PENDING`— Der Job befindet sich in einer Warteschlange. Sie können Jobs in diesem Status von der AWS IoT SiteWise Konsole aus stornieren, aber alle anderen Status bleiben bis zum Ende bestehen.
- `RUNNING`— Der Job wird bearbeitet. Es erstellt und aktualisiert Ressourcen, wie in der Importdatei definiert, oder exportiert Ressourcen auf der Grundlage der ausgewählten Exportjobfilter. Wenn der Vorgang abgebrochen wird, werden alle durch diesen Job importierten Ressourcen nicht gelöscht. Weitere Informationen finden Sie unter Überprüfen Sie den Auftragsfortschritt und die Details (Konsole).
- `CANCELLING`— Der Job wird aktiv storniert.

- `ERROR`— Eine oder mehrere Ressourcen konnten nicht verarbeitet werden. Weitere Informationen finden Sie im ausführlichen Auftragsbericht. Weitere Informationen finden Sie unter Überprüfen Sie die Fehlerdetails (Konsole).
- `COMPLETED`— Der Job wurde ohne Fehler abgeschlossen.
- `CANCELLED`— Der Job wurde abgebrochen und befindet sich nicht in der Warteschlange. Wenn Sie einen `RUNNING` Job storniert haben, werden Ressourcen, die zum Zeitpunkt des Abbruchs bereits von diesem Job importiert wurden, nicht gelöscht. AWS IoT SiteWise

Themen

Verfolgung des Fortschritts von Aufträgen

Überprüfen Sie den Auftragsfortschritt und die Details (Konsole)

Sehen Sie Metadaten exportieren (Konsole) sich Metadaten importieren (Konsole) oder an, um einen Sammelauftrag zu starten.

Übersicht über den Auftragsfortschritt in der AWS IoT SiteWise Konsole:

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich die Option Massenoperationen Neu aus.
3. In der Fortschrittstabelle „Aufträge“ in der AWS IoT SiteWise Konsole wird die Liste der Aufträge für Massenvorgänge angezeigt.
4. In der Spalte Jobtyp wird beschrieben, ob es sich um einen Export- oder Importjob handelt. In den Spalten Importdatum wird das Datum angezeigt, an dem der Job gestartet wurde.
5. In der Spalte Status wird der Status des Jobs angezeigt. Sie können einen Job auswählen, um Details zu dem Job zu sehen.
6. Für den ausgewählten Job wird Erfolg angezeigt, wenn er erfolgreich war, oder eine Liste mit Fehlern, wenn der Job fehlgeschlagen ist. Außerdem wird für jeden Ressourcentyp eine Fehlerbeschreibung angezeigt.

Übersicht der Jobdetails in der AWS IoT SiteWise Konsole:

In der Tabelle mit dem Auftragsfortschritt in der AWS IoT SiteWise Konsole wird die Liste der Jobs für Massenvorgänge angezeigt.

1. Wählen Sie einen Job aus, um weitere Details zu sehen.
2. Bei einem Importjob `Data source ARN` steht der für den Amazon S3 S3-Speicherort der Importdatei.
3. Bei einem Exportauftrag `Data destination ARN` steht der für den Amazon S3 S3-Speicherort der Datei nach dem Export.
4. Das `Status` und`Status reason`, geben zusätzliche Details zum aktuellen Job an. Weitere Details finden Sie unter Verfolgung des Auftragsfortschritts und Fehlerbehandlung.
5. Das `Queued position` steht für die Position des Auftrags in der Prozesswarteschlange. Die Jobs werden nacheinander verarbeitet. Eine Position von 1 in der Warteschlange gibt an, dass der Job als Nächstes verarbeitet wird.
6. Auf der Seite mit den Auftragsdetails werden auch die Anzahl der Auftragsfortschritte angezeigt.

    - Es gibt folgende Typen für die Zählung des Auftragsfortschritts:

        i. `Total resources`— Gibt die Gesamtzahl der Anlagen an, die sich im Übertragungsprozess befinden.

        ii. `Succeeded`— Gibt die Anzahl der Vermögenswerte an, die während des Prozesses erfolgreich übertragen wurden.

        iii. `Failed`— Gibt die Anzahl der Anlagen an, die während des Vorgangs ausgefallen sind.

        iv. `Skipped`— Gibt die Anzahl der Assets an, die während des Vorgangs übersprungen wurden.
7. Ein Auftragsstatus von `PENDING` oder zeigt an`VALIDATING`, dass der gesamte Auftragsfortschritt als – gezählt wird. Dies weist darauf hin, dass die Fortschrittszahlen der Jobs ausgewertet werden.
8. Ein Auftragsstatus von `RUNNING` zeigt die `Total resources` Anzahl an, d. h. den Job, der zur Verarbeitung weitergeleitet wurde. Die detaillierten Zählungen (`Succeeded``Failed`, und`Skipped`) beziehen sich auf die verarbeiteten Ressourcen. Die Summe der detaillierten Zählungen ist kleiner als die `Total resources` Anzahl, bis der Status des Jobs `COMPLETED` oder lautet`ERROR`.
9. Wenn der Status eines Jobs `COMPLETED` oder lautet`ERROR`, entspricht die `Total resources` Anzahl der Summe der detaillierten Anzahlen (`Succeeded``Failed`, und`Skipped`).

10. Wenn der Status eines Job lautet`ERROR`, finden Sie in der Tabelle Auftragsfehler Einzelheiten zu den spezifischen Fehlern und Ausfällen. Weitere Details finden Sie unter Überprüfen Sie die Fehlerdetails (Konsole).

Überprüfen Sie den Auftragsfortschritt und die Einzelheiten (AWS CLI)

Nachdem Sie einen Massenvorgang gestartet haben, können Sie seinen Status mithilfe der folgenden API-Aktionen überprüfen oder aktualisieren:

- Verwenden Sie die GetMetadataTransferJobAPI-Aktion, um Informationen zu einem bestimmten Job abzurufen.

  Informationen mit der **`GetMetadataTransferJob`** API abrufen:

  1. Erstellen Sie einen Übertragungsauftrag und führen Sie ihn aus. Rufen Sie die `GetMetadataTransferJob`-API auf.

     Example AWS CLI Befehl:

     ```
     aws iottwinmaker get-metadata-transfer-job \
             --metadata-transfer-job-id your_metadata_transfer_job_id \
             --region your_region
     ```

  2. Die `GetMetadataTransferJob` API gibt ein `MetadataTransferJobProgress` Objekt mit den folgenden Parametern zurück:
     - succeededCount — Gibt die Anzahl der Assets an, die im Prozess erfolgreich übertragen wurden.
     - FailedCount — Gibt die Anzahl der Assets an, die während des Vorgangs ausgefallen sind.
     - skippedCount — Gibt die Anzahl der Assets an, die während des Vorgangs übersprungen wurden.
     - TotalCount — Gibt die Gesamtzahl der Vermögenswerte an, die sich im Übertragungsprozess befinden.

     Diese Parameter geben den Status des Auftragsfortschritts an. Wenn der Status lautet`RUNNING`, helfen sie dabei, die Anzahl der Ressourcen nachzuverfolgen, die noch verarbeitet werden müssen.

Wenn bei der Schemavalidierung Fehler auftreten oder wenn FailedCount größer oder gleich 1 ist, wechselt der Status des Jobs zu. ERROR Ein vollständiger Fehlerbericht für den Job wird in Ihrem Amazon S3 S3-Bucket abgelegt. Weitere Details finden Sie unter Überprüfen Sie die Fehler.

- Verwenden Sie die ListMetadataTransferJobsAPI-Aktion, um aktuelle Jobs aufzulisten.

  Verwenden Sie eine JSON-Datei, um die zurückgegebenen Jobs nach ihrem aktuellen Status zu filtern. Sehen Sie sich das folgende Verfahren an:

  1. Um die Filter anzugeben, die Sie verwenden möchten, erstellen Sie eine AWS CLI JSON-Eingabedatei. Sie möchten Folgendes verwenden:

     ```
     {
         "sourceType": "s3",
         "destinationType": "iottwinmaker",
         "filters": [{
             "state": "COMPLETED"
         }]
     }
     ```

     Eine Liste der gültigen `state` Werte finden Sie unter ListMetadataTransferJobsFilter im AWS IoT TwinMaker API-Referenzhandbuch.

  2. Verwenden Sie die JSON-Datei als Argument im folgenden AWS CLI Beispielbefehl:

     ```
     aws iottwinmaker list-metadata-transfer-job --region your_region \
             --cli-input-json file://ListMetadataTransferJobsExample.json
     ```

- Verwenden Sie die CancelMetadataTransferJobAPI-Aktion, um einen Job abzubrechen. Diese API storniert den spezifischen Metadatentransferauftrag, ohne dass sich dies auf bereits exportierte oder importierte Ressourcen auswirkt:

  ```
  aws iottwinmaker cancel-metadata-transfer-job \
          --region your_region \
          --metadata-transfer-job-id job-to-cancel-id
  ```

Überprüfen Sie die Fehler

Überprüfen Sie die Fehlerdetails (Konsole)

Fehlerdetails in der AWS IoT SiteWise Konsole:

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Eine Liste der Aufträge AWS-IoT-SiteWise-Konsole für Massenvorgänge finden Sie in der Tabelle mit dem Auftragsfortschritt unter.
3. Wählen Sie einen Auftrag aus, um die Auftragsdetails anzuzeigen.
4. Wenn der Status eines Jobs `COMPLETED` oder lautet`ERROR`, entspricht die `Total resources` Anzahl der Summe der detaillierten Anzahlen (`SucceededFailed`, und`Skipped`).
5. Wenn der Status eines Job lautet`ERROR`, finden Sie in der Tabelle Auftragsfehler Einzelheiten zu den spezifischen Fehlern und Ausfällen.
6. In der Tabelle Auftragsfehler wird der Inhalt des Jobberichts angezeigt. Das `Resource type` Feld gibt den Ort des Fehlers oder der Ausfälle an, z. B. im Folgenden:

   - Ein Validierungsfehler im `Resource type` Feld weist beispielsweise darauf hin, dass die Importvorlage und das Metadaten-Schemadateiformat nicht übereinstimmen. `Bulk operations template` Weitere Informationen finden Sie unter AWS IoT SiteWise Auftragsschema für die Übertragung von Metadaten.
   - Ein Fehler `Asset` im `Resource type` Feld bedeutet, dass das Asset aufgrund eines Konflikts mit einem anderen Asset nicht erstellt wurde. Informationen zu AWS IoT SiteWise Ressourcenfehlern und Konflikten finden Sie unter Häufige Fehler.

Überprüfen Sie die Fehlerdetails (AWS CLI)

Informationen zur Behandlung und Diagnose von Fehlern, die während eines Übertragungsauftrags auftreten, finden Sie im folgenden Verfahren zur Verwendung der `GetMetadataTransferJob` API-Aktion:

1. Rufen Sie nach dem Erstellen und Ausführen eines Übertragungsauftrags folgenden Befehl auf GetMetadataTransferJob:

```
aws iottwinmaker get-metadata-transfer-job \
        --metadata-transfer-job-id your_metadata_transfer_job_id \
        --region us-east-1
```

2. Sobald der Status des Auftrags angezeigt wird`COMPLETED`, können Sie mit der Überprüfung der Ergebnisse des Auftrags beginnen.
3. Wenn Sie aufrufen`GetMetadataTransferJob`, wird ein Objekt zurückgegeben, das aufgerufen wurde `MetadataTransferJobProgress`.

   Das MetadataTransferJobProgress Objekt enthält die folgenden Parameter:

   - FailedCount: Gibt die Anzahl der Assets an, die während des Übertragungsvorgangs ausgefallen sind.
   - skippedCount: Gibt die Anzahl der Assets an, die während des Übertragungsvorgangs übersprungen wurden.
   - succeededCount: Gibt die Anzahl der Assets an, die während des Übertragungsvorgangs erfolgreich waren.
   - TotalCount: Gibt die Gesamtzahl der am Übertragungsprozess beteiligten Vermögenswerte an.
4. Darüber hinaus gibt der API-Aufruf ein Element zurück`reportUrl`, das eine vorsignierte URL enthält. Wenn bei Ihrem Übertragungsauftrag Probleme auftreten, die Sie weiter untersuchen müssen, besuchen Sie diese URL.

Beispiele für den Import von Metadaten

In diesem Abschnitt wird gezeigt, wie Sie Metadatendateien erstellen, um Asset-Modelle und Assets mit einem einzigen Massenimportvorgang zu importieren.

Beispiel für einen Massenimport

Sie können viele Asset-Modelle und Assets mit einem einzigen Massenimportvorgang importieren. Das folgende Beispiel zeigt, wie Sie zu diesem Zweck eine Metadatendatei erstellen.

In diesem Beispielszenario haben Sie verschiedene Baustellen, auf denen Industrieroboter in Arbeitszellen installiert sind.

Das Beispiel definiert zwei Anlagenmodelle:

- `RobotModel1`: Dieses Anlagenmodell stellt einen bestimmten Robotertyp dar, den Sie auf Ihren Baustellen einsetzen. Der Roboter hat eine Messeigenschaft,`Temperature`.

- `WorkCell`: Dieses Anlagenmodell stellt eine Sammlung von Robotern auf einer Ihrer Baustellen dar. Das Anlagenmodell definiert eine Hierarchie`robotHierarchyOEM1`, um die Beziehung zwischen Robotern in einer Arbeitszelle darzustellen.

Das Beispiel definiert auch einige Vermögenswerte:

- `WorkCell1`: eine Arbeitszelle an Ihrem Standort in Boston
- `RobotArm123456`: ein Roboter in dieser Arbeitszelle
- `RobotArm987654`: ein weiterer Roboter in dieser Arbeitszelle

Die folgende JSON-Metadatendatei definiert diese Asset-Modelle und Assets. Wenn Sie einen Massenimport mit diesen Metadaten ausführen, werden die darin enthaltenen Asset-Modelle und Assets AWS IoT SiteWise einschließlich ihrer hierarchischen Beziehungen erstellt.

Metadatendatei für den Import

```
{
    "assetModels": [
        {
            "assetModelExternalId": "Robot.OEM1.3536",
            "assetModelName": "RobotModel1",
            "assetModelProperties": [
                {
                    "dataType": "DOUBLE",
                    "externalId": "Temperature",
                    "name": "Temperature",
                    "type": {
                        "measurement": {
                            "processingConfig": {
                                "forwardingConfig": {
                                    "state": "ENABLED"
                                }
                            }
                        }
                    },
                    "unit": "fahrenheit"
                }
            ]
        },
        {
```

```
            "assetModelExternalId": "ISA95.WorkCell",
            "assetModelName": "WorkCell",
            "assetModelProperties": [],
            "assetModelHierarchies": [
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "name": "robotHierarchyOEM1",
                    "childAssetModelExternalId": "Robot.OEM1.3536"
                }
            ]
        }
    ],
    "assets": [
        {
            "assetExternalId": "Robot.OEM1.3536.123456",
            "assetName": "RobotArm123456",
            "assetModelExternalId": "Robot.OEM1.3536"
        },
        {
            "assetExternalId": "Robot.OEM1.3536.987654",
            "assetName": "RobotArm987654",
            "assetModelExternalId": "Robot.OEM1.3536"
        },
        {
            "assetExternalId": "BostonSite.Area1.Line1.WorkCell1",
            "assetName": "WorkCell1",
            "assetModelExternalId": "ISA95.WorkCell",
            "assetHierarchies": [
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "childAssetExternalId": "Robot.OEM1.3536.123456"
                },
                {
                    "externalId": "workCellHierarchyWithOEM1Robot",
                    "childAssetExternalId": "Robot.OEM1.3536.987654"
                }
            ]
        }
    ]
}
```

Beispiel für das erste Onboarding von Modellen und Ressourcen

In diesem Beispielszenario gibt es in einem Unternehmen verschiedene Baustellen mit Industrierobotern.

Das Beispiel definiert mehrere Anlagenmodelle:

- `Sample_Enterprise`— Dieses Vermögensmodell steht für das Unternehmen, zu dem die Standorte gehören. Das Anlagenmodell definiert eine Hierarchie`Enterprise to Site`, um die Beziehung der Standorte zum Unternehmen darzustellen.
- `Sample_Site`— Dieses Anlagenmodell repräsentiert die Produktionsstätten innerhalb des Unternehmens. Das Anlagenmodell definiert eine Hierarchie`Site to Line`, um die Beziehung der Linien zum Standort darzustellen.
- `Sample_Welding Line`— Dieses Anlagenmodell stellt eine Montagelinie innerhalb von Baustellen dar. Das Anlagenmodell definiert eine Hierarchie`Line to Robot`, um die Beziehung der Roboter zur Linie darzustellen.
- `Sample_Welding Robot`— Dieses Anlagenmodell steht für einen bestimmten Robotertyp auf Ihren Baustellen.

Das Beispiel definiert auch Vermögenswerte auf der Grundlage der Anlagenmodelle.

- `Sample_AnyCompany Motor`— Dieses Asset wird anhand des `Sample_Enterprise` Asset-Modells erstellt.
- `Sample_Chicago`— Dieses Asset wurde anhand des `Sample_Site` Asset-Modells erstellt.
- `Sample_Welding Line 1`— Dieses Asset wurde anhand des `Sample_Welding Line` Asset-Modells erstellt.
- `Sample_Welding Robot 1`— Dieses Asset wurde anhand des `Sample_Welding Robot` Asset-Modells erstellt.
- `Sample_Welding Robot 2`— Dieses Asset wurde anhand des `Sample_Welding Robot` Asset-Modells erstellt.

Die folgende JSON-Metadatendatei definiert diese Asset-Modelle und Assets. Wenn Sie einen Massenimport mit diesen Metadaten ausführen, werden die darin enthaltenen Asset-Modelle und Assets AWS IoT SiteWise einschließlich ihrer hierarchischen Beziehungen erstellt.

JSON-Datei zur Einbindung von Assets und Modellen für den Import

```
{
    "assetModels": [
        {
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetModelName": "Sample_Welding Robot",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "name": "Serial Number",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "name": "CycleCount",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "EA"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "name": "Joint 1 Current",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Max_Current",
                    "name": "Max Joint 1 Current",
                    "type": {
                        "metric": {
```

```
                            "expression": "max(joint1current)",
                            "variables": [
                                {
                                    "name": "joint1current",
                                    "value": {
                                        "propertyExternalId":
"External_Id_Welding_Robot_Joint_1_Current"
                                    }
                                }
                            ],
                            "window": {
                                "tumbling": {
                                    "interval": "5m"
                                }
                            }
                        }
                    },
                    "unit": "Amps"
                }
            ]
        },
        {
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetModelName": "Sample_Welding Line",
            "assetModelProperties": [
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Line_Availability",
                    "name": "Availability",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "%"
                }
            ],
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "name": "Line to Robot",
                    "childAssetModelExternalId": "External_Id_Welding_Robot"
                }
            ]
        },
        {
```

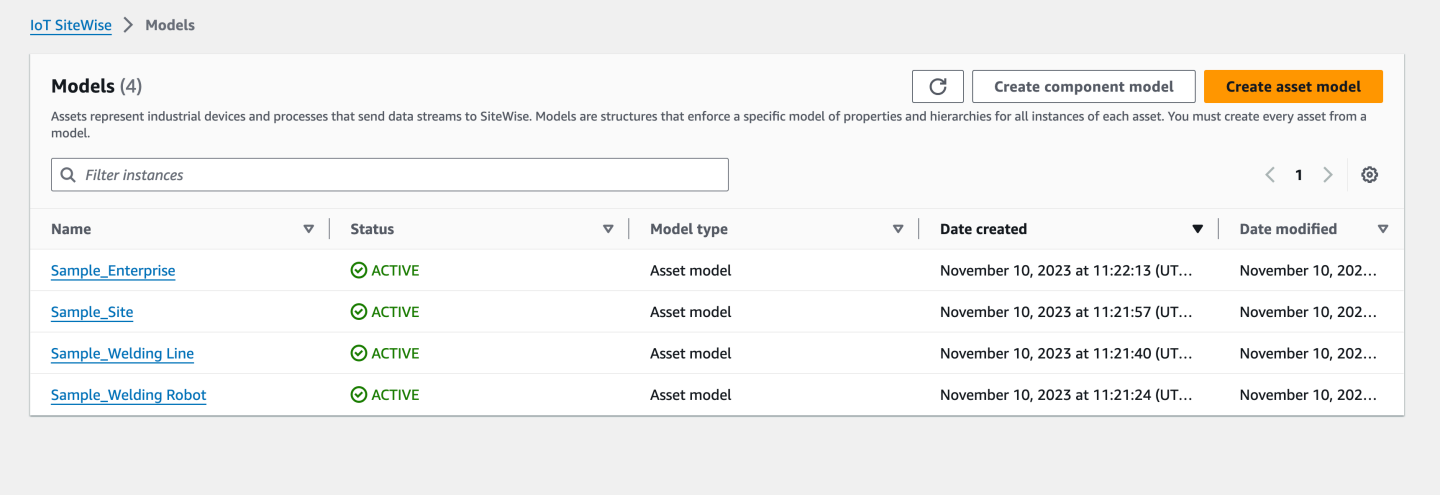
```
            "assetModelExternalId": "External_Id_Site",
            "assetModelName": "Sample_Site",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Site_Street_Address",
                    "name": "Street Address",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                }
            ],
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "name": "Site to Line",
                    "childAssetModelExternalId": "External_Id_Welding_Line"
                }
            ]
        },
        {
            "assetModelExternalId": "External_Id_Enterprise",
            "assetModelName": "Sample_Enterprise",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "name": "Company Name",
                    "externalId": "External_Id_Enterprise_Company_Name",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                }
            ],
            "assetModelHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "name": "Enterprise to Site",
                    "childAssetModelExternalId": "External_Id_Site"
```

```
                }
            ]
        }
    ],
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_1",
            "assetName": "Sample_Welding Robot 1",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S1000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S1000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_2",
            "assetName": "Sample_Welding Robot 2",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S2000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S2000/1/Current"
                }
            ]
        },
        {
```

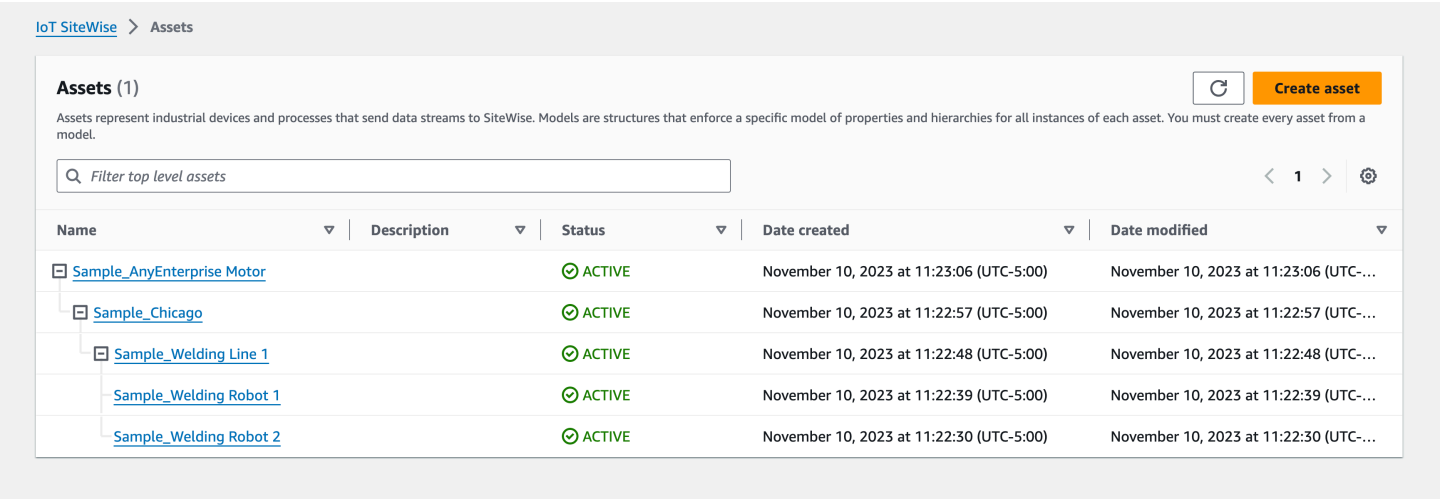
```
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Line_Availability",
                    "alias": "AnyCompany/Chicago/Welding Line/Availability"
                }
            ],
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Enterprise_AnyCompany",
            "assetName": "Sample_AnyEnterprise Motor",
            "assetModelExternalId": "External_Id_Enterprise",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Enterprise_TO_Site",
                    "childAssetExternalId": "External_Id_Site_Chicago"
                }
            ]
        }
    ]
```

```
}
```

Der folgende Screenshot zeigt Modelle, die AWS-IoT-SiteWise-Konsole nach der Ausführung des vorherigen Codebeispiels angezeigt werden.



Der folgende Screenshot zeigt Modelle, Anlagen und Hierarchien, die AWS-IoT-SiteWise-Konsole nach der Ausführung des vorherigen Codebeispiels angezeigt werden.



Beispiel für das Onboarding zusätzlicher Ressourcen

In diesem Beispiel werden zusätzliche Vermögenswerte definiert, die in ein vorhandenes Vermögensmodell in Ihrem Konto importiert werden sollen:

- `Sample_Welding Line 2`— Dieses Asset wird anhand des `Sample_Welding Line` Asset-Modells erstellt.

- `Sample_Welding Robot 3`— Dieses Asset wurde anhand des `Sample_Welding Robot` Asset-Modells erstellt.
- `Sample_Welding Robot 4`— Dieses Asset wurde anhand des `Sample_Welding Robot` Asset-Modells erstellt.

Informationen zum Erstellen der ersten Anlagen für dieses Beispiel finden Sie unterBeispiel für das erste Onboarding von Modellen und Ressourcen.

Die folgende JSON-Metadatendatei definiert diese Asset-Modelle und Assets. Wenn Sie einen Massenimport mit diesen Metadaten ausführen, werden die darin enthaltenen Asset-Modelle und Assets AWS IoT SiteWise einschließlich ihrer hierarchischen Beziehungen erstellt.

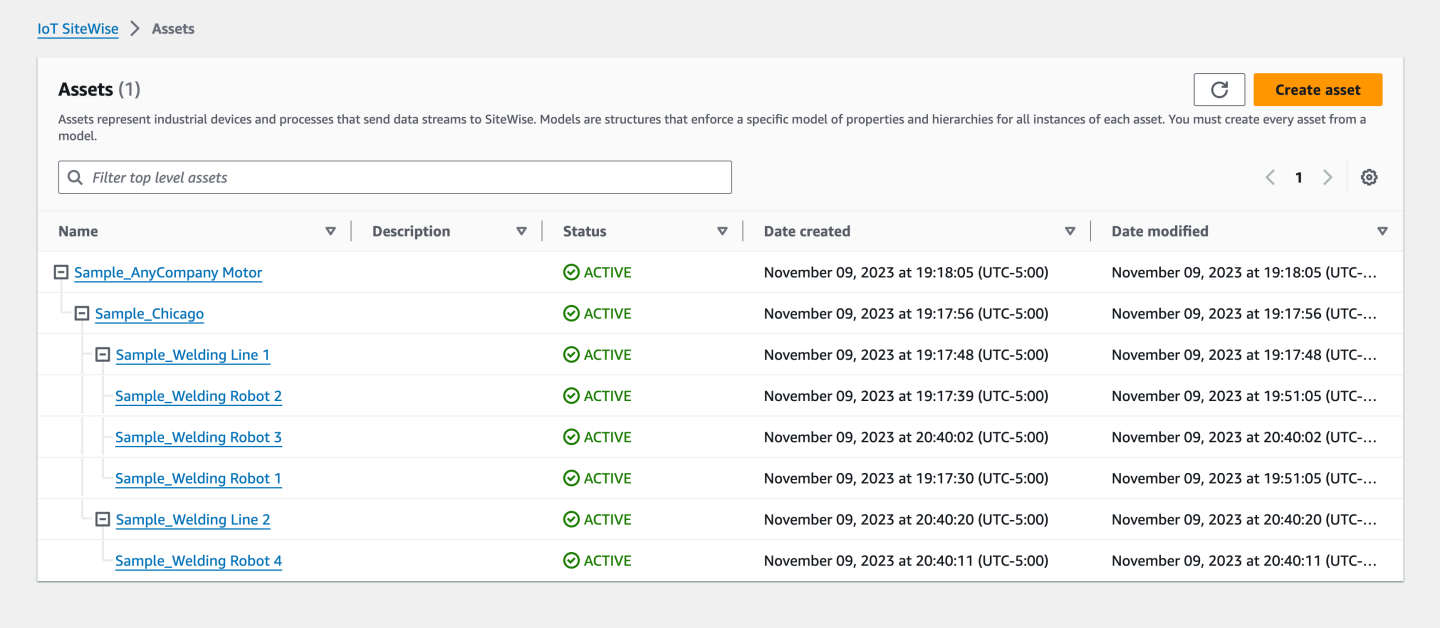
JSON-Datei zum Onboarding zusätzlicher Assets

```
{
    "assets": [
        {
            "assetExternalId": "External_Id_Welding_Robot_3",
            "assetName": "Sample_Welding Robot 3",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S3000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S3000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Robot_4",
            "assetName": "Sample_Welding Robot 4",
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetProperties": [
                {
```

```
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "attributeValue": "S4000"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/Count"
                },
                {
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "alias": "AnyCompany/Chicago/Welding Line/S4000/1/Current"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_1",
            "assetName": "Sample_Welding Line 1",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_1"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_2"
                },
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_3"
                }
            ]
        },
        {
            "assetExternalId": "External_Id_Welding_Line_2",
            "assetName": "Sample_Welding Line 2",
            "assetModelExternalId": "External_Id_Welding_Line",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Welding_Line_TO_Robot",
                    "childAssetExternalId": "External_Id_Welding_Robot_4"
                }
            ]
        },
        {
```

```
            "assetExternalId": "External_Id_Site_Chicago",
            "assetName": "Sample_Chicago",
            "assetModelExternalId": "External_Id_Site",
            "assetHierarchies": [
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_1"
                },
                {
                    "externalId": "External_Id_Site_TO_Line",
                    "childAssetExternalId": "External_Id_Welding_Line_2"
                }
            ]
        }
    ]
}
```

Der folgende Screenshot zeigt Modelle, Assets und Hierarchien, die AWS-IoT-SiteWise-Konsole nach der Ausführung des vorherigen Codebeispiels angezeigt werden.



Beispiel für das Onboarding neuer Immobilien

In diesem Beispiel werden neue Immobilien in bestehenden Anlagemodellen definiert. Erfahren SieBeispiel für das Onboarding zusätzlicher Ressourcen, wie Sie zusätzliche Anlagen und Modelle integrieren können.

- `Joint 1 Temperature`— Diese Eigenschaft wird dem `Sample_Welding Robot` Asset-Modell hinzugefügt. Diese neue Eigenschaft wird auch auf jedes Asset übertragen, das mit dem `Sample_Welding Robot` Asset-Modell erstellt wurde.

Informationen zum Hinzufügen einer neuen Eigenschaft zu einem vorhandenen Asset-Modell finden Sie im folgenden Beispiel für eine JSON-Metadatendatei. Wie in der JSON-Datei gezeigt, muss die gesamte bestehende `Sample_Welding Robot` Asset-Modelldefinition zusammen mit der neuen Eigenschaft bereitgestellt werden. Wenn die gesamte Eigenschaftsliste aus der vorhandenen Definition nicht bereitgestellt wird, werden die ausgelassenen Eigenschaften AWS IoT SiteWise gelöscht.

JSON-Datei zum Integrieren neuer Eigenschaften

In diesem Beispiel wird dem Asset-Modell eine neue Eigenschaft `Joint 1 Temperature` hinzugefügt.

```
{
    "assetModels": [
        {
            "assetModelExternalId": "External_Id_Welding_Robot",
            "assetModelName": "Sample_Welding Robot",
            "assetModelProperties": [
                {
                    "dataType": "STRING",
                    "externalId": "External_Id_Welding_Robot_Serial_Number",
                    "name": "Serial Number",
                    "type": {
                        "attribute": {
                            "defaultValue": "-"
                        }
                    },
                    "unit": "-"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Cycle_Count",
                    "name": "CycleCount",
                    "type": {
                        "measurement": {}
                    },
```

```
                    "unit": "EA"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Current",
                    "name": "Joint 1 Current",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Max_Current",
                    "name": "Max Joint 1 Current",
                    "type": {
                        "metric": {
                            "expression": "max(joint1current)",
                            "variables": [
                                {
                                    "name": "joint1current",
                                    "value": {
                                        "propertyExternalId":
"External_Id_Welding_Robot_Joint_1_Current"
                                    }
                                }
                            ],
                            "window": {
                                "tumbling": {
                                    "interval": "5m"
                                }
                            }
                        }
                    },
                    "unit": "Amps"
                },
                {
                    "dataType": "DOUBLE",
                    "externalId": "External_Id_Welding_Robot_Joint_1_Temperature",
                    "name": "Joint 1 Temperature",
                    "type": {
                        "measurement": {}
                    },
                    "unit": "degC"
```

```
                }
            ]
        }
    ]
}
```

Beispiele für den Export von Metadaten

Wenn Sie einen Massenexport Ihrer AWS IoT SiteWise Inhalte nach Amazon S3 durchführen, können Sie Filter angeben, um einzuschränken, welche spezifischen Asset-Modelle und Assets Sie exportieren möchten.

Sie geben die Filter in einem `iotSiteWiseConfiguration` Abschnitt innerhalb des `sources` Abschnitts Ihres Anfragetextes an.

> **Note**
>
> Sie können mehrere Filter einbeziehen. Bei der Massenoperation werden alle Asset-Modelle oder Assets exportiert, die einem der Filter entsprechen.
> Wenn Sie keine Filter angeben, exportiert der Vorgang alle Ihre Asset-Modelle und Assets.

```
{
    "metadataTransferJobId": "your-transfer-job-id",
    "sources": [{
        "type": "iotsitewise",
        "iotSiteWiseConfiguration": {
            "filters": [{
                list of filters
            }]
        }
    }],
    "destination": {
        "type": "s3",
        "s3Configuration": {
            "location": "arn:aws:s3:::your-S3-bucket-location"
        }
    }
}
```

Filterung nach Asset-Modell

Sie können ein bestimmtes Asset-Modell filtern. Sie können auch alle Anlagen, die dieses Modell verwenden, oder alle Anlagenmodelle innerhalb seiner Hierarchie einbeziehen. Sie können nicht sowohl Vermögenswerte als auch Hierarchien einbeziehen.

Weitere Informationen zu Hierarchien finden Sie unter Definition von Hierarchien für Anlagenmodelle.

Asset model

Dieser Filter umfasst das angegebene Asset-Modell:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID"
}
```

Asset model and its assets

Dieser Filter umfasst das angegebene Asset-Modell sowie alle Assets, die dieses Asset-Modell verwenden:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeAssets": true
}
```

Asset model and its hierarchy

Dieser Filter umfasst das angegebene Asset-Modell zusammen mit allen zugehörigen Asset-Modellen in seiner Hierarchie:

```
"filterByAssetModel": {
    "assetModelId": "asset model ID",
    "includeOffspring": true
}
```

Nach Vermögenswert filtern

Sie können ein bestimmtes Asset filtern. Sie können auch das zugehörige Asset-Modell oder alle zugehörigen Assets in die Hierarchie einbeziehen. Sie können nicht sowohl das Vermögensmodell als auch die Hierarchie einbeziehen.

Weitere Informationen zu Hierarchien finden Sie unter Definition von Hierarchien für Anlagenmodelle.

Asset

Dieser Filter umfasst das angegebene Asset:

```
"filterByAsset": {
    "assetId": "asset ID"
}
```

Asset and its asset model

Dieser Filter umfasst das angegebene Asset zusammen mit dem verwendeten Asset-Modell:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeAssetModel": true
}
```

Asset and its hierarchy

Dieser Filter umfasst das angegebene Asset zusammen mit allen zugehörigen Assets in seiner Hierarchie:

```
"filterByAsset": {
    "assetId": "asset ID",
    "includeOffspring": true
}
```

AWS IoT SiteWise Auftragsschema für die Übertragung von Metadaten

Verwenden Sie das Auftragsschema für die AWS IoT SiteWise Metadatentransferübertragung als Referenz, wenn Sie Ihre eigenen Massenimport- und -exportvorgänge durchführen:

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "IoTSiteWise",
  "description": "Metadata transfer job resource schema for IoTSiteWise",
  "definitions": {
    "Name": {
      "type": "string",
```

```
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "Description": {
      "type": "string",
      "minLength": 1,
      "maxLength": 2048,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "ID": {
      "type": "string",
      "minLength": 36,
      "maxLength": 36,
      "pattern": "^[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$"
    },
    "ExternalId": {
      "type": "string",
      "minLength": 2,
      "maxLength": 128,
      "pattern": "[a-zA-Z0-9_][a-zA-Z_\\-0-9.:]*[a-zA-Z0-9_]+"
    },
    "AttributeValue": {
      "description": "The value of the property attribute.",
      "type": "string",
      "minLength": 1,
      "maxLength": 1024,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyUnit": {
      "description": "The unit of measure (such as Newtons or RPM) of the asset
property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 256,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
    "PropertyAlias": {
      "description": "The property alias that identifies the property.",
      "type": "string",
      "minLength": 1,
      "maxLength": 1000,
      "pattern": "[^\\u0000-\\u001F\\u007F]+"
    },
```

```
    "AssetProperty": {
      "description": "The asset property's definition, alias, unit, and notification
 state.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset property.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset property.",
          "$ref": "#/definitions/ExternalId"
        },
        "alias": {
          "$ref": "#/definitions/PropertyAlias"
        },
        "unit": {
          "$ref": "#/definitions/PropertyUnit"
        },
        "attributeValue": {
          "$ref": "#/definitions/AttributeValue"
        },
        "retainDataOnAliasChange": {
          "type": "string",
          "default": "TRUE",
          "enum": [
            "TRUE",
            "FALSE"
          ]
        },
        "propertyNotificationState": {
```

```
          "description": "The MQTT notification state (ENABLED or DISABLED) for this
 asset property.",
          "type": "string",
          "enum": [
            "ENABLED",
            "DISABLED"
          ]
        }
      }
    },
    "AssetHierarchy": {
      "description": "A hierarchy specifies allowed parent/child asset relationships.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetId"
          ]
        },
        {
          "required": [
            "id",
            "childAssetExternalId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetExternalId"
          ]
        }
      ],
      "properties": {
        "id": {
          "description": "The ID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ID"
```

```
        },
        "externalId": {
          "description": "The ExternalID of a hierarchy in the parent asset's model.",
          "$ref": "#/definitions/ExternalId"
        },
        "childAssetId": {
          "description": "The ID of the child asset to be associated.",
          "$ref": "#/definitions/ID"
        },
        "childAssetExternalId": {
          "description": "The ExternalID of the child asset to be associated.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "Tag": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "key",
        "value"
      ],
      "properties": {
        "key": {
          "type": "string"
        },
        "value": {
          "type": "string"
        }
      }
    },
    "AssetModelType": {
      "type": "string",
      "default": null,
      "enum": [
        "ASSET_MODEL",
        "COMPONENT_MODEL"
      ]
    },
    "AssetModelCompositeModel": {
      "description": "Contains a composite model definition in an asset model. This
composite model definition is applied to all assets created from the asset model.",
      "type": "object",
      "additionalProperties": false,
```

```
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model composite model.",
          "$ref": "#/definitions/ExternalId"
        },
        "parentId": {
          "description": "The ID of the parent asset model composite model.",
          "$ref": "#/definitions/ID"
        },
        "parentExternalId": {
          "description": "The ExternalID of the parent asset model composite model.",
          "$ref": "#/definitions/ExternalId"
        },
        "composedAssetModelId": {
          "description": "The ID of the composed asset model.",
          "$ref": "#/definitions/ID"
        },
        "composedAssetModelExternalId": {
          "description": "The ExternalID of the composed asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "description": {
          "description": "A description for the asset composite model.",
          "$ref": "#/definitions/Description"
```

```
        },
        "name": {
          "description": "A unique, friendly name for the asset composite model.",
          "$ref": "#/definitions/Name"
        },
        "type": {
          "description": "The type of the composite model. For alarm composite models,
 this type is AWS/ALARM.",
          "$ref": "#/definitions/Name"
        },
        "properties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
          }
        }
      }
    },
    "AssetModelProperty": {
      "description": "Contains information about an asset model property.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id"
          ]
        },
        {
          "required": [
            "externalId"
          ]
        }
      ],
      "required": [
        "name",
        "dataType",
        "type"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model property.",
          "$ref": "#/definitions/ID"
```

```
        },
        "externalId": {
          "description": "The ExternalID of the asset model property.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
          "description": "The name of the asset model property.",
          "$ref": "#/definitions/Name"
        },
        "dataType": {
          "description": "The data type of the asset model property.",
          "$ref": "#/definitions/DataType"
        },
        "dataTypeSpec": {
          "description": "The data type of the structure for this property.",
          "$ref": "#/definitions/Name"
        },
        "unit": {
          "description": "The unit of the asset model property, such as Newtons or
RPM.",
          "type": "string",
          "minLength": 1,
          "maxLength": 256,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
        },
        "type": {
          "description": "The property type",
          "$ref": "#/definitions/PropertyType"
        }
      }
    },
    "DataType": {
      "type": "string",
      "enum": [
        "STRING",
        "INTEGER",
        "DOUBLE",
        "BOOLEAN",
        "STRUCT"
      ]
    },
    "PropertyType": {
      "description": "Contains a property type, which can be one of attribute,
measurement, metric, or transform.",
```

```
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "attribute": {
          "$ref": "#/definitions/Attribute"
        },
        "transform": {
          "$ref": "#/definitions/Transform"
        },
        "metric": {
          "$ref": "#/definitions/Metric"
        },
        "measurement": {
          "$ref": "#/definitions/Measurement"
        }
      }
    },
    "Attribute": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "defaultValue": {
          "type": "string",
          "minLength": 1,
          "maxLength": 1024,
          "pattern": "[^\\u0000-\\u001F\\u007F]+"
        }
      }
    },
    "Transform": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the transformation
function.",
          "type": "string",
          "minLength": 1,
          "maxLength": 1024
        },
```

```
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/ExpressionVariable"
          }
        },
        "processingConfig": {
          "$ref": "#/definitions/TransformProcessingConfig"
        }
      }
    },
    "TransformProcessingConfig": {
      "description": "The processing configuration for the given transform property.",
      "type": "object",
      "additionalProperties": false,
      "required": [
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given transform property.",
          "$ref": "#/definitions/ComputeLocation"
        },
        "forwardingConfig": {
          "description": "The forwarding configuration for a given property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "Metric": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "expression",
        "variables",
        "window"
      ],
      "properties": {
        "expression": {
          "description": "The mathematical expression that defines the metric
aggregation function.",
          "type": "string",
          "minLength": 1,
```

```
          "maxLength": 1024
        },
        "variables": {
          "description": "The list of variables used in the expression.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/ExpressionVariable"
          }
        },
        "window": {
          "description": "The window (time interval) over which AWS IoT SiteWise
computes the metric's aggregation expression",
          "$ref": "#/definitions/MetricWindow"
        },
        "processingConfig": {
          "$ref": "#/definitions/MetricProcessingConfig"
        }
      }
    },
    "MetricProcessingConfig": {
      "description": "The processing configuration for the metric.",
      "type": "object",
      "additionalProperties": false,
      "required": [
        "computeLocation"
      ],
      "properties": {
        "computeLocation": {
          "description": "The compute location for the given metric property.",
          "$ref": "#/definitions/ComputeLocation"
        }
      }
    },
    "ComputeLocation": {
      "type": "string",
      "enum": [
        "EDGE",
        "CLOUD"
      ]
    },
    "ForwardingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
```

```
        "state"
      ],
      "properties": {
        "state": {
          "type": "string",
          "enum": [
            "ENABLED",
            "DISABLED"
          ]
        }
      }
    },
    "MetricWindow": {
      "description": "Contains a time interval window used for data aggregate
computations (for example, average, sum, count, and so on).",
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "tumbling": {
          "description": "The tumbling time interval window.",
          "type": "object",
          "additionalProperties": false,
          "required": [
            "interval"
          ],
          "properties": {
            "interval": {
              "description": "The time interval for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 23
            },
            "offset": {
              "description": "The offset for the tumbling window.",
              "type": "string",
              "minLength": 2,
              "maxLength": 25
            }
          }
        }
      }
    },
    "ExpressionVariable": {
      "type": "object",
```

```
      "additionalProperties": false,
      "required": [
        "name",
        "value"
      ],
      "properties": {
        "name": {
          "description": "The friendly name of the variable to be used in the
expression.",
          "type": "string",
          "minLength": 1,
          "maxLength": 64,
          "pattern": "^[a-z][a-z0-9_]*$"
        },
        "value": {
          "description": "The variable that identifies an asset property from which to
use values.",
          "$ref": "#/definitions/VariableValue"
        }
      }
    },
    "VariableValue": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "propertyId"
          ]
        },
        {
          "required": [
            "propertyExternalId"
          ]
        }
      ],
      "properties": {
        "propertyId": {
          "$ref": "#/definitions/ID"
        },
        "propertyExternalId": {
          "$ref": "#/definitions/ExternalId"
        },
        "hierarchyId": {
```

```
          "$ref": "#/definitions/ID"
        },
        "hierarchyExternalId": {
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
    "Measurement": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "processingConfig": {
          "$ref": "#/definitions/MeasurementProcessingConfig"
        }
      }
    },
    "MeasurementProcessingConfig": {
      "type": "object",
      "additionalProperties": false,
      "required": [
        "forwardingConfig"
      ],
      "properties": {
        "forwardingConfig": {
          "description": "The forwarding configuration for the given measurement
property.",
          "$ref": "#/definitions/ForwardingConfig"
        }
      }
    },
    "AssetModelHierarchy": {
      "description": "Contains information about an asset model hierarchy.",
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "id",
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "id",
```

```
            "childAssetModelExternalId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetModelId"
          ]
        },
        {
          "required": [
            "externalId",
            "childAssetModelExternalId"
          ]
        }
      ],
      "required": [
        "name"
      ],
      "properties": {
        "id": {
          "description": "The ID of the asset model hierarchy.",
          "$ref": "#/definitions/ID"
        },
        "externalId": {
          "description": "The ExternalID of the asset model hierarchy.",
          "$ref": "#/definitions/ExternalId"
        },
        "name": {
          "description": "The name of the asset model hierarchy.",
          "$ref": "#/definitions/Name"
        },
        "childAssetModelId": {
          "description": "The ID of the asset model. All assets in this hierarchy must
be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ID"
        },
        "childAssetModelExternalId": {
          "description": "The ExternalID of the asset model. All assets in this
hierarchy must be instances of the child AssetModelId asset model.",
          "$ref": "#/definitions/ExternalId"
        }
      }
    },
```

```
    "AssetModel": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetModelName"
      ],
      "properties": {
        "assetModelId": {
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
          "description": "The ID of the asset model.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelName": {
          "description": "A unique, friendly name for the asset model.",
          "$ref": "#/definitions/Name"
        },
        "assetModelDescription": {
          "description": "A description for the asset model.",
          "$ref": "#/definitions/Description"
        },
        "assetModelType": {
          "description": "The type of the asset model.",
          "$ref": "#/definitions/AssetModelType"
        },
        "assetModelProperties": {
          "description": "The property definitions of the asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelProperty"
```

```
          }
        },
        "assetModelCompositeModels": {
          "description": "The composite asset models that are part of this asset model.
Composite asset models are asset models that contain specific properties.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelCompositeModel"
          }
        },
        "assetModelHierarchies": {
          "description": "The hierarchy definitions of the asset model. Each hierarchy
specifies an asset model whose assets can be children of any other assets created from
this asset model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetModelHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the asset
model.",
          "type": "array",
          "items": {
            "$ref": "#/definitions/Tag"
          }
        }
      }
    },
    "Asset": {
      "type": "object",
      "additionalProperties": false,
      "anyOf": [
        {
          "required": [
            "assetId",
            "assetModelId"
          ]
        },
        {
          "required": [
            "assetExternalId",
            "assetModelId"
          ]
```

```
        },
        {
          "required": [
            "assetId",
            "assetModelExternalId"
          ]
        },
        {
          "required": [
            "assetExternalId",
            "assetModelExternalId"
          ]
        }
      ],
      "required": [
        "assetName"
      ],
      "properties": {
        "assetId": {
          "description": "The ID of the asset",
          "$ref": "#/definitions/ID"
        },
        "assetExternalId": {
          "description": "The external ID of the asset",
          "$ref": "#/definitions/ExternalId"
        },
        "assetModelId": {
          "description": "The ID of the asset model from which to create the asset.",
          "$ref": "#/definitions/ID"
        },
        "assetModelExternalId": {
          "description": "The ExternalID of the asset model from which to create the
asset.",
          "$ref": "#/definitions/ExternalId"
        },
        "assetName": {
          "description": "A unique, friendly name for the asset.",
          "$ref": "#/definitions/Name"
        },
        "assetDescription": {
          "description": "A description for the asset",
          "$ref": "#/definitions/Description"
        },
        "assetProperties": {
```

```
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetProperty"
          }
        },
        "assetHierarchies": {
          "type": "array",
          "items": {
            "$ref": "#/definitions/AssetHierarchy"
          }
        },
        "tags": {
          "description": "A list of key-value pairs that contain metadata for the
 asset.",
          "type": "array",
          "uniqueItems": false,
          "items": {
            "$ref": "#/definitions/Tag"
          }
        }
      }
    }
  },
  "additionalProperties": false,
  "properties": {
    "assetModels": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/AssetModel"
      }
    },
    "assets": {
      "type": "array",
      "uniqueItems": false,
      "items": {
        "$ref": "#/definitions/Asset"
      }
    }
  }
}
```

Daten mit Alarmen überwachen

Sie können Alarme für Ihre Daten konfigurieren, um Ihr Team zu benachrichtigen, wenn Geräte oder Prozesse nicht optimal funktionieren. Optimale Leistung eines Geräts oder Prozesses bedeutet, dass die Werte für bestimmte Metriken innerhalb des Bereichs zwischen einem unteren und einem oberen Grenzwert liegen sollten. Wenn diese Metriken außerhalb ihres Betriebsbereichs liegen, müssen Gerätebediener benachrichtigt werden, damit sie das Problem beheben können. Verwenden Sie Alarme, um Probleme schnell zu erkennen und die Bediener zu benachrichtigen, um die Leistung Ihrer Geräte und Prozesse zu maximieren.

Themen

Arten von Alarmen

Sie können Alarme definieren, die in der AWS Cloud erkannt werden, und Alarme, die Sie bei externen Prozessen erkennen. AWS IoT SiteWise unterstützt die folgenden Arten von Alarmen:

- AWS IoT Events Alarme

  AWS IoT Events Alarme sind Alarme, die eintreffen AWS IoT Events. AWS IoT SiteWise sendet Eigenschaftswerte einer Anlage an ein Alarmmodell in AWS IoT Events. AWS IoT Events Sendet dann den Alarmstatus an AWS IoT SiteWise. Sie können Optionen konfigurieren, z. B. wann der Alarm erkannt wird und wen benachrichtigt werden soll, wenn sich der Alarmstatus ändert. Sie können auch die AWS IoT Events Aktionen definieren, die ausgeführt werden, wenn sich der Alarmstatus ändert.

  Alarme in AWS IoT Events sind Instanzen von Alarmmodellen. Das Alarmmodell spezifiziert den Schwellenwert und den Schweregrad des Alarms, was zu tun ist, wenn sich der Alarmstatus

ändert, und vieles mehr. Wenn Sie jedes Merkmal des Alarmmodells konfigurieren, geben Sie eine Attributeigenschaft aus dem Objektmodell an, das der Alarm überwacht. Alle auf dem Asset-Modell basierenden Assets verwenden den Wert des Attributs, wenn sie dieses AWS IoT Events Merkmal des Alarms auswerten. Weitere Informationen finden Sie unter Verwenden von Alarmen im AWS IoT Events Entwicklerhandbuch.

Sie können auf einen AWS IoT Events Alarm reagieren, wenn er seinen Status ändert. Sie können beispielsweise einen Alarm bestätigen oder die Schlummerfunktion deaktivieren, wenn er aktiv wird. Sie können Alarme auch aktivieren, deaktivieren und zurücksetzen.

SiteWise Monitor-Benutzer können AWS IoT Events Alarme in SiteWise Monitor-Portalen visualisieren, konfigurieren und darauf reagieren. Weitere Informationen finden Sie unter Überwachung mit Alarmen im AWS IoT SiteWise Monitor Anwendungsleitfaden.

> **Note**
>
> AWS IoT Events Für die Auswertung dieser Alarme und die Übertragung von Daten zwischen AWS IoT SiteWise und fallen Gebühren an AWS IoT Events. Weitere Informationen finden Sie unter AWS IoT Events Preise.

- Externe Alarme

  Externe Alarme sind Alarme, die Sie außerhalb auswerten AWS IoT SiteWise. Verwenden Sie externe Alarme, wenn Sie über eine Datenquelle verfügen, die den Alarmstatus meldet. Der externe Alarm enthält eine Messeigenschaft, in die Sie die Alarmzustandsdaten aufnehmen.

  Sie können einen externen Alarm nicht bestätigen oder in den Schlummermodus versetzen, wenn er seinen Status ändert.

  SiteWise Monitor-Benutzer können den Status externer Alarme in SiteWise Monitor-Portalen sehen, sie können diese Alarme jedoch nicht konfigurieren oder darauf reagieren.

  AWS IoT SiteWise bewertet den Status externer Alarme nicht.

Alarmzustände

Industriealarme enthalten Informationen über den Zustand der Geräte oder Prozesse, die sie überwachen, und (optional) Informationen über die Reaktion des Bedieners auf den Alarmzustand.

Wenn Sie einen AWS IoT Events Alarm definieren, geben Sie an, ob der Bestätigungsfluss aktiviert werden soll oder nicht. Der Bestätigungsfluss ist standardmäßig aktiviert. Wenn Sie diese Option aktivieren, können die Bediener den Alarm bestätigen und eine Notiz mit Einzelheiten zum Alarm oder zu den Maßnahmen hinterlassen, die sie zu seiner Behebung ergriffen haben. Wenn ein Bediener einen aktiven Alarm nicht bestätigt, bevor er inaktiv wird, wird der Alarm gesperrt. Der verriegelte Zustand bedeutet, dass der Alarm aktiv wurde und nicht bestätigt wurde. Der Bediener muss also die Ausrüstung oder den Prozess überprüfen und den eingeschalteten Alarm bestätigen.

Alarme haben die folgenden Zustände:

- Normal (`Normal`) — Der Alarm ist aktiviert, aber inaktiv. Der industrielle Prozess oder die industrielle Ausrüstung funktioniert erwartungsgemäß.
- Aktiv (`Active`) — Der Alarm ist aktiv. Der industrielle Prozess oder die industrielle Ausrüstung befindet sich außerhalb des Betriebsbereichs und erfordert besondere Aufmerksamkeit.
- Bestätigt (`Acknowledged`) — Ein Bediener hat den Zustand des Alarms bestätigt.

  Dieser Status gilt nur für Alarme, bei denen Sie den Bestätigungsfluss aktivieren.
- Eingeschaltet (`Latched`) — Der Alarm wurde wieder normal, war aber aktiv und kein Bediener hat ihn bestätigt. Der industrielle Prozess oder die industrielle Ausrüstung erfordert die Aufmerksamkeit eines Bedieners, um den Alarm wieder in den Normalzustand zu versetzen.

  Dieser Status gilt nur für Alarme, bei denen Sie den Bestätigungsfluss aktivieren.
- Snoozed (`SnoozeDisabled`) — Der Alarm ist deaktiviert, weil ein Bediener den Alarm ausgeschaltet hat. Der Operator definiert die Dauer, für die der Alarm in den Schlummermodus versetzt wird. Nach dieser Dauer kehrt der Alarm in den Normalzustand zurück.
- Deaktiviert (`Disabled`) — Der Alarm ist deaktiviert und wird nicht erkannt.

Eigenschaften des Alarmstatus

AWS IoT SiteWise speichert Alarmzustandsdaten als JSON-Objekt, das in eine Zeichenfolge serialisiert ist. Dieses Objekt enthält den Status und zusätzliche Informationen über den Alarm, z. B. Aktionen zur Reaktion des Bedieners und die Regel, die der Alarm auswertet.

Sie identifizieren die Alarmstatuseigenschaft anhand ihres Namens und Strukturtyps,`AWS/ALARM_STATE`. Weitere Informationen finden Sie unter Definition von Alarmen für Anlagenmodelle.

Das Datenobjekt für den Alarmstatus enthält die folgenden Informationen:

`stateName`

Der Zustand des Alarms. Weitere Informationen finden Sie unter Alarmzustände.

Datentyp: `STRING`

`customerAction`

(Optional) Ein Objekt, das Informationen über die Reaktion eines Bedieners auf den Alarm enthält. Bediener können Alarme aktivieren, deaktivieren, bestätigen und die Schlummerfunktion aktivieren. Wenn sie dies tun, umfassen die Daten zum Alarmstatus ihre Reaktion und den Hinweis, den sie hinterlassen können, wenn sie reagieren. Dieses Objekt enthält die folgenden Informationen:

`actionName`

Der Name der Aktion, die der Bediener ergreift, um auf den Alarm zu reagieren. Dieser Wert enthält eine der folgenden Zeichenketten:

- `ENABLE`
- `DISABLE`
- `SNOOZE`
- `ACKNOWLEDGE`
- `RESET`

Datentyp: `STRING`

`enable`

(Optional) Ein Objekt, das vorhanden ist, `customerAction` wenn der Bediener den Alarm aktiviert. Wenn ein Bediener den Alarm aktiviert, wechselt der Alarmstatus zu`Normal`. Dieses Objekt enthält die folgenden Informationen:

`note`

(Optional) Die Notiz, die der Kunde hinterlässt, wenn er den Alarm aktiviert.

Datentyp: `STRING`

Maximale Länge: 128 Zeichen

`disable`

(Optional) Ein Objekt, das vorhanden ist, `customerAction` wenn der Bediener den Alarm deaktiviert. Wenn ein Bediener den Alarm aktiviert, wechselt der Alarmstatus zu`Disabled`. Dieses Objekt enthält die folgenden Informationen:

`note`

(Optional) Die Notiz, die der Kunde hinterlässt, wenn er den Alarm deaktiviert.

Datentyp: `STRING`

Maximale Länge: 128 Zeichen

`acknowledge`

(Optional) Ein Objekt, das vorhanden ist, `customerAction` wenn der Bediener den Alarm bestätigt. Wenn ein Bediener den Alarm aktiviert, wechselt der Alarmstatus zu`Acknowledged`. Dieses Objekt enthält die folgenden Informationen:

`note`

(Optional) Die Notiz, die der Kunde hinterlässt, wenn er den Alarm bestätigt.

Datentyp: `STRING`

Maximale Länge: 128 Zeichen

`snooze`

(Optional) Ein Objekt, das vorhanden ist, `customerAction` wenn der Bediener den Alarm aktiviert. Wenn ein Bediener den Alarm aktiviert, wechselt der Alarmstatus zu. `SnoozeDisabled` Dieses Objekt enthält die folgenden Informationen:

`snoozeDuration`

Die Dauer in Sekunden, für die der Bediener den Alarm aktiviert. Nach Ablauf dieser Dauer wechselt der Alarm in `Normal` den Status.

Datentyp: `INTEGER`

`note`

(Optional) Die Notiz, die der Kunde hinterlässt, wenn er den Alarm aktiviert.

Datentyp: `STRING`

Maximale Länge: 128 Zeichen

`ruleEvaluation`

(Optional) Ein Objekt, das Informationen über die Regel enthält, die den Alarm auswertet. Dieses Objekt enthält die folgenden Informationen:

`simpleRule`

Ein Objekt, das Informationen über eine einfache Regel enthält, die einen Eigenschaftswert mit einem Schwellenwert anhand eines Vergleichsoperators vergleicht. Dieses Objekt enthält die folgenden Informationen:

`inputProperty`

Der Wert der Eigenschaft, die dieser Alarm auswertet.

Datentyp: `DOUBLE`

`operator`

Der Vergleichsoperator, den dieser Alarm verwendet, um die Eigenschaft mit dem Schwellenwert zu vergleichen. Dieser Wert enthält eine der folgenden Zeichenketten:

- `<` — Weniger als
- `<=` — Weniger als oder gleich
- `==` — Gleich
- `!=` — Nicht gleich
- `>=` — Größer als oder gleich
- `>` — Größer als

Datentyp: `STRING`

`threshold`

Der Schwellenwert, mit dem dieser Alarm den Eigenschaftswert vergleicht.

Datentyp: `DOUBLE`

Definition von Alarmen für Anlagenmodelle

Anlagenmodelle fördern die Standardisierung Ihrer industriellen Daten und Alarme. Sie können Alarmdefinitionen für Anlagenmodelle definieren, um die Alarme für alle Anlagen auf der Grundlage eines Anlagenmodells zu standardisieren.

Sie verwenden zusammengesetzte Asset-Modelle, um Alarme für Asset-Modelle zu definieren. Bei zusammengesetzten Anlagenmodellen handelt es sich um Anlagenmodelle, die einen bestimmten Satz von Eigenschaften auf ein anderes Anlagenmodell standardisieren. Zusammengesetzte Anlagemodelle stellen sicher, dass bestimmte Eigenschaften in einem Anlagemodell vorhanden sind. Alarme verfügen über Typ-, Status- und (optionale) Quelleneigenschaften, sodass das zusammengesetzte Alarmmodell erzwingt, dass diese Eigenschaften vorhanden sind.

Jedes zusammengesetzte Objektmodell hat einen Typ, der die Eigenschaften für dieses zusammengesetzte Modell definiert. Verbundmodelle für Alarme definieren Eigenschaften für den Alarmtyp, den Alarmstatus und die (optionale) Alarmquelle. Wenn Sie ein Asset aus einem Asset-Modell mit zusammengesetzten Modellen erstellen, enthält das Asset neben den Eigenschaften, die Sie im Asset-Modell angeben, auch die Eigenschaften aus dem Verbundmodell.

Jede Eigenschaft in einem zusammengesetzten Modell muss den Namen haben, der sie für ihren Typ des zusammengesetzten Modells kennzeichnet. Die Eigenschaften eines zusammengesetzten Modells unterstützen Eigenschaften mit komplexen Datentypen. Diese Eigenschaften haben den `STRUCT` Datentyp und ein `dataTypeSpec` Merkmal, das den komplexen Datentyp der Eigenschaft angibt. Eigenschaften komplexer Datentypen enthalten JSON-Daten, die als Zeichenfolgen serialisiert sind.

Verbundmodelle von Alarmen haben die folgenden Eigenschaften. Jede Eigenschaft muss den Namen haben, der sie für diesen Typ von Verbundmodell identifiziert.

Typ des Alarms

Der Typ des Alarms. Geben Sie eines der folgenden Elemente an:

- `IOT_EVENTS`— Ein AWS IoT Events Alarm. AWS IoT SiteWise sendet Daten an, AWS IoT Events um den Status dieses Alarms auszuwerten. Sie müssen die Eigenschaft Alarmquelle angeben, um das AWS IoT Events Alarmmodell für diese Alarmdefinition zu definieren.
- `EXTERNAL`— Ein externer Alarm. Sie nehmen den Zustand des Alarms als Messwert auf.

Name der Immobilie: `AWS/ALARM_TYPE`

Art der Immobilie: Attribut

Datentyp: `STRING`

Zustand des Alarms

Die Zeitreihendaten für den Status des Alarms. Dies ist ein als Zeichenfolge serialisiertes Objekt, das den Status und andere Informationen über den Alarm enthält. Weitere Informationen finden Sie unter Eigenschaften des Alarmstatus.

Name der Immobilie: `AWS/ALARM_STATE`

Art der Immobilie: Messung

Datentyp: `STRUCT`

Typ der Datenstruktur: `AWS/ALARM_STATE`

Quelle des Alarms

(Optional) Der Amazon-Ressourcenname (ARN) der Ressource, die den Status des Alarms auswertet. Für AWS IoT Events Alarme ist dies der ARN des Alarmmodells.

Name der Immobilie: `AWS/ALARM_SOURCE`

Art der Immobilie: Attribut

Datentyp: `STRING`

Example Beispiel für ein zusammengesetztes Alarmmodell

Das folgende Anlagenmodell stellt einen Kessel dar, dessen Temperatur über einen Alarm überwacht wird. AWS IoT SiteWise sendet die Temperaturdaten an, AWS IoT Events um den Alarm zu erkennen.

```
{
  "assetModelName": "Boiler",
  "assetModelDescription": "A boiler that alarms when its temperature exceeds its
 limit.",
  "assetModelProperties": [
    {
      "name": "Temperature",
      "dataType": "DOUBLE",
      "unit": "Celsius",
      "type": {
        "measurement": {}
      }
    },
```

```
    {
      "name": "High Temperature",
      "dataType": "DOUBLE",
      "unit": "Celsius",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ],
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        },
        {
          "name": "AWS/ALARM_SOURCE",
          "dataType": "STRING",
          "type": {
            "attribute": {}
          }
        }
      ]
    }
  ]
```

```
}
```

Themen

- AWS IoT Events Alarme definieren
- Definition externer Alarme

AWS IoT Events Alarme definieren

Wenn Sie einen AWS IoT Events Alarm erstellen, AWS IoT SiteWise sendet die Eigenschaftswerte der Anlage an AWS IoT Events , um den Status des Alarms auszuwerten. AWS IoT Events Alarmdefinitionen hängen von einem Alarmmodell ab, in dem Sie sie definieren AWS IoT Events. Um einen AWS IoT Events Alarm anhand eines Anlagenmodells zu definieren, definieren Sie ein zusammengesetztes Alarmmodell, das das AWS IoT Events Alarmmodell als Alarmquelleneigenschaft angibt.

AWS IoT Events Alarme hängen von Eingaben wie Alarmschwellenwerten und Einstellungen für Alarmbenachrichtigungen ab. Sie definieren diese Eingaben als Attribute im Asset-Modell. Sie können diese Eingaben dann für jedes Asset auf der Grundlage des Modells anpassen. Die AWS IoT SiteWise Konsole kann diese Attribute für Sie erstellen. Wenn Sie Alarme mit der API AWS CLI oder definieren, müssen Sie diese Attribute im Asset-Modell manuell definieren.

Sie können auch andere Aktionen definieren, die ausgeführt werden, wenn Ihr Alarm erkannt wird, z. B. benutzerdefinierte Aktionen für Alarmbenachrichtigungen. Sie können beispielsweise eine Aktion konfigurieren, die eine Push-Benachrichtigung an ein Amazon SNS SNS-Thema sendet. Weitere Informationen zu den Aktionen, die Sie definieren können, finden Sie unter Arbeiten mit anderen AWS Diensten im AWS IoT Events Entwicklerhandbuch.

Wenn Sie ein Asset-Modell aktualisieren oder löschen, AWS IoT SiteWise kann überprüft werden, ob ein Alarmmodell eine mit diesem Asset-Modell verknüpfte Anlageneigenschaft überwacht. AWS IoT Events Dadurch wird verhindert, dass Sie eine Anlageneigenschaft löschen, die derzeit von einem AWS IoT Events Alarm verwendet wird. Um diese Funktion in zu aktivieren AWS IoT SiteWise, benötigen Sie die `iotevents:ListInputRoutings` entsprechende Genehmigung. Diese Berechtigung ermöglicht das Ausführen AWS IoT SiteWise von Aufrufen des ListInputRoutings-API-Vorgangs, der von AWS IoT Events unterstützt wird. Weitere Informationen finden Sie unter (Optionale) ListInputRoutings Erlaubnis.

> **Note**
>
> Die Funktion für Alarmbenachrichtigungen ist in der Region China (Peking) nicht verfügbar.

Themen

Anforderungen für Alarmbenachrichtigungen

AWS IoT Events verwendet eine AWS Lambda Funktion in Ihrem AWS Konto, um Alarmbenachrichtigungen zu senden. Sie müssen diese Lambda-Funktion in derselben AWS Region wie Ihre Alarme erstellen, um Alarmbenachrichtigungen zu aktivieren. Diese Lambda-Funktion verwendet Amazon Simple Notification Service (Amazon SNS) zum Senden von Textbenachrichtigungen und Amazon Simple Email Service (Amazon SES) zum Senden von E-Mail-Benachrichtigungen. Wenn Sie den AWS IoT Events Alarm erstellen, konfigurieren Sie die Protokolle und Einstellungen, die der Alarm zum Senden von Benachrichtigungen verwendet.

AWS IoT Events stellt eine AWS CloudFormation Stack-Vorlage bereit, mit der Sie diese Lambda-Funktion in Ihrem Konto erstellen können. Weitere Informationen finden Sie unter Lambda-Funktion für Alarmbenachrichtigungen im AWS IoT Events Entwicklerhandbuch.

Definition eines AWS IoT Events Alarms (AWS IoT SiteWise Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um einen AWS IoT Events Alarm für ein vorhandenes Asset-Modell zu definieren. Um einen AWS IoT Events Alarm für ein neues Asset-Modell zu definieren, erstellen Sie das Asset-Modell und führen Sie dann diese Schritte aus. Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen.

> **Important**
>
> Für jeden Alarm ist ein Attribut erforderlich, das den Schwellenwert angibt, mit dem für den Alarm verglichen werden soll. Sie müssen das Schwellenwertattribut im Asset-Modell definieren, bevor Sie einen Alarm definieren können.

Stellen Sie sich ein Beispiel vor, bei dem Sie einen Alarm definieren möchten, der erkennt, wenn eine Windkraftanlage ihre maximale Nennwindgeschwindigkeit von 50 mph überschreitet. Bevor Sie den Alarm definieren, müssen Sie ein Attribut (Maximale Windgeschwindigkeit) mit dem Standardwert definieren`50`.

Um einen AWS IoT Events Alarm für ein Asset-Modell zu definieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das Asset-Modell aus, für das Sie einen Alarm definieren möchten.
4. Wählen Sie die Registerkarte Alarm.
5. Wählen Sie Alarm hinzufügen.
6. Wählen Sie im Bereich Optionen für den Alarmtyp die Option AWS IoT Events Alarm aus.
7. Gehen Sie im Abschnitt Alarmdetails wie folgt vor:
   a. Geben Sie einen Namen für den Alarm ein.
   b. (Optional) Geben Sie eine Beschreibung für Ihren Alarm ein.
8. Im Abschnitt Schwellenwertdefinitionen legen Sie fest, wann der Alarm erkannt wird und wie schwerwiegend der Alarm ist. Gehen Sie wie folgt vor:
   a. Wählen Sie die Eigenschaft aus, bei der der Alarm erkannt wird. Jedes Mal, wenn diese Eigenschaft einen neuen Wert erhält, wird der Wert AWS IoT SiteWise an gesendet, AWS IoT Events um den Status des Alarms auszuwerten.
   b. Wählen Sie den Operator aus, der verwendet werden soll, um die Eigenschaft mit dem Schwellenwert zu vergleichen. Wählen Sie aus den folgenden Optionen aus:
      - < weniger als
      - <= kleiner als oder gleich
      - == gleich
      - ! = nicht gleich
      - >= größer als oder gleich
      - > größer als
   c. Wählen Sie unter Wert die Attributeigenschaft aus, die als Schwellenwert verwendet werden soll. AWS IoT Events vergleicht den Wert der Eigenschaft mit dem Wert dieses Attributs.

d. Geben Sie den Schweregrad des Alarms ein. Verwenden Sie eine Zahl, die Ihr Team versteht, um den Schweregrad dieses Alarms wiederzugeben.

9. (Optional) Gehen Sie im Abschnitt Benachrichtigungseinstellungen — optional wie folgt vor:

a. Wählen Sie Aktiv.

> **Note**
>
> Wenn Sie Inaktiv wählen, erhalten Sie und Ihr Team keine Alarmbenachrichtigungen.

b. Wählen Sie unter Empfänger den Empfänger aus.

> **Important**
>
> Sie können Alarmbenachrichtigungen an AWS IAM Identity Center Benutzer senden. Um diese Funktion nutzen zu können, müssen Sie IAM Identity Center aktivieren. Sie können IAM Identity Center jeweils nur in einer AWS Region aktivieren. Das bedeutet, dass Sie Alarmbenachrichtigungen nur in der Region definieren können, in der Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie unter Erste Schritte im AWS IAM Identity Center -Benutzerhandbuch.

c. Wählen Sie unter Protokoll eine der folgenden Optionen aus:

- E-Mail und Text — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer SMS-Nachricht und einer E-Mail-Nachricht.
- E-Mail — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer E-Mail-Nachricht.
- Text — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer SMS-Nachricht.

d. Wählen Sie unter Absender den Absender aus.

> **Important**
>
> Sie müssen die Absender-E-Mail-Adresse in Amazon Simple Email Service (Amazon SES) verifizieren. Weitere Informationen finden Sie unter Verifizieren von E-Mail-Adressen in Amazon SES im Amazon Simple Email Service Developer Guide.

10. Im Abschnitt Standard-Asset-Status können Sie den Standardstatus für Alarme festlegen, die mit diesem Asset-Modell erstellt wurden.

    > **Note**
    >
    > Sie aktivieren oder deaktivieren diesen Alarm für Assets, die Sie in einem späteren Schritt anhand dieses Asset-Modells erstellen.

11. Im Bereich Erweiterte Einstellungen können Sie die Berechtigungen, die zusätzlichen Benachrichtigungseinstellungen, die Alarmstatusaktionen, das Alarmmodell in SiteWise Monitor und den Bestätigungsablauf konfigurieren.

    > **Note**
    >
    > AWS IoT Events Für Alarme sind die folgenden Servicerollen erforderlich:
    >
    > - Eine Rolle, die AWS IoT Events davon ausgeht, Alarmstatuswerte an zu senden AWS IoT SiteWise.
    > - Eine Rolle, die AWS IoT Events davon ausgeht, Daten an Lambda zu senden. Sie benötigen diese Rolle nur, wenn Ihr Alarm Benachrichtigungen sendet.

    Gehen Sie im Abschnitt Berechtigungen wie folgt vor:

    a. Verwenden Sie als AWS IoT Events Rolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Diese Rolle erfordert die `iotsitewise:BatchPutAssetPropertyValue` Erlaubnis und eine Vertrauensbeziehung, die es iotevents.amazonaws.com ermöglicht, die Rolle zu übernehmen.

    b. Verwenden Sie für die AWS IoT Events Lambda-Rolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Für diese Rolle sind die `sso-directory:DescribeUser` Berechtigungen `lambda:InvokeFunction` und sowie eine Vertrauensbeziehung erforderlich, die es ermöglicht, die Rolle `iotevents.amazonaws.com` zu übernehmen.

12. (Optional) Gehen Sie im Abschnitt Zusätzliche Benachrichtigungseinstellungen wie folgt vor:

a. Für das Empfängerattribut definieren Sie ein Attribut, dessen Wert den Empfänger der Benachrichtigung angibt. Sie können IAM Identity Center-Benutzer als Empfänger auswählen.

   Sie können ein Attribut erstellen oder ein vorhandenes Attribut im Asset-Modell verwenden.

   - Wenn Sie Neues Empfängerattribut erstellen wählen, geben Sie den Namen des Empfängerattributs und den Standardwert Empfänger an — optional für das Attribut.
   - Wenn Sie Bestehendes Empfängerattribut verwenden wählen, wählen Sie das Attribut im Feld Name des Empfängerattributs aus. Der Alarm verwendet den Standardwert des von Ihnen ausgewählten Attributs.

   Sie können den Standardwert für jedes Asset, das Sie anhand dieses Asset-Modells erstellen, überschreiben.

b. Für das benutzerdefinierte Nachrichtenattribut definieren Sie ein Attribut, dessen Wert die benutzerdefinierte Nachricht angibt, die zusätzlich zur Standardnachricht zur Statusänderung gesendet werden soll. Sie können beispielsweise eine Nachricht angeben, die Ihrem Team hilft, zu verstehen, wie mit diesem Alarm umgegangen werden kann.

   Sie können wählen, ob Sie ein Attribut erstellen oder ein vorhandenes Attribut im Asset-Modell verwenden möchten.

   - Wenn Sie sich dafür entscheiden, ein neues benutzerdefiniertes Nachrichtenattribut zu erstellen, geben Sie den Namen des benutzerdefinierten Nachrichtenattributs und den Standardwert für benutzerdefinierte Nachricht an — optional für das Attribut.
   - Wenn Sie Ein vorhandenes benutzerdefiniertes Nachrichtenattribut verwenden wählen, wählen Sie das Attribut unter Name des benutzerdefinierten Nachrichtenattributs aus. Der Alarm verwendet den Standardwert des von Ihnen ausgewählten Attributs.

   Sie können den Standardwert für jedes Asset, das Sie anhand dieses Asset-Modells erstellen, überschreiben.

c. Führen Sie für Manage your Lambda function einen der folgenden Schritte aus:

   - Um eine neue Lambda-Funktion AWS IoT SiteWise erstellen zu lassen, wählen Sie Create a new lambda from an AWS managed template.

- Um eine bestehende Lambda-Funktion zu verwenden, wählen Sie Use an existing lambda und wählen Sie den Namen der Funktion.

Weitere Informationen finden Sie unter Verwaltung von Alarmbenachrichtigungen im AWS IoT Events Entwicklerhandbuch.

13. (Optional) Gehen Sie im Abschnitt Statusaktion festlegen wie folgt vor:

    a. Wählen Sie Aktion bearbeiten aus.

    b. Fügen Sie unter Aktionen zum Alarmstatus hinzufügen die Aktionen hinzu und wählen Sie dann Speichern aus.

    Sie können bis zu 10 Aktionen hinzufügen.

    AWS IoT Events kann Aktionen ausführen, wenn der Alarm aktiv ist. Sie können integrierte Aktionen definieren, um einen Timer zu verwenden oder eine Variable festzulegen oder Daten an andere AWS Ressourcen zu senden. Weitere Informationen finden Sie im AWS IoT Events Entwicklerhandbuch unter Unterstützte Aktionen.

14. (Optional) Wählen Sie unter Alarmmodell im SiteWise Monitor verwalten — optional die Option Aktiv oder Inaktiv aus.

    Verwenden Sie diese Option, damit Sie das Alarmmodell in SiteWise Monitoren aktualisieren können. Diese Option ist standardmäßig aktiviert.

15. Wählen Sie unter Acknowledge-Flow die Option Aktiv oder Inaktiv aus. Weitere Informationen zum Bestätigungsablauf finden Sie unterAlarmzustände.

16. Wählen Sie Alarm hinzufügen.

> **Note**
>
> Die AWS IoT SiteWise Konsole stellt mehrere API-Anfragen, um den Alarm zum Asset-Modell hinzuzufügen. Wenn Sie Alarm hinzufügen wählen, öffnet die Konsole ein Dialogfeld, in dem der Status dieser API-Anfragen angezeigt wird. Bleiben Sie auf dieser Seite, bis jede API-Anfrage erfolgreich ist oder bis eine API-Anfrage fehlschlägt. Wenn eine Anfrage fehlschlägt, schließen Sie das Dialogfeld, beheben Sie das Problem und wählen Sie Alarm hinzufügen, um es erneut zu versuchen.

Einen AWS IoT Events Alarm definieren (AWS IoT Events Konsole)

Sie können die AWS IoT Events Konsole verwenden, um einen AWS IoT Events Alarm für ein vorhandenes Anlagenmodell zu definieren. Um einen AWS IoT Events Alarm für ein neues Asset-Modell zu definieren, erstellen Sie das Asset-Modell und führen Sie dann diese Schritte aus. Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen.

> **Important**
>
> Für jeden Alarm ist ein Attribut erforderlich, das den Schwellenwert angibt, mit dem für den Alarm verglichen werden soll. Sie müssen das Schwellenwertattribut im Asset-Modell definieren, bevor Sie einen Alarm definieren können.
> Stellen Sie sich ein Beispiel vor, bei dem Sie einen Alarm definieren möchten, der erkennt, wenn eine Windkraftanlage ihre maximale Nennwindgeschwindigkeit von 50 mph überschreitet. Bevor Sie den Alarm definieren, müssen Sie ein Attribut (Maximale Windgeschwindigkeit) mit dem Standardwert definieren`50`.

Um einen AWS IoT Events Alarm für ein Asset-Modell zu definieren

1. Navigieren Sie zur AWS IoT Events -Konsole.
2. Wählen Sie im Navigationsbereich die Option Alarmmodelle aus.
3. Wählen Sie Alarmmodell erstellen aus.
4. Geben Sie einen Namen für den Alarm ein.
5. (Optional) Geben Sie eine Beschreibung für Ihren Alarm ein.
6. Gehen Sie im Bereich Alarmziel wie folgt vor:
   a. Wählen Sie unter Zieloptionen die Option AWS IoT SiteWise Asset-Eigenschaft aus.
   b. Wählen Sie das Asset-Modell aus, für das Sie den Alarm hinzufügen möchten.
7. Im Abschnitt Schwellenwertdefinitionen legen Sie fest, wann der Alarm erkannt wird und wie schwerwiegend der Alarm ist. Gehen Sie wie folgt vor:
   a. Wählen Sie die Eigenschaft aus, bei der der Alarm erkannt wird. Jedes Mal, wenn diese Eigenschaft einen neuen Wert erhält, wird der Wert AWS IoT SiteWise an gesendet, AWS IoT Events um den Status des Alarms auszuwerten.
   b. Wählen Sie den Operator aus, der verwendet werden soll, um die Eigenschaft mit dem Schwellenwert zu vergleichen. Wählen Sie aus den folgenden Optionen aus:

- < weniger als
- <= kleiner als oder gleich
- == gleich
- ! = nicht gleich
- >= größer als oder gleich
- > größer als

c. Wählen Sie unter Wert die Attributeigenschaft aus, die als Schwellenwert verwendet werden soll. AWS IoT Events vergleicht den Wert der Eigenschaft mit dem Wert dieses Attributs.

d. Geben Sie den Schweregrad des Alarms ein. Verwenden Sie eine Zahl, die Ihr Team versteht, um den Schweregrad dieses Alarms wiederzugeben.

8. (Optional) Gehen Sie im Abschnitt Benachrichtigungseinstellungen — optional wie folgt vor:

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

- E-Mail und Text — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer SMS-Nachricht und einer E-Mail-Nachricht.
- E-Mail — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer E-Mail-Nachricht.
- Text — Der Alarm benachrichtigt IAM Identity Center-Benutzer mit einer SMS-Nachricht.

b. Wählen Sie unter Absender den Absender aus.

> **Important**
>
> Sie müssen die Absender-E-Mail-Adresse in Amazon Simple Email Service (Amazon SES) verifizieren. Weitere Informationen finden Sie unter Verifizieren von E-Mail-Adressen in Amazon SES im Amazon Simple Email Service Developer Guide.

c. Wählen Sie das Attribut unter Empfängerattribut — optional aus. Der Alarm verwendet den Standardwert des von Ihnen ausgewählten Attributs.

d. Wählen Sie das Attribut unter Benutzerdefiniertes Nachrichtenattribut — optional aus. Der Alarm verwendet den Standardwert des von Ihnen ausgewählten Attributs.

9. Geben Sie im Abschnitt Instanz den Standardstatus für diesen Alarm an. Sie können diesen Alarm in einem späteren Schritt für alle Assets aktivieren oder deaktivieren, die Sie anhand dieses Asset-Modells erstellen.
10. In den erweiterten Einstellungen können Sie die Berechtigungen, die zusätzlichen Benachrichtigungseinstellungen, die Alarmstatusaktionen, das Alarmmodell in SiteWise Monitor und den Bestätigungsablauf konfigurieren.

> **Note**
>
> AWS IoT Events Für Alarme sind die folgenden Servicerollen erforderlich:
>
> - Eine Rolle, die AWS IoT Events davon ausgeht, Alarmstatuswerte an zu senden AWS IoT SiteWise.
> - Eine Rolle, die AWS IoT Events davon ausgeht, Daten an Lambda zu senden. Sie benötigen diese Rolle nur, wenn Ihr Alarm Benachrichtigungen sendet.

a. Wählen Sie im Abschnitt Bestätigungsablauf die Option Aktiviert oder Deaktiviert aus. Weitere Informationen zum Bestätigungsablauf finden Sie unterAlarmzustände.

b. Gehen Sie im Abschnitt „Berechtigungen“ wie folgt vor:

   i. Verwenden Sie als AWS IoT Events Rolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Diese Rolle erfordert die `iotsitewise:BatchPutAssetPropertyValue` Erlaubnis und eine Vertrauensbeziehung, die es iotevents.amazonaws.com ermöglicht, die Rolle zu übernehmen.

   ii. Verwenden Sie für die Lambda-Rolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Für diese Rolle sind die `sso-directory:DescribeUser` Berechtigungen `lambda:InvokeFunction` und sowie eine Vertrauensbeziehung erforderlich, die es ermöglicht, die Rolle `iotevents.amazonaws.com` zu übernehmen.

c. (Optional) Gehen Sie im Bereich Zusätzliche Benachrichtigungseinstellungen wie folgt vor:

   - Gehen Sie für Manage your Lambda function wie folgt vor:

     - Um eine neue Lambda-Funktion AWS IoT Events erstellen zu lassen, wählen Sie Create a new Lambda-Funktion.

- Um eine bestehende Lambda-Funktion zu verwenden, wählen Sie Bestehende Lambda-Funktion verwenden und wählen Sie den Namen der Funktion.

Weitere Informationen finden Sie unter Verwaltung von Alarmbenachrichtigungen im AWS IoT Events Entwicklerhandbuch.

d. (Optional) Gehen Sie im Abschnitt Statusaktion festlegen — optional wie folgt vor:

- Fügen Sie unter Aktionen zum Alarmstatus die Aktionen hinzu und wählen Sie dann Speichern aus.

  Sie können bis zu 10 Aktionen hinzufügen.

AWS IoT Events kann Aktionen ausführen, wenn der Alarm aktiv ist. Sie können integrierte Aktionen definieren, um einen Timer zu verwenden oder eine Variable festzulegen oder Daten an andere AWS Ressourcen zu senden. Weitere Informationen finden Sie im AWS IoT Events Entwicklerhandbuch unter Unterstützte Aktionen.

11. Wählen Sie Erstellen.

> **Note**
>
> Die AWS IoT Events Konsole stellt mehrere API-Anfragen, um den Alarm zum Asset-Modell hinzuzufügen. Wenn Sie Alarm hinzufügen wählen, öffnet die Konsole ein Dialogfeld, in dem der Status dieser API-Anfragen angezeigt wird. Bleiben Sie auf dieser Seite, bis jede API-Anfrage erfolgreich ist oder bis eine API-Anfrage fehlschlägt. Wenn eine Anfrage fehlschlägt, schließen Sie das Dialogfeld, beheben Sie das Problem und wählen Sie Alarm hinzufügen, um es erneut zu versuchen.

Einen AWS IoT Events Alarm definieren (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um einen AWS IoT Events Alarm zu definieren, der eine Anlageneigenschaft überwacht. Sie können den Alarm für ein neues oder vorhandenes Asset-Modell definieren. Nachdem Sie den Alarm für das Asset-Modell definiert haben, erstellen Sie einen Alarm im Asset-Modell AWS IoT Events und verbinden ihn mit dem Asset-Modell. In diesem Prozess gehen Sie wie folgt vor:

Schritte

- Schritt 1: Definieren eines Alarms für ein Anlagenmodell
- Schritt 2: Definition eines Alarmmodells AWS IoT Events
- Schritt 3: Aktivieren des Datenflusses zwischen AWS IoT SiteWise und AWS IoT Events

Schritt 1: Definieren eines Alarms für ein Anlagenmodell

Fügen Sie eine Alarmdefinition und zugehörige Eigenschaften zu einem neuen oder vorhandenen Anlagenmodell hinzu.

So definieren Sie einen Alarm für ein Asset-Modell (CLI)

1. Erstellen Sie eine Datei mit dem Namen `asset-model-payload.json`. Folgen Sie den Schritten in diesen anderen Abschnitten, um die Details Ihres Asset-Modells zur Datei hinzuzufügen, reichen Sie jedoch nicht die Anfrage zur Erstellung oder Aktualisierung des Asset-Modells ein. In diesem Abschnitt fügen Sie den Asset-Modelldetails in der `asset-model-payload.json` Datei eine Alarmdefinition hinzu.
   - Weitere Informationen zum Erstellen eines Asset-Modells finden Sie unterEin Asset-Modell erstellen (AWS CLI).
   - Weitere Informationen zum Aktualisieren eines vorhandenen Asset-Modells finden Sie unterAktualisierung eines Asset- oder Komponentenmodells (AWS CLI).

   > **Note**
   >
   > Ihr Anlagenmodell muss mindestens eine Anlageneigenschaft definieren, einschließlich der Anlageneigenschaft, die mit dem Alarm überwacht werden soll.

2. Fügen Sie dem Anlagenmodell ein zusammengesetztes Alarmmodell (`assetModelCompositeModels`) hinzu. Ein zusammengesetztes AWS IoT Events Alarmmodell spezifiziert den `IOT_EVENTS` Typ und gibt eine Alarmquelleneigenschaft an. Sie fügen die Eigenschaft Alarmquelle hinzu, nachdem Sie das Alarmmodell in erstellt haben AWS IoT Events.

   > **Important**
   >
   > Das zusammengesetzte Alarmmodell muss denselben Namen haben wie das AWS IoT Events Alarmmodell, das Sie später erstellen. Namen von Alarmmodellen dürfen nur

alphanumerische Zeichen enthalten. Geben Sie einen eindeutigen, alphanumerischen Namen an, sodass Sie denselben Namen für das Alarmmodell verwenden können.

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

3. Fügen Sie dem Asset-Modell ein Alarmschwellenwertattribut hinzu. Geben Sie den Standardwert an, der für diesen Schwellenwert verwendet werden soll. Sie können diesen Standardwert für jedes Asset, das auf diesem Modell basiert, überschreiben.

> **Note**
>
> Das Alarmschwellenwertattribut muss ein `INTEGER` oder a sein`DOUBLE`.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    }
  ]
}
```

4. (Optional) Fügen Sie dem Asset-Modell Attribute für Alarmbenachrichtigungen hinzu. Diese Attribute geben den IAM Identity Center-Empfänger und andere Eingaben an, die zum Senden von Benachrichtigungen AWS IoT Events verwendet werden, wenn sich der Status des Alarms ändert. Sie können diese Standardwerte für jedes Asset, das auf diesem Modell basiert, überschreiben.

   > **Important**
   >
   > Sie können Alarmbenachrichtigungen an AWS IAM Identity Center Benutzer senden. Um diese Funktion nutzen zu können, müssen Sie IAM Identity Center aktivieren. Sie können IAM Identity Center jeweils nur in einer AWS Region aktivieren. Das bedeutet, dass Sie Alarmbenachrichtigungen nur in der Region definieren können, in der Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie unter Erste Schritte im AWS IAM Identity Center -Benutzerhandbuch.

   Gehen Sie wie folgt vor:

   a. Fügen Sie ein Attribut hinzu, das die ID Ihres IAM Identity Center-Identitätsspeichers angibt. Sie können den IAM Identity Center ListInstancesAPI-Vorgang verwenden, um Ihre Identitätsspeicher aufzulisten. Dieser Vorgang funktioniert nur in der Region, in der Sie IAM Identity Center aktivieren.

```
aws sso-admin list-instances
```

Geben Sie dann die Identitätsspeicher-ID (z. B.`d-123EXAMPLE`) als Standardwert für das Attribut an.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    }
  ]
}
```

b. Fügen Sie ein Attribut hinzu, das die ID des IAM Identity Center-Benutzers angibt, der Benachrichtigungen erhält. Um einen Standardempfänger für Benachrichtigungen zu definieren, fügen Sie eine IAM Identity Center-Benutzer-ID als Standardwert hinzu. Gehen Sie wie folgt vor, um eine IAM Identity Center-Benutzer-ID zu erhalten:

   i. Sie können die IAM Identity ListUsersCenter-API verwenden, um die ID eines Benutzers abzurufen, dessen Benutzernamen Sie kennen. Ersetzen Sie *D-123Example* durch die ID Ihres Identitätsspeichers und *Name* durch den Benutzernamen des Benutzers.

```
aws identitystore list-users \
  --identity-store-id d-123EXAMPLE \
  --filters AttributePath=UserName,AttributeValue=Name
```

   ii. Verwenden Sie die IAM Identity Center-Konsole, um Ihre Benutzer zu durchsuchen und eine Benutzer-ID zu finden.

Geben Sie dann die Benutzer-ID (z. B.`123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`) als Standardwert für das Attribut an, oder definieren Sie das Attribut ohne Standardwert.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    }
  ]
}
```

c. (Optional) Fügen Sie ein Attribut hinzu, das die Standard-Absender-ID für SMS-Benachrichtigungen (Text) angibt. Die Absender-ID wird in Nachrichten, die Amazon Simple Notification Service (Amazon SNS) sendet, als Nachrichtenabsender angezeigt. Weitere Informationen finden Sie unter Absender-IDs für SMS-Nachrichten mit Amazon SNS anfordern im Amazon Simple Notification Service Developer Guide.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
    }
  ]
```

```
}
```

d. (Optional) Fügen Sie ein Attribut hinzu, das die Standard-E-Mail-Adresse angibt, die als Absenderadresse in E-Mail-Benachrichtigungen verwendet werden soll.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    }
  ]
}
```

e. (Optional) Fügen Sie ein Attribut hinzu, das den Standard-Betreff angibt, der in E-Mail-Benachrichtigungen verwendet werden soll.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    }
  ]
}
```

f. (Optional) Fügen Sie ein Attribut hinzu, das eine zusätzliche Nachricht angibt, die in Benachrichtigungen aufgenommen werden soll. Standardmäßig enthalten

Benachrichtigungen Informationen über den Alarm. Sie können auch eine zusätzliche Nachricht hinzufügen, die dem Benutzer weitere Informationen gibt.

```
{
  ...
  "assetModelProperties": [
    ...
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ]
}
```

5. Erstellen Sie das Asset-Modell oder aktualisieren Sie das bestehende Asset-Modell. Führen Sie eine der folgenden Aktionen aus:

   - Führen Sie den folgenden Befehl aus, um das Asset-Modell zu erstellen.

     ```
     aws iotsitewise create-asset-model --cli-input-json file://asset-model-
     payload.json
     ```

   - Führen Sie den folgenden Befehl aus, um das vorhandene Asset-Modell zu aktualisieren. Ersetzen Sie *asset-model-id* durch die ID des Komponentenmodells.

     ```
     aws iotsitewise update-asset-model \
       --asset-model-id asset-model-id \
       --cli-input-json file://asset-model-payload.json
     ```

   Nachdem Sie den Befehl ausgeführt haben, notieren Sie sich das `assetModelId` in der Antwort.

Beispiel: Modell der Kesselanlage

Das folgende Anlagenmodell stellt einen Kessel dar, der Temperaturdaten meldet. Dieses Anlagenmodell definiert einen Alarm, der erkennt, wenn der Kessel überhitzt.

```
{
  "assetModelName": "Boiler Model",
  "assetModelDescription": "Represents a boiler.",
  "assetModelProperties": [
    {
      "name": "Temperature",
      "dataType": "DOUBLE",
      "unit": "C",
      "type": {
        "measurement": {}
      }
    },
    {
      "name": "Temperature Max Threshold",
      "dataType": "DOUBLE",
      "type": {
        "attribute": {
          "defaultValue": "105.0"
        }
      }
    },
    {
      "name": "identityStoreId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "d-123EXAMPLE"
        }
      }
    },
    {
      "name": "userId",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "123EXAMPLE-a1b2c3d4-5678-90ab-cdef-33333EXAMPLE"
        }
      }
    },
    {
      "name": "senderId",
      "dataType": "STRING",
      "type": {
```

```
        "attribute": {
          "defaultValue": "MyFactory"
        }
      }
    },
    {
      "name": "fromAddress",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "my.factory@example.com"
        }
      }
    },
    {
      "name": "emailSubject",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "[ALERT] High boiler temperature"
        }
      }
    },
    {
      "name": "additionalMessage",
      "dataType": "STRING",
      "type": {
        "attribute": {
          "defaultValue": "Turn off the power before you check the alarm."
        }
      }
    }
  ],
  "assetModelHierarchies": [

  ],
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
```

```
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

Schritt 2: Definition eines Alarmmodells AWS IoT Events

Erstellen Sie das Alarmmodell in AWS IoT Events. In AWS IoT Events verwenden Sie Ausdrücke, um Werte in Alarmmodellen anzugeben. Sie können Ausdrücke verwenden, um Werte anzugeben AWS IoT SiteWise , die ausgewertet und als Eingaben für den Alarm verwendet werden sollen. Wenn die Eigenschaftswerte einer Anlage AWS IoT SiteWise an das Alarmmodell sendet, AWS IoT Events wertet sie den Ausdruck aus, um den Wert der Eigenschaft oder die ID der Anlage zu ermitteln. Sie können die folgenden Ausdrücke im Alarmmodell verwenden:

- Werte von Vermögenswerten

  Verwenden Sie den folgenden Ausdruck, um den Wert einer Anlageneigenschaft zu ermitteln. Ersetzen Sie *`Asset ModelId`* durch die ID des Asset-Modells und *`propertyId`* durch die ID der Eigenschaft.

  ```
  $sitewise.assetModel.`assetModelId`.`propertyId`.propertyValue.value
  ```

- Objekt-IDs

  Verwenden Sie den folgenden Ausdruck, um die ID des Assets abzurufen. Ersetzen Sie *`Asset ModelId`* durch die ID des Asset-Modells und *`propertyId`* durch die ID der Eigenschaft.

```
$sitewise.assetModel.`assetModelId`.`propertyId`.assetId
```

> **Note**
>
> Wenn Sie das Alarmmodell erstellen, können Sie Literale anstelle von Ausdrücken definieren, die zu Werten ausgewertet werden AWS IoT SiteWise . Dadurch kann die Anzahl der Attribute, die Sie in Ihrem Asset-Modell definieren, reduziert werden. Wenn Sie jedoch einen Wert als Literalwert definieren, können Sie diesen Wert nicht für Anlagen anpassen, die auf dem Anlagemodell basieren. Ihre AWS IoT SiteWise Monitor Benutzer können den Alarm auch nicht anpassen, da sie Alarmeinstellungen nur für Assets konfigurieren können.

So erstellen Sie ein AWS IoT Events Alarmmodell (CLI)

1. Wenn Sie das Alarmmodell in erstellen AWS IoT Events, müssen Sie die ID jeder Eigenschaft angeben, die der Alarm verwendet. Dazu gehören:

   - Die Eigenschaft „Alarmstatus“ im zusammengesetzten Objektmodell
   - Die Eigenschaft, die der Alarm überwacht
   - Das Schwellenwertattribut
   - (Optional) Das ID-Attribut für den Identitätsspeicher von IAM Identity Center
   - (Optional) Das IAM Identity Center-Benutzer-ID-Attribut
   - (Optional) Das SMS-Absender-ID-Attribut
   - (Optional) Das E-Mail-Absender-Adressattribut
   - (Optional) Das E-Mail-Betreff-Attribut
   - (Optional) Das zusätzliche Nachrichtenattribut

   Führen Sie den folgenden Befehl aus, um die IDs dieser Eigenschaften im Asset-Modell abzurufen. Ersetzen Sie *asset-model-id durch die ID* des Asset-Modells aus dem vorherigen Schritt.

   ```
   aws iotsitewise describe-asset-model --asset-model-id asset-model-id
   ```

Die Operation gibt eine Antwort zurück, die Details des Komponentenmodells enthält. Notieren Sie sich die ID jeder Eigenschaft, die der Alarm verwendet. Sie verwenden diese IDs, wenn Sie das AWS IoT Events Alarmmodell im nächsten Schritt erstellen.

2. Erstellen Sie das Alarmmodell in AWS IoT Events. Gehen Sie wie folgt vor:

   a. Erstellen Sie eine Datei mit dem Namen `alarm-model-payload.json`.

   b. Kopieren Sie das folgende JSON-Objekt in die Datei.

   c. Geben Sie einen Namen (`alarmModelName`), eine Beschreibung (`alarmModelDescription`) und einen Schweregrad (`severity`) für Ihren Alarm ein. Geben Sie für den Schweregrad eine Ganzzahl an, die den Schweregrad Ihres Unternehmens widerspiegelt.

   > **Important**
   >
   > Das Alarmmodell muss denselben Namen haben wie das zusammengesetzte Alarmmodell, das Sie zuvor für Ihr Anlagenmodell definiert haben.
   > Namen von Alarmmodellen dürfen nur alphanumerische Zeichen enthalten.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3
}
```

   d. Fügen Sie dem Alarm die Vergleichsregel (`alarmRule`) hinzu. Diese Regel definiert die zu überwachende Eigenschaft (`inputProperty`), den zu vergleichenden Schwellenwert (`threshold`) und den zu verwendenden Vergleichsoperator (`comparisonOperator`).

   - Ersetzen Sie *`Asset ModelId`* durch die ID des Asset-Modells.
   - Ersetzen Sie den *`Alarm PropertyId`* durch die ID der Immobilie, die der Alarm überwacht.
   - Ersetzen Sie den *`Schwellenwert AttributeId`* durch die ID der Attributeigenschaft des Schwellenwerts.

- Ersetzen Sie *GREATER* durch den Operator, der verwendet werden soll, um die Eigenschaftswerte mit dem Schwellenwert zu vergleichen. Wählen Sie aus den folgenden Optionen aus:
  - LESS
  - LESS_OR_EQUAL
  - EQUAL
  - NOT_EQUAL
  - GREATER_OR_EQUAL
  - GREATER

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  }
}
```

e. Fügen Sie eine Aktion (`alarmEventActions`) hinzu, um den Alarmstatus an den AWS IoT SiteWise Zeitpunkt zu senden, an dem der Alarm seinen Status ändert.

> **Note**
>
> Für eine erweiterte Konfiguration können Sie zusätzliche Aktionen definieren, die ausgeführt werden, wenn sich der Zustand des Alarms ändert. Sie können beispielsweise eine AWS Lambda Funktion aufrufen oder zu einem MQTT-Thema veröffentlichen. Weitere Informationen finden Sie unter Arbeiten mit anderen AWS Diensten im AWS IoT Events Entwicklerhandbuch.

- Ersetzen Sie *Asset ModelId* durch die ID des Asset-Modells.
- Ersetzen Sie den *Alarm PropertyId* durch die ID der Immobilie, die der Alarm überwacht.
- Ersetzen Sie die *StatePropertyAlarm-ID* durch die ID der Eigenschaft „Alarmstatus“ im zusammengesetzten Alarm-Modell.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  }
}
```

f. (Optional) Konfigurieren Sie die Einstellungen für die Alarmbenachrichtigung. Die Alarmbenachrichtigungsaktion verwendet eine Lambda-Funktion in Ihrem Konto, um Alarmbenachrichtigungen zu senden. Weitere Informationen finden Sie unter Anforderungen für Alarmbenachrichtigungen. In den Einstellungen für Alarmbenachrichtigungen können Sie SMS- und E-Mail-Benachrichtigungen konfigurieren, die an IAM Identity Center-Benutzer gesendet werden. Gehen Sie wie folgt vor:

i. Fügen Sie die Konfiguration für Alarmbenachrichtigungen (`alarmNotification`) zur Payload in hinzu. `alarm-model-payload.json`

- Ersetzen Sie *`NotificationFunctionAlarm-Arn`* durch den ARN der Lambda-Funktion, die Alarmbenachrichtigungen verarbeitet.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        }
      }
    ]
  }
```

```
}
```

ii. (Optional) Konfigurieren Sie die SMS-Benachrichtigungen (`smsConfigurations`), die an einen IAM Identity Center-Benutzer gesendet werden, wenn sich der Status des Alarms ändert.

- Ersetzen Sie *`identity StoreId AttributeId`* durch die ID des Attributs, das die ID des IAM Identity Center-Identitätsspeichers enthält.
- Ersetzen Sie *`IdAttributeBenutzer-ID`* durch die ID des Attributs, das die ID des IAM Identity Center-Benutzers enthält.
- Ersetzen Sie die *`IdAttributeAbsender-ID`* durch die ID des Attributs, das die Amazon SNS SNS-Sender-ID enthält, oder entfernen Sie sie `senderId` aus der Payload.
- Ersetzen Sie die *`zusätzliche MessageAttribute ID`* durch die ID des Attributs, das die zusätzliche Nachricht enthält, oder entfernen Sie sie `additionalMessage` aus der Payload.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
```

```
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
          }
        ]
      }
    ]
  }
}
```

iii. (Optional) Konfigurieren Sie die E-Mail-Benachrichtigungen (`emailConfigurations`), die an einen IAM Identity Center-Benutzer gesendet werden, wenn sich der Status des Alarms ändert.

- Ersetzen Sie *`identity StoreId AttributeId`* durch die ID der IAM Identity Center Identity Store-ID-Attributeigenschaft.
- Ersetzen Sie *`IdAttributeBenutzer-ID`* durch die ID der IAM Identity Center-Benutzer-ID-Attributeigenschaft.
- Ersetzen Sie *`from AddressAttribute Id`* durch die ID der Adressattributeigenschaft „from“ oder entfernen Sie sie `from` aus der Payload.

- Ersetzen Sie die *SubjectAttributeE-Mail-ID* durch die ID der Eigenschaft des E-Mail-Betreff-Attributs oder entfernen Sie es `subject` aus der Payload.
- Ersetzen Sie die *zusätzliche MessageAttribute ID* durch die ID der zusätzlichen Nachrichtenattributeigenschaft oder entfernen Sie sie `additionalMessage` aus der Payload.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
```

```
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value"
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.va
                    "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
            "content": {
              "subject":
"$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value
              "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.
            }
          }
        ]
      }
    ]
  }
}
```

g. (Optional) Fügen Sie die Alarmfunktionen (`alarmCapabilities`) zur Payload in hinzu. `alarm-model-payload.json` In diesem Objekt können Sie angeben, ob der Bestätigungsfluss aktiviert ist, und den standardmäßigen Aktivierungsstatus für Anlagen auf der Grundlage des Asset-Modells festlegen. Weitere Informationen zum Bestätigungsfluss finden Sie unterAlarmzustände.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
```

```
              "ssoIdentity": {
                "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
              }
            }
          ],
          "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
          "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
        }
      ],
      "emailConfigurations": [
        {
          "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
          "recipients": {
            "to": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ]
          },
          "content": {
            "subject":
"$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        }
      ]
    }
  ]
 },
 "alarmCapabilities": {
   "initializationConfiguration": {
     "disabledOnInitialization": false
```

```
    },
    "acknowledgeFlow": {
      "enabled": true
    }
  }
}
```

h. Fügen Sie die IAM-Dienstrolle (`roleArn`) hinzu, die davon ausgehen AWS IoT Events kann, Daten an zu AWS IoT SiteWise senden. Für diese Rolle sind die `iotsitewise:BatchPutAssetPropertyValue` Genehmigung und eine Vertrauensbeziehung erforderlich, die es ermöglichen, die Rolle `iotevents.amazonaws.com` zu übernehmen. Zum Senden von Benachrichtigungen benötigt diese Rolle auch die `sso-directory:DescribeUser` Berechtigungen `lambda:InvokeFunction` und. Weitere Informationen finden Sie unter Alarm-Dienstrollen im AWS IoT Events Entwicklerhandbuch.

- Ersetzen Sie das `roleArn` durch den ARN der Rolle, die diese Aktionen ausführen AWS IoT Events kann.

```
{
  "alarmModelName": "BoilerTemperatureHighAlarm",
  "alarmModelDescription": "Detects when the boiler temperature is high.",
  "severity": 3,
  "alarmRule": {
    "simpleRule": {
      "inputProperty":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.propertyValue.value",
      "comparisonOperator": "GREATER",
      "threshold":
 "$sitewise.assetModel.`assetModelId`.`thresholdAttributeId`.propertyValue.value"
    }
  },
  "alarmEventActions": {
    "alarmActions": [
      {
        "iotSiteWise": {
          "assetId":
 "$sitewise.assetModel.`assetModelId`.`alarmPropertyId`.assetId",
          "propertyId": "'alarmStatePropertyId'"
        }
      }
```

```
    ]
  },
  "alarmNotification": {
    "notificationActions": [
      {
        "action": {
          "lambdaAction": {
            "functionArn": "alarmNotificationFunctionArn"
          }
        },
        "smsConfigurations": [
          {
            "recipients": [
              {
                "ssoIdentity": {
                  "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                  "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                }
              }
            ],
            "senderId":
"$sitewise.assetModel.`assetModelId`.`senderIdAttributeId`.propertyValue.value",
            "additionalMessage":
"$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
          }
        ],
        "emailConfigurations": [
          {
            "from":
"$sitewise.assetModel.`assetModelId`.`fromAddressAttributeId`.propertyValue.value",
            "recipients": {
              "to": [
                {
                  "ssoIdentity": {
                    "identityStoreId":
"$sitewise.assetModel.`assetModelId`.`identityStoreIdAttributeId`.propertyValue.value"
                    "userId":
"$sitewise.assetModel.`assetModelId`.`userIdAttributeId`.propertyValue.value"
                  }
                }
              ]
            },
```

```
            "content": {
              "subject":
 "$sitewise.assetModel.`assetModelId`.`emailSubjectAttributeId`.propertyValue.value",
              "additionalMessage":
 "$sitewise.assetModel.`assetModelId`.`additionalMessageAttributeId`.propertyValue.valu
            }
          }
        ]
      }
    ]
  },
  "alarmCapabilities": {
    "initializationConfiguration": {
      "disabledOnInitialization": false
    },
    "acknowledgeFlow": {
      "enabled": false
    }
  },
  "roleArn": "arn:aws:iam::123456789012:role/MyIoTEventsAlarmRole"
}
```

i. Führen Sie den folgenden Befehl aus, um das AWS IoT Events Alarmmodell aus der Payload in `alarm-model-payload.json` zu erstellen.

```
aws iotevents create-alarm-model --cli-input-json file://alarm-model-
payload.json
```

j. Die Operation gibt eine Antwort zurück, die den ARN des Alarmmodells enthält,`alarmModelArn`. Kopieren Sie diesen ARN, um ihn im nächsten Schritt in der Alarmdefinition Ihres Asset-Modells festzulegen.

Schritt 3: Aktivieren des Datenflusses zwischen AWS IoT SiteWise und AWS IoT Events

Nachdem Sie die erforderlichen Ressourcen in AWS IoT SiteWise und erstellt haben AWS IoT Events, können Sie den Datenfluss zwischen den Ressourcen aktivieren, um Ihren Alarm zu aktivieren. In diesem Abschnitt aktualisieren Sie die Alarmdefinition im Asset-Modell, um das Alarmmodell zu verwenden, das Sie im vorherigen Schritt erstellt haben.

So aktivieren Sie den Datenfluss zwischen AWS IoT SiteWise und AWS IoT Events (CLI)

- Stellen Sie das Alarmmodell als Alarmquelle im Asset-Modell ein. Gehen Sie wie folgt vor:

a. Führen Sie den folgenden Befehl aus, um die vorhandene Komponentenmodelldefinition abzurufen. Ersetzen Sie *asset-model-id* durch die ID des Komponentenmodells.

```
aws iotsitewise describe-asset-model --asset-model-id asset-model-id
```

Die Operation gibt eine Antwort zurück, die Details des Komponentenmodells enthält.

b. Erstellen Sie eine Datei namens `update-asset-model-payload.json` und kopieren Sie die Antwort des vorherigen Befehls in die Datei.

c. Entfernen Sie die folgenden Schlüssel-Wert-Paare aus der `update-asset-model-payload.json` Datei:

- `assetModelId`
- `assetModelArn`
- `assetModelCreationDate`
- `assetModelLastUpdateDate`
- `assetModelStatus`

d. Fügen Sie dem zuvor definierten zusammengesetzten Alarmmodell die Eigenschaft Alarmquelle (`AWS/ALARM_SOURCE`) hinzu. Ersetzen Sie *alarm ModelArn* durch den ARN des Alarmmodells, der den Wert der Eigenschaft Alarmquelle festlegt.

```
{
  ...
  "assetModelCompositeModels": [
    ...
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
        {
          "id": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "IOT_EVENTS"
            }
          }
        },
```

```
        {
          "id": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        },
        {
          "name": "AWS/ALARM_SOURCE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "alarmModelArn"
            }
          }
        }
      ]
    }
  ]
}
```

e. Führen Sie den folgenden Befehl aus, um das Asset-Modell mit der in der `update-asset-model-payload.json` Datei gespeicherten Definition zu aktualisieren. Ersetzen Sie *`asset-model-id`* durch die ID des Komponentenmodells.

```
aws iotsitewise update-asset-model \
  --asset-model-id asset-model-id \
  --cli-input-json file://update-asset-model-payload.json
```

Ihr Asset-Modell definiert jetzt einen Alarm, der in erkennt AWS IoT Events. Der Alarm überwacht die Zielimmobilie in allen Anlagen, die auf diesem Anlagenmodell basieren. Sie können den Alarm für jedes Asset konfigurieren, um Eigenschaften wie den Schwellenwert oder den IAM Identity Center-Empfänger für jedes Asset anzupassen. Weitere Informationen finden Sie unter Konfiguration von Alarmen für Anlagen.

Definition externer Alarme

Externe Alarme enthalten den Status eines Alarms, den Sie außerhalb eines AWS IoT SiteWise Alarms erkennen.

Definition eines externen Alarms (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um einen externen Alarm für ein vorhandenes Anlagenmodell zu definieren. Um einen externen Alarm für ein neues Asset-Modell zu definieren, erstellen Sie das Asset-Modell und führen Sie dann diese Schritte aus. Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen.

Um einen Alarm für ein Asset-Modell zu definieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Klicken Sie im Navigationsbereich auf Models (Modelle).
3. Wählen Sie das Asset-Modell aus, für das Sie einen Alarm definieren möchten.
4. Wählen Sie die Registerkarte Alarmdefinitionen.
5. Wählen Sie Alarm hinzufügen.
6. Wählen Sie in den Optionen für den Alarmtyp die Option Externer Alarm aus.
7. Geben Sie einen Namen für den Alarm ein.
8. (Optional) Geben Sie eine Beschreibung für Ihren Alarm ein.
9. Wählen Sie Alarm hinzufügen.

Definition eines externen Alarms (CLI)

Sie können den verwenden AWS CLI , um einen externen Alarm für ein neues oder vorhandenes Anlagenmodell zu definieren.

Um einem Asset-Modell einen externen Alarm hinzuzufügen, fügen Sie dem Asset-Modell ein zusammengesetztes Alarmmodell hinzu. Ein zusammengesetztes externes Alarmmodell spezifiziert den `EXTERNAL` Typ und keine Eigenschaft der Alarmquelle. Das folgende Beispiel für einen zusammengesetzten Alarm definiert einen externen Temperaturalarm.

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "BoilerTemperatureHighAlarm",
      "type": "AWS/ALARM",
      "properties": [
```

```
        {
          "name": "AWS/ALARM_TYPE",
          "dataType": "STRING",
          "type": {
            "attribute": {
              "defaultValue": "EXTERNAL"
            }
          }
        },
        {
          "name": "AWS/ALARM_STATE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/ALARM_STATE",
          "type": {
            "measurement": {}
          }
        }
      ]
    }
  ]
}
```

Weitere Informationen zum Hinzufügen eines zusammengesetzten Modells zu einem neuen oder vorhandenen Anlagenmodell finden Sie im Folgenden:

- Ein Asset-Modell erstellen (AWS CLI)
- Aktualisierung eines Asset- oder Komponentenmodells (AWS CLI)

Nachdem Sie den externen Alarm definiert haben, können Sie den Alarmstatus auf der Grundlage des Asset-Modells in Anlagen aufnehmen. Weitere Informationen finden Sie unter Status eines externen Alarms wird aufgenommen.

Konfiguration von Alarmen für Anlagen

Nachdem Sie einen AWS IoT Events Alarm für ein Asset-Modell definiert haben, können Sie den Alarm für jedes Asset basierend auf dem Asset-Modell konfigurieren. Sie können den Schwellenwert und die Benachrichtigungseinstellungen für den Alarm bearbeiten. Jeder dieser Werte ist ein Attribut auf dem Asset, sodass Sie den Standardwert des Attributs aktualisieren können, um diese Werte zu konfigurieren.

> **Note**
>
> Sie können diese Werte für AWS IoT Events Alarme konfigurieren, jedoch nicht für externe Alarme.

Themen

Konfiguration eines Schwellenwerts (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um den Wert des Attributs zu aktualisieren, das den Schwellenwert eines Alarms angibt.

Um den Schwellenwert eines Alarms zu aktualisieren (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarmschwellenwert aktualisieren möchten.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Suchen Sie das Attribut, das der Alarm für seinen Schwellenwert verwendet, und geben Sie dann seinen neuen Wert ein.
6. Wählen Sie Speichern.

Einen Schwellenwert konfigurieren (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um den Wert des Attributs zu aktualisieren, das den Schwellenwert eines Alarms angibt.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

Verwenden Sie die Operation „BatchPutAssetPropertyWert“, um Ihrem Objekt Attributwerte zuzuweisen. Mit dieser Operation können Sie mehrere Attribute gleichzeitig festlegen. Die Nutzlast dieser Operation enthält eine Liste von Einträgen, jeweils mit der Komponenten-ID, der Eigenschafts-ID und dem Attributwert.

Um den Wert eines Attributs zu aktualisieren (AWS CLI)

1. Erstellen Sie eine Datei namens `batch-put-payload.json` und kopieren Sie das folgende JSON-Objekt in die Datei. In diesem Nutzlast-Beispiel wird veranschaulicht, wie der Breiten- und Längengrad einer Windturbine festgelegt wird. Aktualisieren Sie die IDs, Werte und Zeitstempel, um die Nutzlast für Ihren Anwendungsfall zu ändern.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
```

```
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

- Jeder Eintrag in der Nutzlast enthält eine `entryId`, die Sie als eindeutige Zeichenfolge definieren können. Bei fehlgeschlagenen Anforderungseinträgen enthält jeder Fehler die `entryId` der entsprechenden Anforderung, woran Sie erkennen können, welche Anforderungen zu wiederholen sind.
- Um einen Attributwert festzulegen, können Sie `propertyValues` für jede Attributeigenschaft eine timestamp-quality-value (TQV-) Struktur in die Liste aufnehmen. Diese Struktur muss den neuen `value` und den aktuellen `timestamp` enthalten.
  - `value`— Eine Struktur, die je nach Typ der festzulegenden Eigenschaft eines der folgenden Felder enthält:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Eine Struktur, die die aktuelle Unix-Epoche in Sekunden enthält,`timeInSeconds`. AWS IoT SiteWise lehnt alle Datenpunkte mit Zeitstempeln ab, die länger als 7 Tage in der Vergangenheit oder neuer als 5 Minuten in der future existierten.

Weitere Hinweise zur Vorbereitung einer Payload für BatchPutAssetPropertyValue finden Sie unter. Daten mithilfe der AWS IoT SiteWise API aufnehmen

2. Führen Sie den folgenden Befehl aus, um die Attributwerte an zu AWS IoT SiteWise senden:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-
payload.json
```

Konfiguration der Benachrichtigungseinstellungen (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um den Wert der Attribute zu aktualisieren, die die Benachrichtigungseinstellungen für einen Alarm angeben.

Um die Benachrichtigungseinstellungen eines Alarms zu aktualisieren (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie die Alarmeinstellungen aktualisieren möchten.
4. Wählen Sie Bearbeiten aus.
5. Suchen Sie das Attribut, das der Alarm für die Benachrichtigungseinstellung verwendet, die Sie ändern möchten, und geben Sie dann den neuen Wert ein.
6. Wählen Sie Speichern.

Konfiguration der Benachrichtigungseinstellungen (CLI)

Sie können die AWS Command Line Interface (AWS CLI) verwenden, um den Wert des Attributs zu aktualisieren, das die Benachrichtigungseinstellungen für einen Alarm angibt.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

Verwenden Sie die Operation „BatchPutAssetPropertyWert“, um Ihrem Objekt Attributwerte zuzuweisen. Mit dieser Operation können Sie mehrere Attribute gleichzeitig festlegen. Die Nutzlast dieser Operation enthält eine Liste von Einträgen, jeweils mit der Komponenten-ID, der Eigenschafts-ID und dem Attributwert.

Um den Wert eines Attributs zu aktualisieren (AWS CLI)

1. Erstellen Sie eine Datei namens `batch-put-payload.json` und kopieren Sie das folgende JSON-Objekt in die Datei. In diesem Nutzlast-Beispiel wird veranschaulicht, wie der Breiten- und Längengrad einer Windturbine festgelegt wird. Aktualisieren Sie die IDs, Werte und Zeitstempel, um die Nutzlast für Ihren Anwendungsfall zu ändern.

```
{
  "entries": [
    {
      "entryId": "windfarm3-turbine7-latitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 47.6204
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    },
    {
      "entryId": "windfarm3-turbine7-longitude",
      "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
      "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE",
      "propertyValues": [
        {
          "value": {
            "doubleValue": 122.3491
          },
          "timestamp": {
            "timeInSeconds": 1575691200
          }
        }
      ]
    }
  ]
}
```

- Jeder Eintrag in der Nutzlast enthält eine `entryId`, die Sie als eindeutige Zeichenfolge definieren können. Bei fehlgeschlagenen Anforderungseinträgen enthält jeder Fehler die `entryId` der entsprechenden Anforderung, woran Sie erkennen können, welche Anforderungen zu wiederholen sind.
- Um einen Attributwert festzulegen, können Sie `propertyValues` für jede Attributeigenschaft eine timestamp-quality-value (TQV-) Struktur in die Liste aufnehmen. Diese Struktur muss den neuen `value` und den aktuellen `timestamp` enthalten.
  - `value`— Eine Struktur, die je nach Typ der festzulegenden Eigenschaft eines der folgenden Felder enthält:
    - `booleanValue`
    - `doubleValue`
    - `integerValue`
    - `stringValue`
  - `timestamp`— Eine Struktur, die die aktuelle Unix-Epoche in Sekunden enthält,`timeInSeconds`. AWS IoT SiteWise lehnt alle Datenpunkte mit Zeitstempeln ab, die länger als 7 Tage in der Vergangenheit oder neuer als 5 Minuten in der future existierten.

Weitere Hinweise zur Vorbereitung einer Payload für BatchPutAssetPropertyValue finden Sie unter. Daten mithilfe der AWS IoT SiteWise API aufnehmen

2. Führen Sie den folgenden Befehl aus, um die Attributwerte an zu AWS IoT SiteWise senden:

```
aws iotsitewise batch-put-asset-property-value -\-cli-input-json file://batch-put-payload.json
```

Auf Alarme reagieren

Wenn sich der Status eines AWS IoT Events Alarms ändert, können Sie wie folgt auf den Alarm reagieren:

- Bestätigen Sie einen Alarm, um anzuzeigen, dass Sie sich mit dem Problem befassen.
- Schalten Sie einen Alarm in die Schlummerfunktion, um ihn vorübergehend zu deaktivieren.
- Deaktivieren Sie einen Alarm, um ihn dauerhaft zu deaktivieren, bis Sie ihn wieder aktivieren.
- Aktivieren Sie einen deaktivierten Alarm, um den Alarmstatus zu erkennen.

- Setzen Sie einen Alarm zurück, um seinen Status und seinen letzten Wert zu löschen.

Sie können die AWS IoT SiteWise Konsole oder die AWS IoT Events API verwenden, um auf einen Alarm zu reagieren.

> **Note**
>
> Sie können auf AWS IoT Events Alarme reagieren, aber nicht auf externe Alarme.

Themen

Auf einen Alarm reagieren (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um einen Alarm zu bestätigen, in den Schlummermodus zu versetzen, zu deaktivieren oder zu aktivieren.

Themen

Bestätigen Sie einen Alarm (Konsole)

Sie können einen Alarm bestätigen, um anzuzeigen, dass Sie das Problem lösen.

> **Note**
>
> Sie müssen den Bestätigungsfluss für den Alarm aktivieren, damit Sie den Alarm bestätigen können. Diese Option ist standardmäßig aktiviert, wenn Sie den Alarm von der AWS IoT SiteWise Konsole aus definieren.

Um einen Alarm zu bestätigen (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarm bestätigen möchten.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie die Registerkarte Alarme.
5. Wählen Sie den Alarm aus, den Sie bestätigen möchten, und wählen Sie dann Aktionen, um das Aktionsmenü für die Reaktion zu öffnen.
6. Wählen Sie Acknowledge (Bestätigen). Der Status des Alarms wechselt zu Bestätigt.

Alarmanlage ausschalten (Konsole)

Sie können einen Alarm in die Schlummerfunktion versetzen, um ihn vorübergehend zu deaktivieren. Geben Sie die Dauer an, für die der Alarm deaktiviert werden soll.

Um einen Alarm in die Schlummerfunktion zu versetzen (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarm in die Schlummerfunktion versetzen möchten.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie die Registerkarte Alarme.
5. Wählen Sie den Alarm aus, der in den Schlummermodus versetzt werden soll, und wählen Sie dann Aktionen, um das Aktionsmenü für die Reaktion zu öffnen.

6. Wählen Sie „Schlummern“. Es wird ein Modell geöffnet, in dem Sie die Dauer für den Schlummermodus angeben.
7. Wählen Sie die Schlummerlänge oder geben Sie eine benutzerdefinierte Schlummerlänge ein.
8. Wählen Sie Speichern. Der Alarmstatus wechselt zu Snoozed.

Deaktiviert einen Alarm (Konsole)

Sie können einen Alarm deaktivieren, sodass er nicht mehr erkannt wird. Nachdem Sie den Alarm deaktiviert haben, müssen Sie ihn erneut aktivieren, wenn der Alarm erkannt werden soll.

Um einen Alarm zu deaktivieren (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarm deaktivieren möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie die Registerkarte Alarme.
5. Wählen Sie den Alarm aus, den Sie deaktivieren möchten, und wählen Sie dann Aktionen, um das Aktionsmenü für die Reaktion zu öffnen.
6. Wählen Sie Disable (deaktivieren) aus. Der Status des Alarms ändert sich zu Deaktiviert.

Aktiviert einen Alarm (Konsole)

Sie können einen Alarm so einrichten, dass er erneut erkannt wird, nachdem Sie ihn deaktiviert oder die Schlummerfunktion aktiviert haben.

Um einen Alarm zu aktivieren (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarm aktivieren möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie die Registerkarte Alarme.
5. Wählen Sie den Alarm aus, den Sie aktivieren möchten, und wählen Sie dann Aktionen, um das Aktionsmenü für die Reaktion zu öffnen.
6. Wählen Sie Enable (Aktivieren) aus. Der Zustand des Alarms wechselt zu Normal.

Einen Alarm zurücksetzen (Konsole)

Sie können einen Alarm zurücksetzen, um seinen Status und seinen letzten Wert zu löschen.

Um einen Alarm zurückzusetzen (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie das Asset aus, für das Sie einen Alarm zurücksetzen möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie die Registerkarte Alarme.
5. Wählen Sie den Alarm aus, den Sie aktivieren möchten, und wählen Sie dann Aktionen, um das Aktionsmenü für die Reaktion zu öffnen.
6. Klicken Sie auf Reset (Zurücksetzen). Der Zustand des Alarms wechselt zu Normal.

Auf einen Alarm reagieren (API)

Sie können die AWS IoT Events API verwenden, um einen Alarm zu bestätigen, in den Schlummermodus zu versetzen, zu deaktivieren, zu aktivieren oder zurückzusetzen. Weitere Informationen finden Sie in der AWS IoT Events API-Referenz zu den folgenden Vorgängen:

- BatchAcknowledgeAlarm
- BatchSnoozeAlarm
- BatchDisableAlarm
- BatchEnableAlarm
- BatchResetAlarm

Weitere Informationen finden Sie unter Reagieren auf Alarme im AWS IoT Events Entwicklerhandbuch.

Status eines externen Alarms wird aufgenommen

Externe Alarme sind Alarme, die Sie außerhalb von auswerten AWS IoT SiteWise. Sie können externe Alarme verwenden, wenn Sie über eine Datenquelle verfügen, die den Alarmstatus meldet und in die Sie Daten aufnehmen möchten AWS IoT SiteWise.

Für die Eigenschaften des Alarmstatus ist ein bestimmtes Format für die Datenwerte des Alarmstatus erforderlich. Jeder Datenwert muss ein JSON-Objekt sein, das in eine Zeichenfolge serialisiert ist. Anschließend nehmen Sie die serialisierte Zeichenfolge als Zeichenkettenwert auf. Weitere Informationen finden Sie unter Eigenschaften des Alarmstatus.

Example Beispiel für einen Datenwert für den Alarmstatus (nicht serialisiert)

```
{
  "stateName": "Active"
}
```

Example Beispiel für einen Datenwert für den Alarmstatus (serialisiert)

```
{\"stateName\":\"Active\"}
```

> **Note**
>
> Wenn Ihre Datenquelle keine Daten in diesem Format melden kann oder Sie Ihre Daten vor der Aufnahme nicht in dieses Format konvertieren können, entscheiden Sie sich möglicherweise dafür, keine Alarm-Eigenschaft zu verwenden. Stattdessen können Sie die Daten beispielsweise als Messeigenschaft mit dem Datentyp Zeichenfolge

aufnehmen. Weitere Informationen finden Sie unter Definition von Datenströmen aus Geräten (Messungen) und Daten aufnehmen zu AWS IoT SiteWise.

Zuordnung externer Alarmzustandsströme

Sie können Eigenschaftsaliase definieren, um Ihre Datenströme Ihren Alarmzustandseigenschaften zuzuordnen. Auf diese Weise können Sie beim Aufnehmen oder Abrufen von Daten auf einfache Weise eine Eigenschaft für den Alarmstatus identifizieren. Weitere Informationen zu Eigenschaftsaliasnamen finden Sie unter. Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften

Themen

- Zuordnung externer Alarmstatus-Streams (Konsole)
- Zuordnen externer Alarmstatus-Streams (AWS CLI)

Zuordnung externer Alarmstatus-Streams (Konsole)

Sie können Eigenschaftsaliase definieren, um Ihre Datenströme Ihren Alarmzustandseigenschaften zuzuordnen. Auf diese Weise können Sie beim Aufnehmen oder Abrufen von Daten auf einfache Weise eine Eigenschaft für den Alarmstatus identifizieren. Weitere Informationen zu Eigenschaftsaliasnamen finden Sie unter. Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften

Sie können die AWS IoT SiteWise Konsole verwenden, um einen Alias für eine Alarmstatuseigenschaft festzulegen.

Um einen Eigenschaftsalias für eine Alarmstatuseigenschaft festzulegen (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die Komponente aus, für die Sie einen Eigenschaftenalias festlegen möchten.

> **Tip**
>
> Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Scrollen Sie zu Alarme und erweitern Sie den Bereich.
6. Geben Sie unter Externe Alarme den Alias im Feld Eigenschaftsalias — optional ein.
7. Wählen Sie Speichern.

Zuordnen externer Alarmstatus-Streams (AWS CLI)

Sie können Eigenschaftsaliase definieren, um Ihre Datenströme Ihren Alarmzustandseigenschaften zuzuordnen. Auf diese Weise können Sie beim Aufnehmen oder Abrufen von Daten auf einfache Weise eine Eigenschaft für den Alarmstatus identifizieren. Weitere Informationen zu Eigenschaftsaliasnamen finden Sie unter. Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um einen Alias für eine Alarmstatuseigenschaft festzulegen.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

> **Note**
>
> Die DescribeAssetAntwort enthält die Liste der zusammengesetzten Asset-Modelle für das Asset. Jeder Alarm ist ein zusammengesetztes Modell. Um das zu finden`propertyId`, suchen Sie das zusammengesetzte Modell für den Alarm und suchen Sie dann die `AWS/ALARM_STATE` Eigenschaft in diesem zusammengesetzten Modell.

Weitere Hinweise zum Festlegen des Eigenschaftsalias finden Sie unterEinen Eigenschaftsalias einrichten (AWS CLI).

Daten zum Alarmstatus werden aufgenommen

Eigenschaften für den Alarmstatus erwarten den Alarmstatus als serialisierte JSON-Zeichenfolge. Um den Alarmstatus in einen externen Alarm zu übernehmen AWS IoT SiteWise, nehmen Sie diese

serialisierte Zeichenfolge als Zeichenkettenwert mit Zeitstempel auf. Das folgende Beispiel zeigt einen Zustandsdatenwert für einen aktiven Alarm.

```
{\"stateName\":\"Active\"}
```

Um eine Eigenschaft für den Alarmstatus zu identifizieren, können Sie eine der folgenden Optionen angeben:

- Das `assetId` Ende `propertyId` der Alarm-Eigenschaft, an die Sie Daten senden.
- Das`propertyAlias`, was ein Datenstream-Alias ist (z. B.`/company/windfarm/3/turbine/7/temperature/high`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias Ihrer Alarm-Eigenschaft festlegen. Informationen zum Festlegen von Eigenschaftsaliasnamen für Eigenschaften des Alarmstatus finden Sie unterZuordnung externer Alarmzustandsströme.

Das folgende Beispiel für eine BatchPutAssetPropertyValue-API-Payload zeigt, wie der Status eines externen Alarms formatiert wird. Dieser externe Alarm meldet, wenn der Wert der Umdrehungen pro Minute (U/min) einer Windturbine zu hoch ist.

Example Beispiel für eine BatchPutAssetPropertyValue Payload für Alarmzustandsdaten

```
{
    "entries": [
      {
        "entryId": "unique entry ID",
        "propertyAlias": "/company/windfarm/3/turbine/7/temperature/high",
        "propertyValues": [
          {
            "value": {
              "stringValue": "{\"stateName\":\"Active\"}"
            },
            "timestamp": {
              "timeInSeconds": 1607550262
            }
          }
        ]
      }
    ]
  }
```

Weitere Hinweise zur Verwendung der `BatchPutAssetPropertyValue` API zum Erfassen von Daten finden Sie unter. Daten mithilfe der AWS IoT SiteWise API aufnehmen

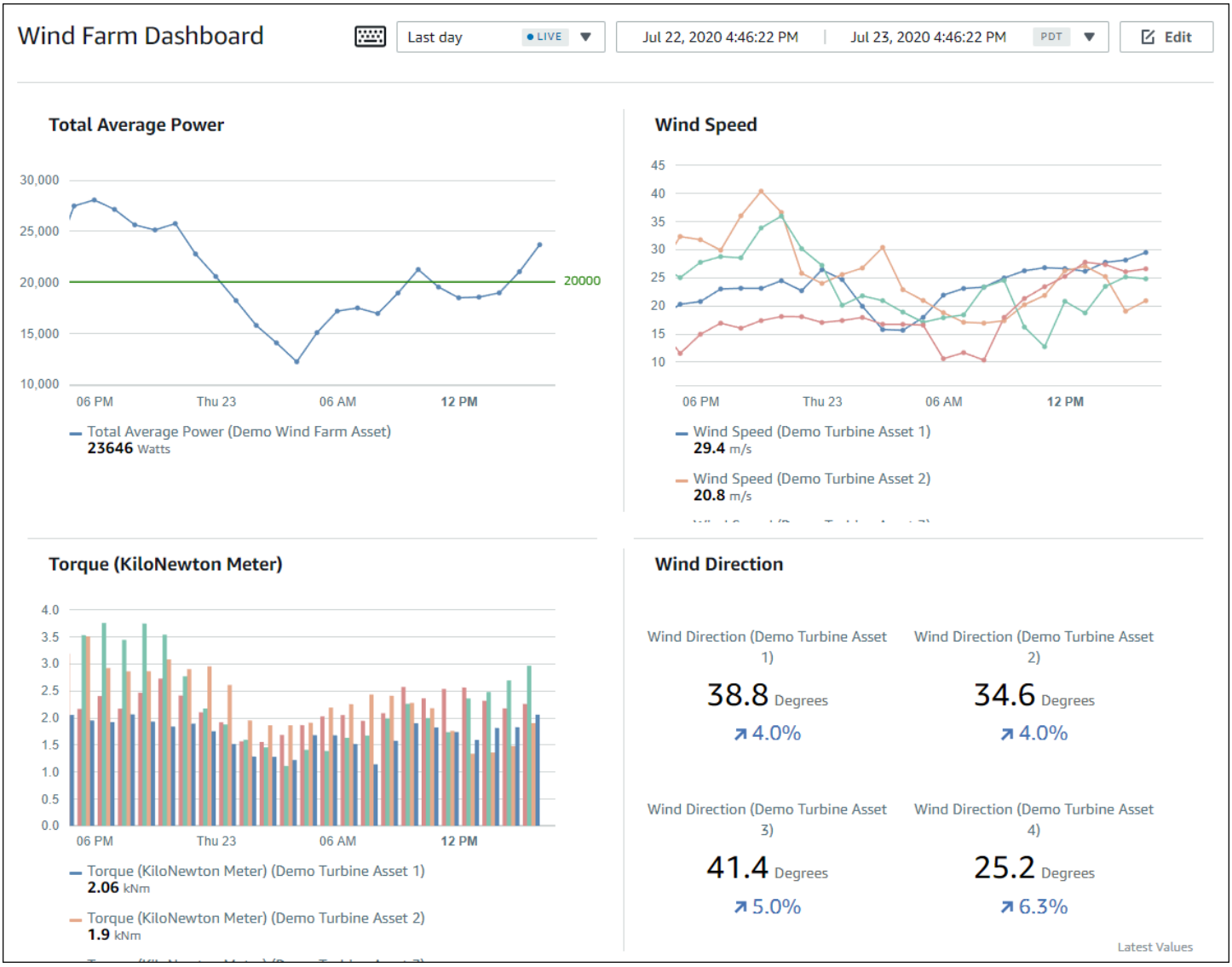
Weitere Hinweise zu anderen Möglichkeiten der Datenaufnahme finden Sie unter. Daten aufnehmen zu AWS IoT SiteWise

Daten überwachen mit AWS IoT SiteWise Monitor

Sie können AWS IoT SiteWise damit die Daten Ihrer Prozesse, Geräte und Geräte überwachen, indem Sie SiteWise Monitor-Webportale erstellen. SiteWise Monitor ist eine Funktion AWS IoT SiteWise , mit der Sie Portale in Form einer verwalteten Webanwendung erstellen können. Sie können diese Portale dann verwenden, um Ihre Betriebsdaten anzuzeigen und freizugeben. Sie können Projekte mit Dashboards erstellen, um Daten aus Ihren Prozessen, Geräten und Anlagen zu visualisieren, die mit AWS IoT verbunden sind.

Fachexperten, wie z. B. Verfahrenstechniker, können diese Portale nutzen, um schnell Einblicke in ihre Betriebsdaten zu erhalten und damit das Verhalten der Geräte und Anlagen zu verstehen.

Das folgende Beispiel zeigt ein Dashboard, das Daten für eine Windkraftanlage anzeigt.



Da Daten im Zeitverlauf AWS IoT SiteWise erfasst werden, können Sie SiteWise Monitor verwenden, um Betriebsdaten im Zeitverlauf oder die zuletzt gemeldeten Werte zu bestimmten Zeitpunkten anzuzeigen. Auf diese Weise können Sie Erkenntnisse gewinnen, die sonst nur schwer möglich sind.

SiteWise Rollen überwachen

Vier Rollen interagieren mit SiteWise Monitor:

AWS Administrator

Der AWS Administrator verwendet die AWS IoT SiteWise Konsole, um Portale zu erstellen. Der AWS -Administrator kann auch Portaladministratoren zuweisen und Portalbenutzer hinzufügen. Portaladministratoren weisen Portalbenutzer später Projekten als Eigentümer oder Betrachter zu. Der AWS Administrator arbeitet ausschließlich in der AWS Konsole.

Portaladministrator

Jedes SiteWise Monitor-Portal hat einen oder mehrere Portaladministratoren. Portaladministratoren verwenden das Portal, um Projekte zu erstellen, die Sammlungen von Komponenten und Dashboards enthalten. Der Portaladministrator weist dann jedem Projekt Komponenten und Eigentümer zu. Durch die Steuerung des Zugriffs auf das Projekt legen Portaladministratoren fest, welche Komponenten von Projekteigentümern und -betrachtern angezeigt werden können.

Projekteigentümer

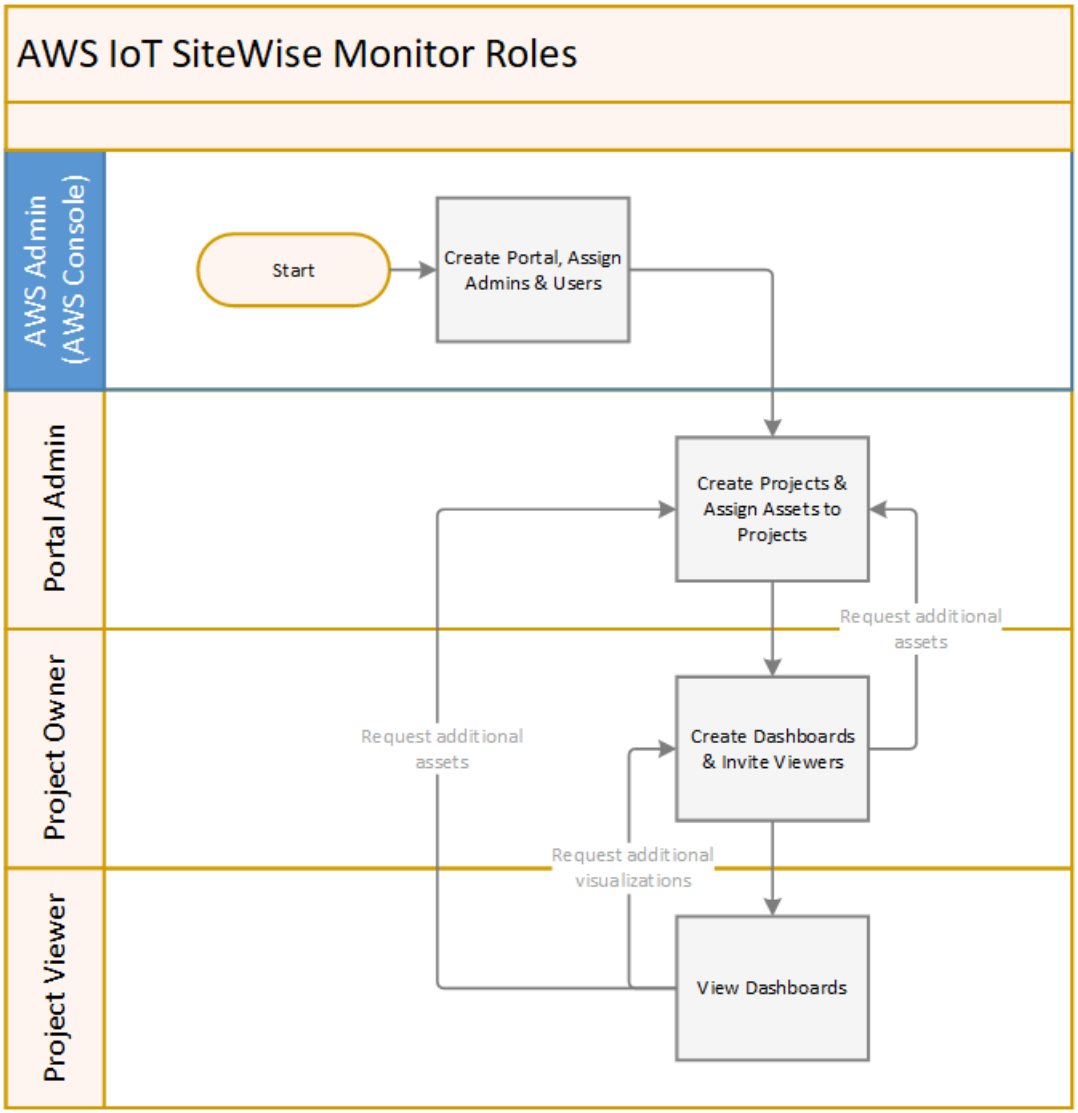
Jedes SiteWise Monitor-Projekt hat Besitzer. Projekteigentümer erstellen Visualisierungen in Form von Dashboards, um Betriebsdaten konsistent darzustellen. Wenn Dashboards zur Freigabe bereit sind, kann der Projekteigentümer Betrachter zu dem Projekt einladen. Projekteigentümer können dem Projekt auch andere Eigentümer zuweisen. Projekteigentümer können Schwellenwerte und Benachrichtigungseinstellungen für Alarme konfigurieren.

Projektbetrachter

Jedes SiteWise Monitor-Projekt hat Zuschauer. Projektbetrachter können eine Verbindung mit dem Portal herstellen, um die Dashboards anzuzeigen, die Projekteigentümer erstellt haben. In jedem Dashboard können Projektbetrachter den Zeitraum anpassen, um die Betriebsdaten besser zu verstehen. Projektbetrachter können nur Dashboards in den Projekten anzeigen, auf die sie Zugriff haben. Projektbeobachter können Alarme bestätigen und die Schlummerfunktion aktivieren.

Je nach Organisation kann dieselbe Person mehrere Rollen ausführen.

Die folgende Abbildung zeigt, wie diese vier Rollen im SiteWise Monitor-Portal interagieren.



Sie können mithilfe von AWS IAM Identity Center oder IAM verwalten, wer Zugriff auf Ihre Daten hat. Ihre Datennutzer können sich von einem Desktop- oder mobilen Browser aus mit ihren IAM Identity Center- oder IAM-Anmeldeinformationen bei SiteWise Monitor anmelden.

SAML-Verbund

IAM Identity Center und IAM unterstützen den Identitätsverbund mit SAML (Security Assertion Markup Language) 2.0. SAML 2.0 ist ein offener Standard, den viele externe Identitätsanbieter (IdPs) verwenden, um Benutzer zu authentifizieren und ihre Identitäts- und Sicherheitsinformationen an Service Provider (SPs) weiterzugeben. SPs sind in der Regel Anwendungen oder Dienste. Der

SAML-Verbund ermöglicht es Ihren SiteWise Monitor-Portaladministratoren und -Benutzern, sich mit externen Anmeldeinformationen, wie z. B. ihren Firmenbenutzernamen und Kennwörtern, bei den ihnen zugewiesenen Portalen anzumelden.

Sie können IAM Identity Center und IAM so konfigurieren, dass sie den SAML-basierten Verbund für den Zugriff auf Ihre Monitor-Portale verwenden. SiteWise

IAM Identity Center

Ihre Portaladministratoren und Benutzer können sich mit ihren Firmenbenutzernamen und AWS Kennwörtern beim Access-Portal anmelden. Sie können dann zu den ihnen zugewiesenen SiteWise Monitor-Portalen navigieren. IAM Identity Center verwendet Zertifikate, um eine SAML-Vertrauensbeziehung zwischen Ihrem Identitätsanbieter und einzurichten. AWSWeitere Informationen zum SCIM-Profil und zur SAML 2.0-Implementierung finden Sie im Benutzerhandbuch.AWS IAM Identity Center

IAM

Ihre Portaladministratoren und Benutzer können temporäre Sicherheitsanmeldedaten anfordern, um auf die ihnen zugewiesenen SiteWise Monitor-Portale zuzugreifen. Sie erstellen eine SAML-Identitätsanbieter-Identität in IAM, um eine Vertrauensbeziehung zwischen Ihrem Identitätsanbieter und einzurichten. AWSWeitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden eines SAML-basierten Verbunds für den API-Zugriff AWS auf.

Ihre Portaladministratoren und Benutzer können sich beim Portal Ihres Unternehmens anmelden und die Option auswählen, um zur Managementkonsole zu wechseln. AWS Sie können dann zu den ihnen zugewiesenen SiteWise Monitor-Portalen navigieren. Das Portal Ihres Unternehmens kümmert sich um den Vertrauensaustausch zwischen Ihrem Identitätsanbieter und AWS. Weitere Informationen finden Sie unter Aktivieren des Zugriffs auf die AWS Management Console durch SAML 2.0-Verbundbenutzer im IAM-Benutzerhandbuch.

> **Note**
>
> Vermeiden Sie beim Hinzufügen von Benutzern oder Administratoren zum Portal die Erstellung von IAM-Richtlinien, die Benutzerberechtigungen einschränken, z. B. eingeschränkte IP-Adressen. Alle angehängten Richtlinien mit eingeschränkten Berechtigungen können keine Verbindung zum AWS IoT SiteWise Portal herstellen.

SiteWise Konzepte überwachen

Um SiteWise Monitor verwenden zu können, sollten Sie mit den folgenden Konzepten vertraut sein:

Portal

Ein AWS IoT SiteWise Monitor Portal ist eine Webanwendung, mit der Sie Ihre AWS IoT SiteWise Daten visualisieren und gemeinsam nutzen können. Ein Portal verfügt über einen oder mehrere Administratoren und enthält keine oder mehrere Projekte.

Projekt

Jedes SiteWise Monitor-Portal enthält eine Reihe von Projekten. Jedem Projekt ist eine Teilmenge Ihrer AWS IoT SiteWise -Komponenten zugeordnet. Projekteigentümer erstellen ein oder mehrere Dashboards, um eine konsistente Möglichkeit zum Anzeigen der mit diesen Komponenten verknüpften Daten bereitzustellen. Projekteigentümer können Betrachter zu dem Projekt einladen, damit diese die Komponenten und Dashboards in dem Projekt anzeigen können. Das Projekt ist die grundlegende Einheit für die gemeinsame Nutzung innerhalb von SiteWise Monitor. Projekteigentümer können Benutzer einladen, denen der AWS Administrator Zugriff auf das Portal gewährt hat. Ein Benutzer muss Zugriff auf ein Portal haben, bevor ein Projekt in diesem Portal für diesen Benutzer freigegeben werden kann.

Komponente

Wenn Daten AWS IoT SiteWise aus Ihren Industrieanlagen aufgenommen werden, werden Ihre Geräte, Anlagen und Prozesse jeweils als Vermögenswerte dargestellt. Jeder Anlage sind Eigenschaften und Alarme zugeordnet. Der Portaladministrator weist jedem Projekt Komponenten zu.

Eigenschaft

Eigenschaften sind Zeitreihendaten, die Objekten zugeordnet sind. Beispielsweise kann ein Gerät eine Seriennummer, einen Standort, eine Marke und ein Modell sowie ein Installationsdatum aufweisen. Es kann auch Zeitreihenwerte für Verfügbarkeit, Leistung, Qualität, Temperatur, Druck usw. enthalten.

Alarm

Alarme überwachen die Eigenschaften, um zu erkennen, wenn sich Geräte außerhalb ihres Betriebsbereichs befinden. Jeder Alarm definiert einen Schwellenwert und eine zu überwachende Eigenschaft. Wenn die Eigenschaft den Schwellenwert überschreitet, wird der Alarm aktiv und weist darauf hin, dass Sie oder jemand aus Ihrem Team das Problem beheben sollten.

Projekteigentümer können die Schwellenwerte und Benachrichtigungseinstellungen für Alarme anpassen. Projektbeobachter können Alarme bestätigen und die Schlummerfunktion aktivieren und eine Nachricht mit Einzelheiten zum Alarm oder zu den Maßnahmen, die sie zu seiner Behebung ergriffen haben, hinterlassen.

Dashboard

Jedes Projekt enthält eine Reihe von Dashboards. Dashboards stellen eine Reihe von Visualisierungen für die Werte einer Gruppe von Komponenten bereit. Projekteigentümer erstellen die Dashboards und die darin enthaltenen Visualisierungen. Wenn ein Projekteigentümer bereit ist, die Gruppe von Dashboards freizugeben, kann der Eigentümer Betrachter zu dem Projekt einladen, wodurch diese Zugriff auf alle Dashboards in dem Projekt erhalten. Wenn Sie eine andere Gruppe von Betrachtern für verschiedene Dashboards wünschen, müssen Sie die Dashboards auf Projekte aufteilen. Wenn sich Zuschauer Dashboards ansehen, können sie den Zeitraum so anpassen, dass sie sich bestimmte Daten ansehen.

Visualisierung

In jedem Dashboard entscheiden die Projekteigentümer, wie die Eigenschaften und Alarme der mit dem Projekt verknüpften Assets angezeigt werden sollen. Die Verfügbarkeit kann als Liniendiagramm dargestellt werden, während andere Werte als Balkendiagramme oder Leistungskennzahlen (KPIs) angezeigt werden können. Alarme lassen sich am besten als Statusraster und Statuszeitleisten anzeigen. Projekteigentümer passen jede Visualisierung an, um die Daten für diese Komponente optimal darzustellen.

Erste Schritte mit AWS IoT SiteWise Monitor

Wenn Sie der AWS Administrator Ihrer Organisation sind, erstellen Sie Portale von der AWS IoT SiteWise Konsole aus. Gehen Sie wie folgt vor, um ein Portal zu erstellen, damit Mitglieder Ihrer Organisation Ihre AWS IoT SiteWise Daten einsehen können:

1. Konfigurieren und erstellen Sie ein Portal.
2. Fügen Sie Portaladministratoren hinzu, und senden Sie Einladungs-E-Mail-Nachrichten.
3. Fügen Sie Portalbenutzer hinzu

Nachdem Sie ein Portal erstellt haben, kann der Portaladministrator Ihre AWS IoT SiteWise Ressourcen anzeigen und sie Projekten im Portal zuweisen. Projekteigentümer können dann Dashboards erstellen, um die Eigenschaften der Komponenten zu visualisieren und den

Projektbetrachtern damit ein besseres Verständnis der Leistung Ihrer Geräte, Prozesse und Anlagen zu ermöglichen.

> **Note**
>
> Vermeiden Sie beim Hinzufügen von Benutzern oder Administratoren zum Portal die Erstellung von AWS Identity and Access Management (IAM-) Richtlinien, die Benutzerberechtigungen einschränken, wie z. B. eingeschränkte IP-Adressen. Alle angehängten Richtlinien mit eingeschränkten Berechtigungen können keine Verbindung zum AWS IoT SiteWise Portal herstellen.

Sie können einem Tutorial folgen, das die Schritte durchläuft, die zum Einrichten eines Portals mit einem Projekt, Dashboards und mehreren Benutzern für ein bestimmtes Szenario unter Verwendung von Windparkdaten erforderlich sind. Weitere Informationen finden Sie unter Visualisierung und gemeinsame Nutzung von Windparkdaten in Monitor SiteWise .

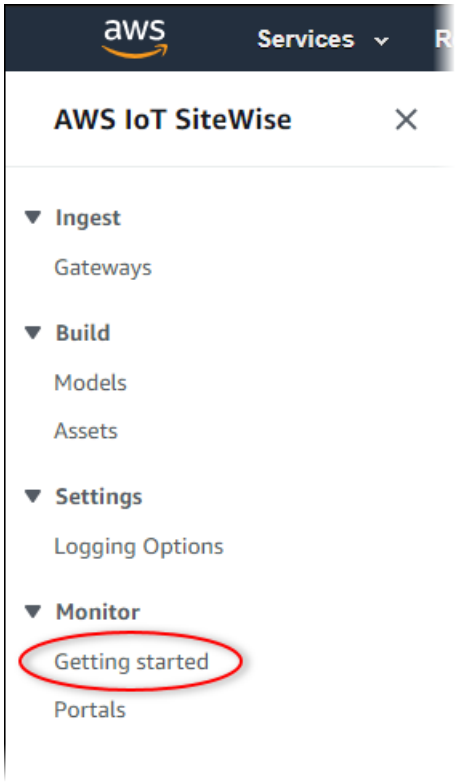
Themen

Erstellen eines Portals

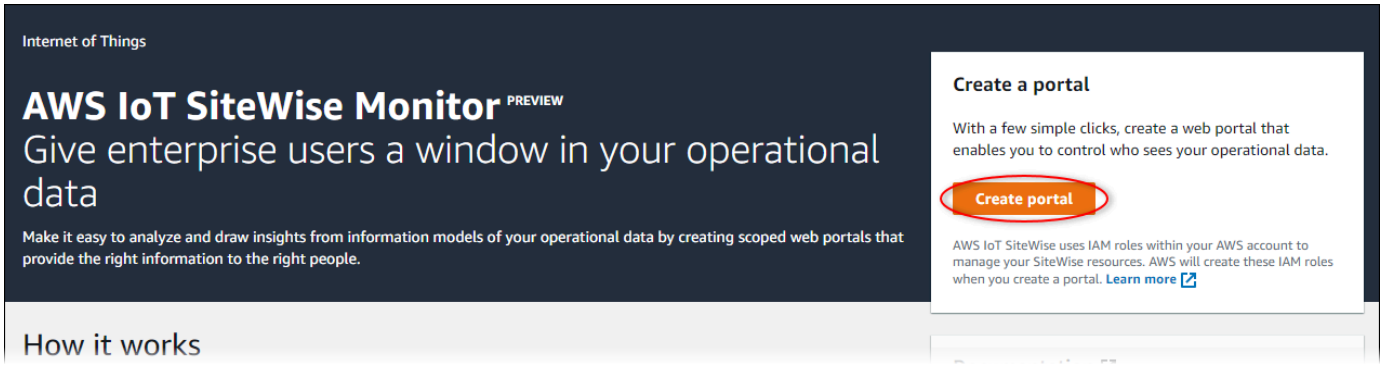
Sie erstellen ein SiteWise Monitor-Portal in der AWS IoT SiteWise Konsole.

So erstellen Sie ein Portal

1. Melden Sie sich an der AWS IoT SiteWise -Konsole an.
2. Wählen Sie im Navigationsbereich Monitor (Überwachen), Getting started (Erste Schritte) aus.



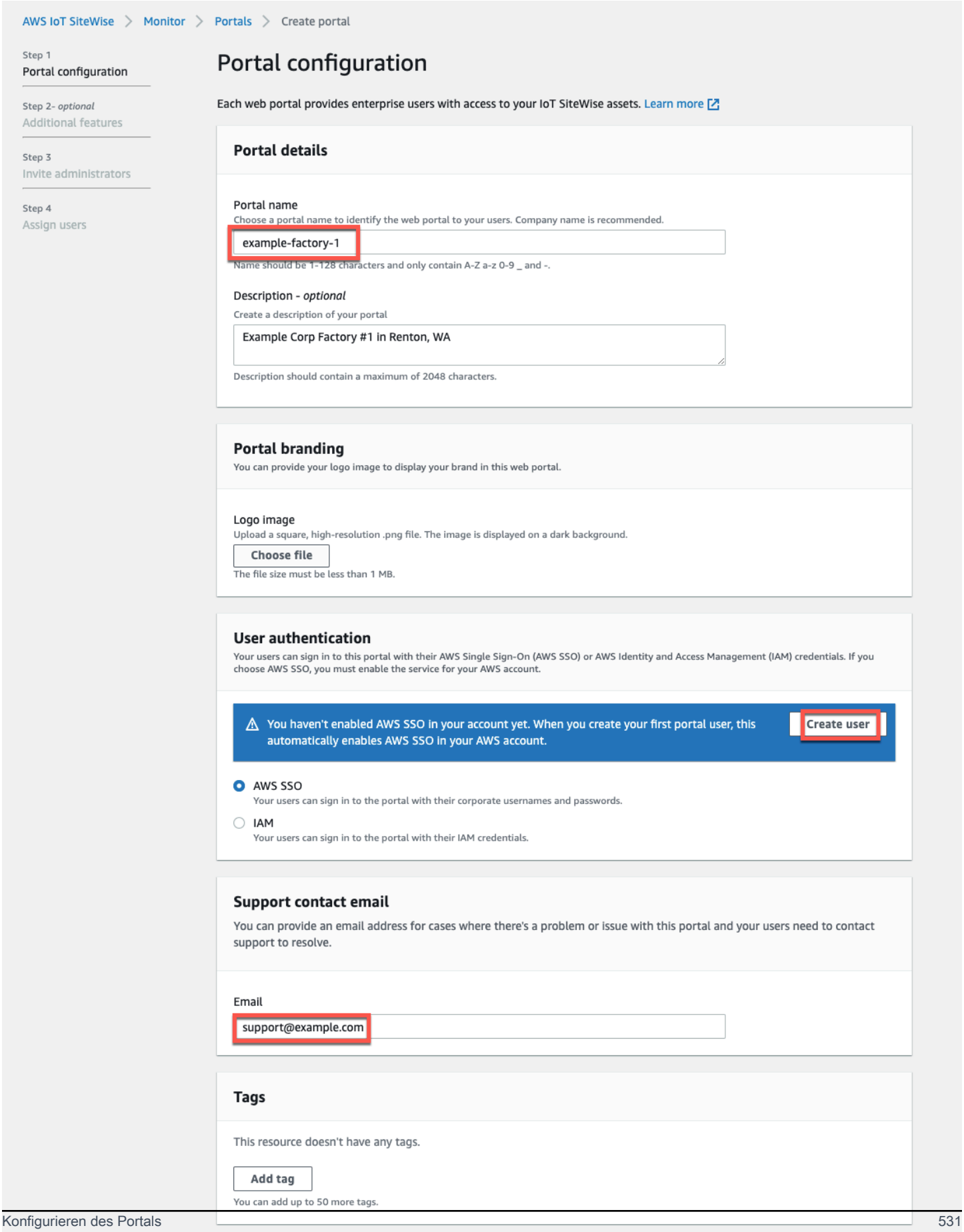
3. Wählen Sie Create Portal (Portal erstellen) aus.



Als Nächstes müssen Sie einige grundlegende Informationen zur Konfiguration des Portals angeben.

Konfigurieren des Portals

Ihre Benutzer verwenden Portale, um Ihre Daten anzuzeigen. Sie können den Namen, die Beschreibung, das Branding, die Benutzerauthentifizierung, die Support-Kontakt-E-Mail und die Berechtigungen eines Portals anpassen.


AWS IoT SiteWise > Monitor > Portals > Create portal
Step 1
Portal configuration
Step 2- optional
Additional features
Step 3
Invite administrators
Step 4
Assign users
Portal configuration
Each web portal provides enterprise users with access to your IoT SiteWise assets. Learn more
Portal details
Portal name
Choose a portal name to identify the web portal to your users. Company name is recommended.
example-factory-1
Name should be 1-128 characters and only contain A-Z a-z 0-9 _ and -.
Description - optional
Create a description of your portal
Example Corp Factory #1 in Renton, WA
Description should contain a maximum of 2048 characters.
Portal branding
You can provide your logo image to display your brand in this web portal.
Logo image
Upload a square, high-resolution .png file. The image is displayed on a dark background.
Choose file
The file size must be less than 1 MB.
User authentication
Your users can sign in to this portal with their AWS Single Sign-On (AWS SSO) or AWS Identity and Access Management (IAM) credentials. If you choose AWS SSO, you must enable the service for your AWS account.
You haven't enabled AWS SSO in your account yet. When you create your first portal user, this automatically enables AWS SSO in your AWS account.
Create user
AWS SSO
Your users can sign in to the portal with their corporate usernames and passwords.
IAM
Your users can sign in to the portal with their IAM credentials.
Support contact email
You can provide an email address for cases where there's a problem or issue with this portal and your users need to contact support to resolve.
Email
support@example.com
Tags
This resource doesn't have any tags.
Add tag
You can add up to 50 more tags.
Permissions
SiteWise Monitor assumes this role to give permissions to your federated users to access AWS IoT SiteWise resources. Learn

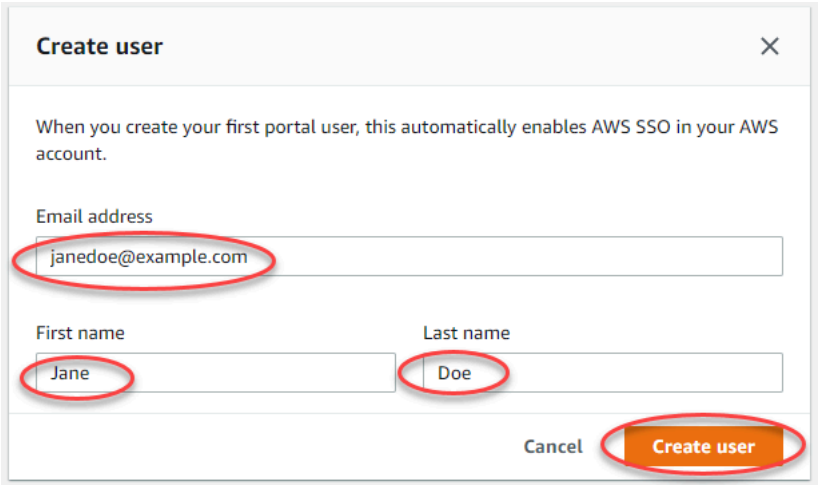
So konfigurieren Sie ein Portal:

1. Geben Sie einen Namen für Ihr Portal ein.
2. (Optional) Geben Sie eine Beschreibung für Ihr Portal ein. Wenn Sie über mehrere Portale verfügen, verwenden Sie aussagekräftige Beschreibungen, um den Überblick über die Inhalte der einzelnen Portale zu behalten.
3. (Optional) Laden Sie ein Bild hoch, um Ihre Marke im Portal anzuzeigen. Wählen Sie ein quadratisches PNG-Bild aus. Wenn Sie ein nicht quadratisches Bild hochladen, skaliert das Portal das Bild zu einem Quadrat.
4. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie IAM Identity Center, wenn sich Ihre Portalbenutzer mit ihren Firmenbenutzernamen und Passwörtern bei diesem Portal anmelden.

     Wenn Sie IAM Identity Center in Ihrem Konto nicht aktiviert haben, gehen Sie wie folgt vor:

     a. Wählen Sie Create user (Benutzer erstellen) aus.

     b. Um das erste Portal zu erstellen, geben Sie auf der Seite Benutzer erstellen die E-Mail-Adresse, den Vor- und Nachnamen des Benutzers ein und wählen Sie dann Benutzer erstellen aus.



> **Note**
>
> - AWS aktiviert IAM Identity Center automatisch in Ihrem Konto, wenn Sie den ersten Portalbenutzer erstellen.
> - Sie können IAM Identity Center jeweils nur in einer Region konfigurieren. SiteWise Monitor stellt eine Verbindung zu der Region her, die Sie für IAM

Identity Center konfiguriert haben. Das bedeutet, dass Sie eine Region für den Zugriff auf das IAM Identity Center verwenden, aber Sie können Portale in jeder Region erstellen.

- Wählen Sie IAM, wenn sich Ihre Portalbenutzer mit ihren IAM-Anmeldeinformationen bei diesem Portal anmelden.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.

5. Geben Sie eine E-Mail-Adresse ein, die Portalbenutzer bei Problemen mit dem Portal kontaktieren können, wenn sie Hilfe bei der Fehlerbehebung benötigen.
6. (Optional) Fügen Sie Tags für Ihr Portal hinzu. Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.
7. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie Neue Servicerolle erstellen und verwenden aus. Standardmäßig erstellt SiteWise Monitor automatisch eine Servicerolle für jedes Portal. Diese Rolle ermöglicht Ihren Portalbenutzern den Zugriff auf Ihre AWS IoT SiteWise Ressourcen. Weitere Informationen finden Sie unter Verwenden von Servicerollen für AWS IoT SiteWise Monitor.
   - Wählen Sie Bestehende Servicerolle verwenden und wählen Sie dann die Zielrolle aus.
8. Wählen Sie Weiter
9. (Optional) Aktivieren Sie Alarme für Ihr Portal. Weitere Informationen finden Sie unter Alarme für Ihre Portale aktivieren.
10. Wählen Sie „Erstellen“. AWS IoT SiteWise wird Ihr Portal erstellen.

> **Note**
>
> Wenn Sie die Konsole schließen, können Sie zum Abschluss der Einrichtung Administratoren und Benutzer hinzufügen. Weitere Informationen finden Sie unter Hinzufügen oder Entfernen von Portaladministratoren. Wenn Sie dieses Portal nicht behalten möchten, löschen Sie es, damit es keine Ressourcen verbraucht. Weitere Informationen finden Sie unter Löschen eines Portals.

Die Spalte Status kann einen der folgenden Werte haben.

- AWS IoT SiteWise CREATING - bearbeitet Ihre Anfrage zur Erstellung des Portals. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.
- UPDATE - AWS IoT SiteWise bearbeitet Ihre Anfrage zur Aktualisierung des Portals. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.
- PENDING - AWS IoT SiteWise wartet darauf, dass die Weitergabe des DNS-Eintrags abgeschlossen ist. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen. Sie können das Portal löschen, solange der Status AUSSTEHEND ist.
- LÖSCHEN - AWS IoT SiteWise bearbeitet Ihre Anfrage zum Löschen des Portals. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.
- AKTIV - Wenn das Portal aktiv wird, können Ihre Portalbenutzer darauf zugreifen.
- FEHLGESCHLAGEN - Ihre Anfrage zur Erstellung, Aktualisierung oder Löschung des Portals AWS IoT SiteWise konnte nicht bearbeitet werden. Wenn Sie AWS IoT SiteWise das Senden von Protokollen an Amazon CloudWatch Logs aktiviert haben, können Sie diese Protokolle zur Behebung von Problemen verwenden. Weitere Informationen finden Sie unter Überwachung AWS IoT SiteWise mit CloudWatch Protokollen.

Wenn Ihr Portal erstellt ist, wird eine Meldung angezeigt.

Als Nächstes müssen Sie einen oder mehrere Portaladministratoren zum Portal einladen. Bislang haben Sie nur ein Portal erstellt, es kann noch niemand darauf zugreifen.

Einladen von Administratoren

Um mit dem neuen Portal zu beginnen, müssen Sie einen Portaladministrator zuweisen. Der Portaladministrator erstellt Projekte, wählt Projekteigentümer aus und weist Projekten Komponenten zu. Portaladministratoren können all Ihre AWS IoT SiteWise Ressourcen sehen.

Wählen Sie je nach Benutzerauthentifizierungsdienst eine der folgenden Optionen aus:

IAM Identity Center

Wenn Sie SiteWise Monitor zum ersten Mal verwenden, können Sie den Benutzer, den Sie zuvor erstellt haben, als Portaladministrator auswählen. Wenn Sie einen weiteren Benutzer als Portaladministrator hinzufügen möchten, können Sie auf dieser Seite einen IAM Identity Center-

Benutzer erstellen. Alternativ können Sie einen externen Identitätsanbieter mit IAM Identity Center verbinden. Weitere Informationen finden Sie im AWS IAM Identity Center -Benutzerhandbuch.

So laden Sie Administratoren ein

1. Aktivieren Sie die Kontrollkästchen für die Benutzer, die Ihre Portaladministratoren sein sollen. Dadurch werden die Benutzer zur Liste der Portaladministratoren hinzugefügt.

   > **Note**
   >
   > Wenn Sie IAM Identity Center als Identitätsspeicher verwenden und mit Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie Benutzer erstellen wählen, um einen IAM Identity Center-Benutzer zu erstellen. IAM Identity Center sendet dem neuen Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Anschließend können Sie den Benutzer dem Portal als Administrator zuweisen. Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.

2. (Optional) Wählen Sie Send invite to selected users (Einladung an ausgewählte Benutzer senden) aus. Ihr E-Mail-Client wird geöffnet und der Nachrichtentext wird mit einer Einladung gefüllt.

   Sie können die E-Mail anpassen, bevor Sie sie an die Portaladministratoren senden. Sie können die E-Mail-Nachricht auch später an Ihre Portaladministratoren senden. Wenn Sie SiteWise Monitor zum ersten Mal ausprobieren und Ihren neuen IAM Identity Center- oder IAM-Benutzer oder Ihre neue Rolle als Portaladministrator hinzufügen, müssen Sie sich keine E-Mail senden.
3. Wenn Sie einen Benutzer hinzufügen, der nicht Administrator sein soll, deaktivieren Sie das Kontrollkästchen für den betreffenden Benutzer.
4. Wenn Sie mit dem Einladen von Portaladministratoren fertig sind, wählen Sie Next (Weiter) aus.

IAM

Sie können einen Benutzer oder eine Rolle als Portaladministrator auswählen. Wenn Sie einen weiteren Benutzer oder eine weitere Rolle als Portaladministrator hinzufügen möchten, können Sie einen Benutzer oder eine Rolle in der IAM-Konsole erstellen. Weitere Informationen finden Sie unter Einen IAM-Benutzer in Ihrem AWS Konto erstellen und IAM-Rollen erstellen im IAM-Benutzerhandbuch.

So laden Sie Administratoren ein

1. Gehen Sie wie folgt vor:
   - Wählen Sie IAM-Benutzer aus, um einen IAM-Benutzer als Portaladministrator hinzuzufügen.
   - Wählen Sie IAM-Rollen aus, um eine IAM-Rolle als Portaladministrator hinzuzufügen.
2. Aktivieren Sie die Kontrollkästchen für die Benutzer oder Rollen, die Sie als Portaladministratoren verwenden möchten. Dadurch werden die Benutzer oder Rollen zur Liste der Portaladministratoren hinzugefügt.
3. Wenn Sie einen Benutzer oder eine Rolle hinzufügen, die Sie nicht als Administrator verwenden möchten, deaktivieren Sie das Kontrollkästchen für diesen Benutzer oder diese Rolle.
4. Wenn Sie mit dem Einladen von Portaladministratoren fertig sind, wählen Sie Next (Weiter) aus.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.

> **Note**
>
> Wenn Sie IAM Identity Center als Identitätsspeicher verwenden und bei Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie Benutzer erstellen wählen, um einen IAM Identity Center-Benutzer zu erstellen. IAM Identity Center sendet dem neuen Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Anschließend können Sie den Benutzer dem Portal als Administrator zuweisen. Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.

Sie können die Liste der Portaladministratoren später ändern. Weitere Informationen finden Sie unter Hinzufügen oder Entfernen von Portaladministratoren.

> **Note**
>
> Da nur ein Portaladministrator Projekte erstellen und ihnen Ressourcen zuweisen kann, sollten Sie mindestens einen Portaladministrator angeben.

Als letzten Schritt fügen Sie Benutzer hinzu, die auf Ihr neues Portal zugreifen können.

Hinzufügen von Portalbenutzern

Sie steuern, welche Benutzer Zugriff auf Ihr Portal haben. In jedem Portal erstellen die Portaladministratoren ein oder mehrere Projekte und weisen Portalbenutzer für jedes Projekt als Eigentümer oder Betrachter zu. Jeder Projekteigentümer kann zusätzliche Portalbenutzer als Projekteigentümer oder -betrachter einladen.

Wählen Sie je nach Benutzerauthentifizierungsdienst eine der folgenden Optionen aus:

IAM Identity Center

Wenn Sie der Benutzerliste einen Benutzer hinzufügen möchten, führen Sie die folgenden Schritte aus.

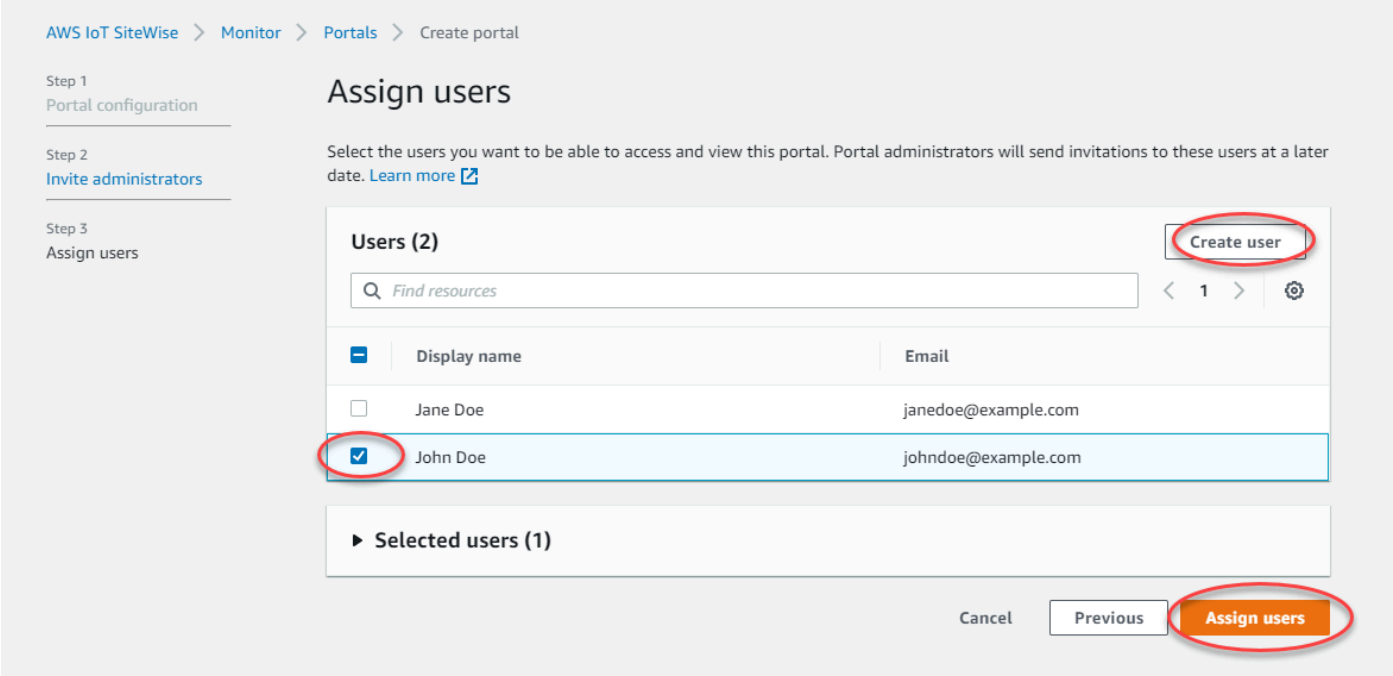
So fügen Sie Portalbenutzer hinzu

1. Wählen Sie Benutzer aus der Benutzerliste aus, die Sie dem Portal hinzufügen möchten. Dadurch werden die Benutzer zur Liste der Portalbenutzer hinzugefügt. Wenn Sie SiteWise Monitor zum ersten Mal verwenden, müssen Sie Ihren Portaladministrator nicht als Portalbenutzer hinzufügen.

   > **Note**
   >
   > Wenn Sie IAM Identity Center als Identitätsspeicher verwenden und bei Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie Benutzer erstellen wählen, um einen IAM Identity Center-Benutzer zu erstellen. IAM Identity Center sendet dem neuen Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Anschließend können Sie den Benutzer dem Portal als Benutzer zuweisen. Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.

2. Wenn Sie einen Benutzer hinzufügen, der keinen Zugriff auf das Portal erhalten soll, deaktivieren Sie das Kontrollkästchen für den betreffenden Benutzer.

3. Wenn Sie mit der Auswahl der Benutzer fertig sind, wählen Sie Benutzer zuweisen.



IAM

Wenn Sie den Benutzer oder die Rolle, die Sie hinzufügen möchten, in der Liste der IAM-Benutzer oder IAM-Rollen sehen, führen Sie die folgenden Schritte aus.

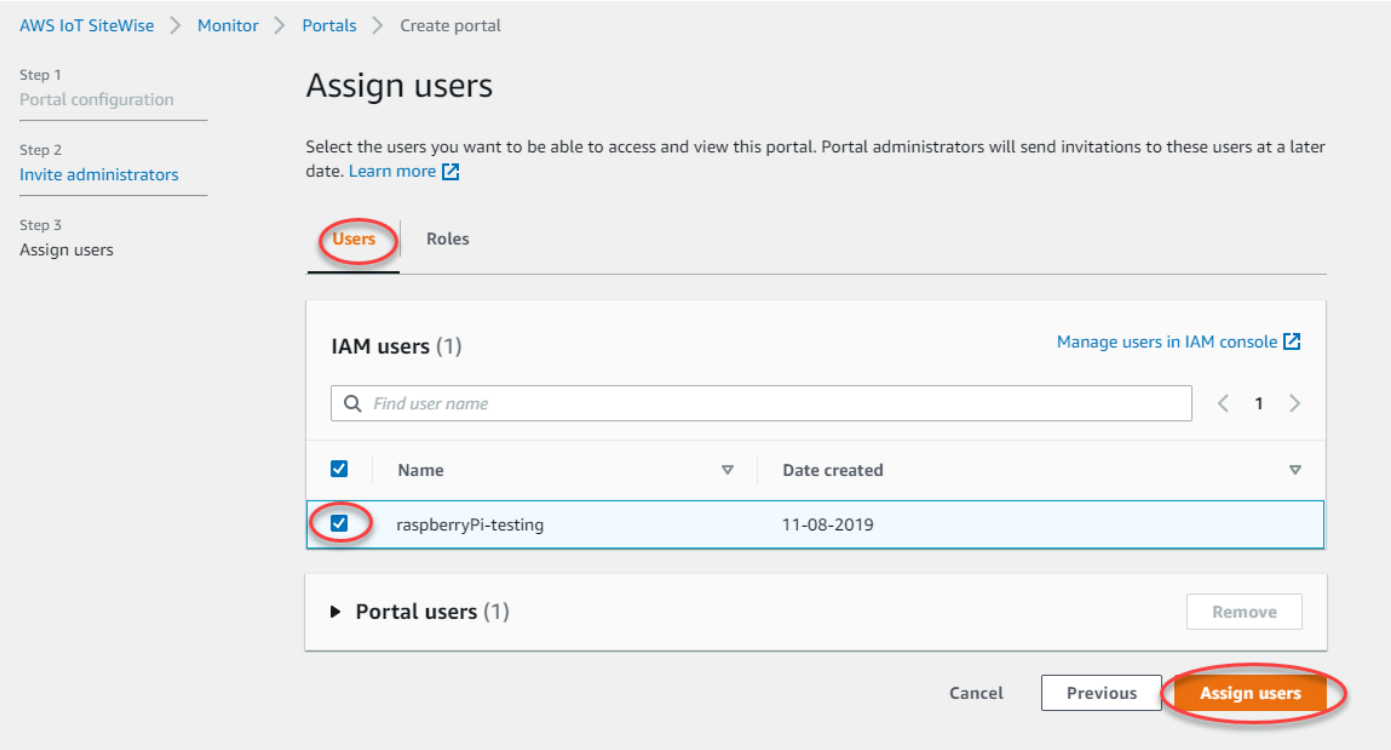
So fügen Sie Portalbenutzer hinzu

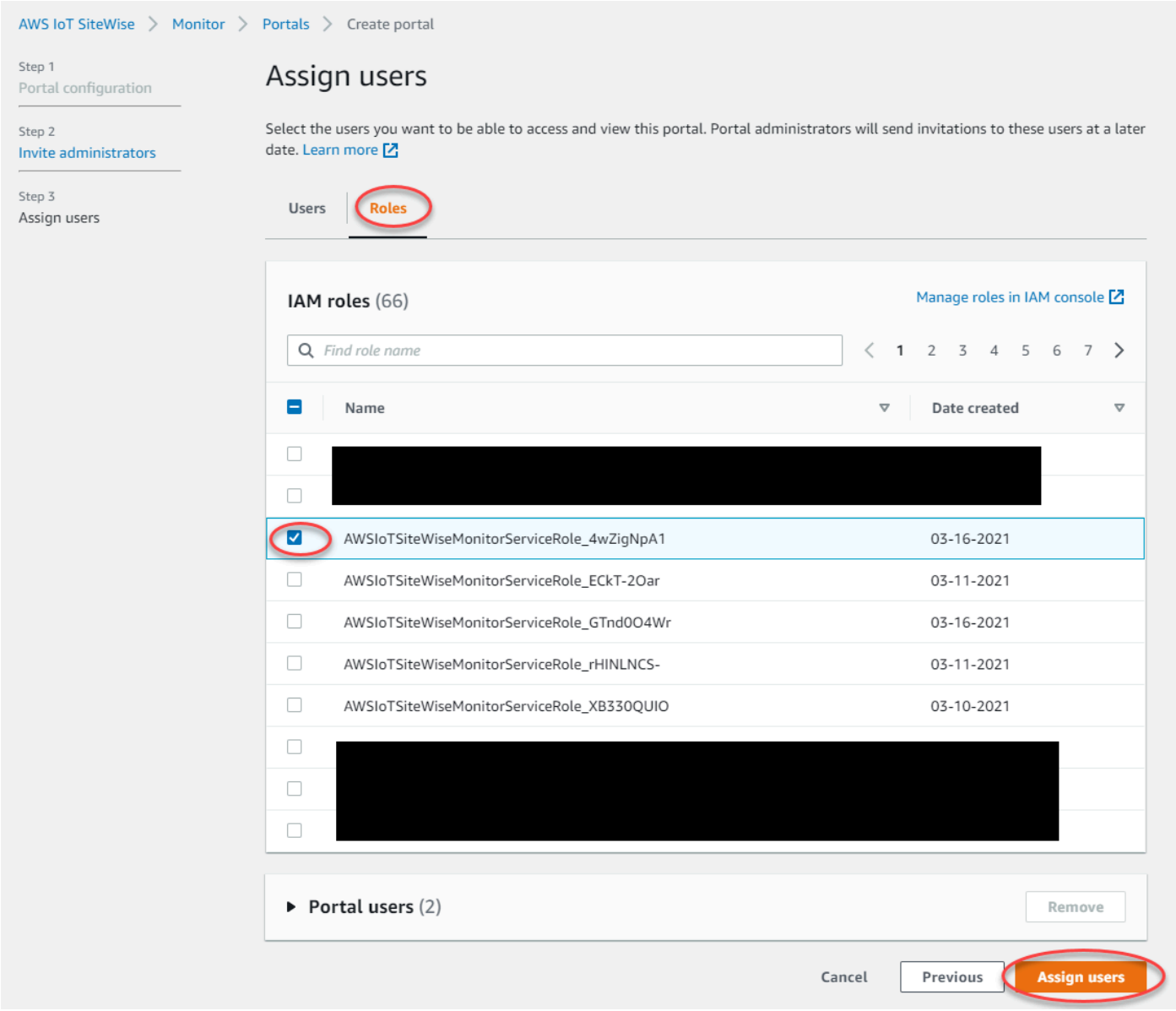
1. Führen Sie die folgenden Optionen aus:

   - Wählen Sie IAM-Benutzer aus, um einen IAM-Benutzer als Portalbenutzer hinzuzufügen.
   - Wählen Sie IAM-Rollen aus, um eine IAM-Rolle als Portalbenutzer hinzuzufügen.

   Wenn Sie SiteWise Monitor zum ersten Mal verwenden, müssen Sie Ihren Portaladministrator nicht als Portalbenutzer hinzufügen.
2. Aktivieren Sie die Kontrollkästchen für die Benutzer oder Rollen, die Sie als Portalbenutzer verwenden möchten. Dadurch werden die Benutzer oder Rollen zur Liste der Portalbenutzer hinzugefügt.
3. Wenn Sie einen Benutzer hinzufügen, der keinen Zugriff auf das Portal erhalten soll, deaktivieren Sie das Kontrollkästchen für den betreffenden Benutzer.
4. Wenn Sie mit der Auswahl der Benutzer fertig sind, wählen Sie Benutzer zuweisen.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.





Herzlichen Glückwunsch! Sie haben erfolgreich ein Portal erstellt, Portaladministratoren zugewiesen und Benutzern zugewiesen, die dieses Portal nutzen können, wenn sie dazu aufgefordert werden. Ihre Portaladministratoren können jetzt Projekte erstellen und diesen Projekten Komponenten zuweisen. Anschließend können Ihre Projekteigentümer Dashboards erstellen, um die Daten für die Komponenten der einzelnen Projekte zu visualisieren.

Sie können die Liste der Portalbenutzer später ändern. Weitere Informationen finden Sie unter Hinzufügen oder Entfernen von Portalbenutzern.

Wenn Sie Änderungen an dem Portal vornehmen müssen, beachten Sie die Informationen unter Verwaltung Ihrer SiteWise Monitor-Portale.

Informationen zu den ersten Schritten im Portal finden Sie unter Erste Schritte im SiteWise Monitor-Anwendungshandbuch.

Erstellen von Dashboards (AWS Command Line Interface)

Wenn Sie Visualisierungen (oder Widgets) in Dashboards über die AWS CLI definieren, müssen Sie im `dashboardDefinition`-JSON-Dokument die folgenden Informationen angeben. Diese Definition ist ein Parameter der UpdateDashboard Operationen CreateDashboard und .

`widgets`

Eine Liste von Widget-Definitionsstrukturen, die jeweils die folgenden Informationen enthalten:

`type`

Der Typ des Widgets. AWS IoT SiteWise stellt die folgenden Widget-Typen bereit:

- `sc-line-chart` – Ein Liniendiagramm. Weitere Informationen finden Sie unter Liniendiagramme im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-scatter-chart` – Ein Streudiagramm. Weitere Informationen finden Sie unter Musterdiagramme im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-bar-chart` – Ein Balkendiagramm. Weitere Informationen finden Sie unter Balkendiagramme im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-status-grid` – Ein Status-Widget, das den neuesten Wert von Komponenteneigenschaften als Raster anzeigt. Weitere Informationen finden Sie unter Status-Widgets im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-status-timeline` – Ein Status-Widget, das die historischen Werte von Komponenteneigenschaften als Zeitleiste anzeigt. Weitere Informationen finden Sie unter Status-Widgets im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-kpi` – Eine Key Performance Indikator (KPI)-Visualisierung. Weitere Informationen finden Sie unter KPI-Widgets im AWS IoT SiteWise Monitor Anwendungshandbuch für .
- `sc-table` – Ein Tabellen-Widget. Weitere Informationen finden Sie unter Tabellen-Widgets im AWS IoT SiteWise Monitor Anwendungshandbuch für .

`title`

Der Titel des Widgets.

`x`

Die horizontale Position des Widgets ausgehend von der linken Seite des Rasters. Dieser Wert bezieht sich auf die Position des Widgets im Raster des Dashboards.

`y`

Die vertikale Position des Widgets ausgehend vom oberen Rand des Rasters. Dieser Wert bezieht sich auf die Position des Widgets im Raster des Dashboards.

`width`

Die Breite des Widgets ausgedrückt als Anzahl der Leerzeichen im Raster des Dashboards.

`height`

Die Höhe des Widgets ausgedrückt als Anzahl der Leerzeichen im Raster des Dashboards.

`metrics`

Eine Liste von Metrikstrukturen, die jeweils einen Datenstrom für dieses Widget definieren. Jede Struktur in der Liste muss folgende Informationen enthalten:

`label`

Eine Beschriftung, die für diese Metrik angezeigt werden soll.

`type`

Der Typ der Datenquelle für diese Metrik. AWS IoT SiteWise stellt die folgenden Metriktypen bereit:

- `iotsitewise` – Das Dashboard ruft Daten für eine Komponenteneigenschaft in abAWS IoT SiteWise. Bei Auswahl dieser Option müssen Sie `assetId` und `propertyId` für diese Metrik definieren.

`assetId`

(Optional) Die ID einer Komponente in AWS IoT SiteWise.

Dieses Feld ist erforderlich, wenn Sie `iotsitewise` für `type` in dieser Metrik auswählen.

`propertyId`

(Optional) Die ID einer Komponenteneigenschaft in AWS IoT SiteWise.

Dieses Feld ist erforderlich, wenn Sie `iotsitewise` für `type` in dieser Metrik auswählen.

`analysis`

(Optional) Eine Struktur, die die Analyse definiert, z. B. Trendlinien, die für das Widget angezeigt werden soll. Weitere Informationen finden Sie unter Konfigurieren von Trendlinien im AWS IoT SiteWise Monitor Anwendungshandbuch für . Sie können eine jeden Typ von Trendlinie pro Eigenschaft im Widget hinzufügen. Die Analysestruktur enthält die folgenden Informationen:

`trends`

(Optional) Eine Liste von Trendstrukturen, die jeweils eine Trendanalyse für dieses Widget definieren. Jede Struktur in der Liste enthält die folgenden Informationen:

`type`

Der Typ der Trendlinie. Wählen Sie die folgende Option aus:

- `linear-regression` – Zeigen Sie eine lineare Regressionslinie an. SiteWise Monitor verwendet die Methode mit den geringsten Quadraten, um die lineare Regression zu berechnen.

`annotations`

(Optional) Eine Anmerkungsstruktur, die Schwellenwerte für das Widget definiert. Weitere Informationen finden Sie unter Konfigurieren von Schwellenwerten im AWS IoT SiteWise Monitor -Anwendungshandbuch. Sie können bis zu sechs Anmerkungen pro Widget hinzufügen. Die Annotationsstruktur enthält die folgenden Informationen:

`y`

(Optional) Eine Liste von Anmerkungsstrukturen, die jeweils einen horizontalen Schwellenwert für dieses Widget definieren. Jede Struktur in der Liste enthält die folgenden Informationen:

`comparisonOperator`

Der Vergleichsoperator für den Schwellenwert. Wählen Sie eine der folgenden Optionen aus:

- `LT` – Markieren Sie Eigenschaften, die mindestens einen Datenpunkt haben, der kleiner ist als `value`.
- `GT` – Markieren Sie Eigenschaften, die mindestens einen Datenpunkt größer als haben`value`.

- `LTE` – Markieren Sie Eigenschaften, die mindestens einen Datenpunkt haben, der kleiner oder gleich dem ist`value`.
- `GTE` – Markieren Sie Eigenschaften, die mindestens einen Datenpunkt haben, der größer oder gleich der ist`value`.
- `EQ` – Markieren Sie Eigenschaften, die mindestens einen Datenpunkt haben, der gleich ist`value`.

`value`

Der Schwellenwert für den Vergleich von Datenpunkten mit dem `comparisonOperator`.

`color`

(Optional) Der sechsstellige Hexadezimalcode der Schwellenwertfarbe. Die Visualisierung zeigt Eigenschaftslegenden in dieser Farbe für Eigenschaften mit mindestens einem Datenpunkt an, der die Schwellenwertregel erfüllt. Standardmäßig schwarz (`#000000`).

`showValue`

(Optional) Gibt an, ob der Wert des Schwellenwerts in den Rändern des Widgets angezeigt werden soll oder nicht. Standardeinstellung: `true`.

`properties`

(Optional) Ein flaches Wörterbuch mit Eigenschaften für das Widget. Die Mitglieder dieser Struktur sind kontextabhängig. AWS IoT SiteWise bietet die folgenden Widgets, die verwenden`properties`:

- Liniendiagramme , Streudiagramme und Balkendiagramme haben die folgende Eigenschaft:

  `colorDataAcrossThresholds`

  (Optional) Gibt an, ob die Farbe der Daten geändert werden soll, die die Schwellenwerte in diesem Widget überschreiten. Wenn Sie diese Option aktivieren, werden die Daten, die einen Schwellenwert überschreiten, in der von Ihnen ausgewählten Farbe angezeigt. Standardeinstellung: `true`.

- Statusraster haben die folgende Eigenschaft:

  `labels`

  (Optional) Eine Struktur, die die Beschriftungen definiert, die im Statusraster angezeigt werden sollen. Die Beschriftungsstruktur enthält die folgenden Informationen:

`showValue`

(Optional) Gibt an, ob die Einheit und der Wert für jede Komponenteneigenschaft in diesem Widget angezeigt werden sollen oder nicht. Standardeinstellung: `true`.

Example Dashboard-Beispieldefinition

Im folgenden Beispiel wird ein Dashboard aus einer Nutzlast definiert, die in einer JSON-Datei gespeichert ist.

```
aws iotsitewise create-dashboard \
  --project-id a1b2c3d4-5678-90ab-cdef-eeeeeEXAMPLE \
  --dashboard-name "Wind Farm Dashboard" \
  --dashboard-definition file://dashboard-definition.json
```

Das folgende JSON-Beispiel für `dashboard-definition.json` definiert ein Dashboard mit den folgenden Visualisierungs-Widgets:

- Ein Liniendiagramm, das die Gesamtleistung des Windparks oben links im Dashboards visualisiert. Dieses Liniendiagramm enthält einen Schwellenwert, der angibt, wann die Stromfarm weniger Strom ausgibt als seine minimal erwartete Ausgabe. Dieses Liniendiagramm enthält auch eine lineare Regressionstrendlinie.
- Ein Balkendiagramm, das die Windgeschwindigkeit für vier Turbinen oben rechts im Dashboard visualisiert.

> **Note**
>
> Dieses Beispiel stellt Linien- und Balkendiagrammvisualisierungen auf einem Dashboard dar. Dieses Dashboard ist dem Beispiel-Dashboard für einen Windpark ähnlich.

```
{
  "widgets": [
    {
      "type": "sc-line-chart",
      "title": "Total Average Power",
      "x": 0,
      "y": 0,
```

```
      "height": 3,
      "width": 3,
      "metrics": [
        {
          "label": "Power",
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
          "analysis": {
            "trends": [
              {
                "type": "linear-regression"
              }
            ]
          }
        }
      ],
      "annotations": {
        "y": [
          {
            "comparisonOperator": "LT",
            "value": 20000,
            "color": "#D13212",
            "showValue": true
          }
        ]
      }
    },
    {
      "type": "sc-bar-chart",
      "title": "Wind Speed",
      "x": 3,
      "y": 3,
      "height": 3,
      "width": 3,
      "metrics": [
        {
          "label": "Turbine 1",
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-2a2a2EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
        },
        {
          "label": "Turbine 2",
```

```
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-2b2b2EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
        },
        {
          "label": "Turbine 3",
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-2c2c2EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
        },
        {
          "label": "Turbine 4",
          "type": "iotsitewise",
          "assetId": "a1b2c3d4-5678-90ab-cdef-2d2d2EXAMPLE",
          "propertyId": "a1b2c3d4-5678-90ab-cdef-55555EXAMPLE"
        }
      ]
    }
  ]
}
```

Alarme für Ihre Portale aktivieren

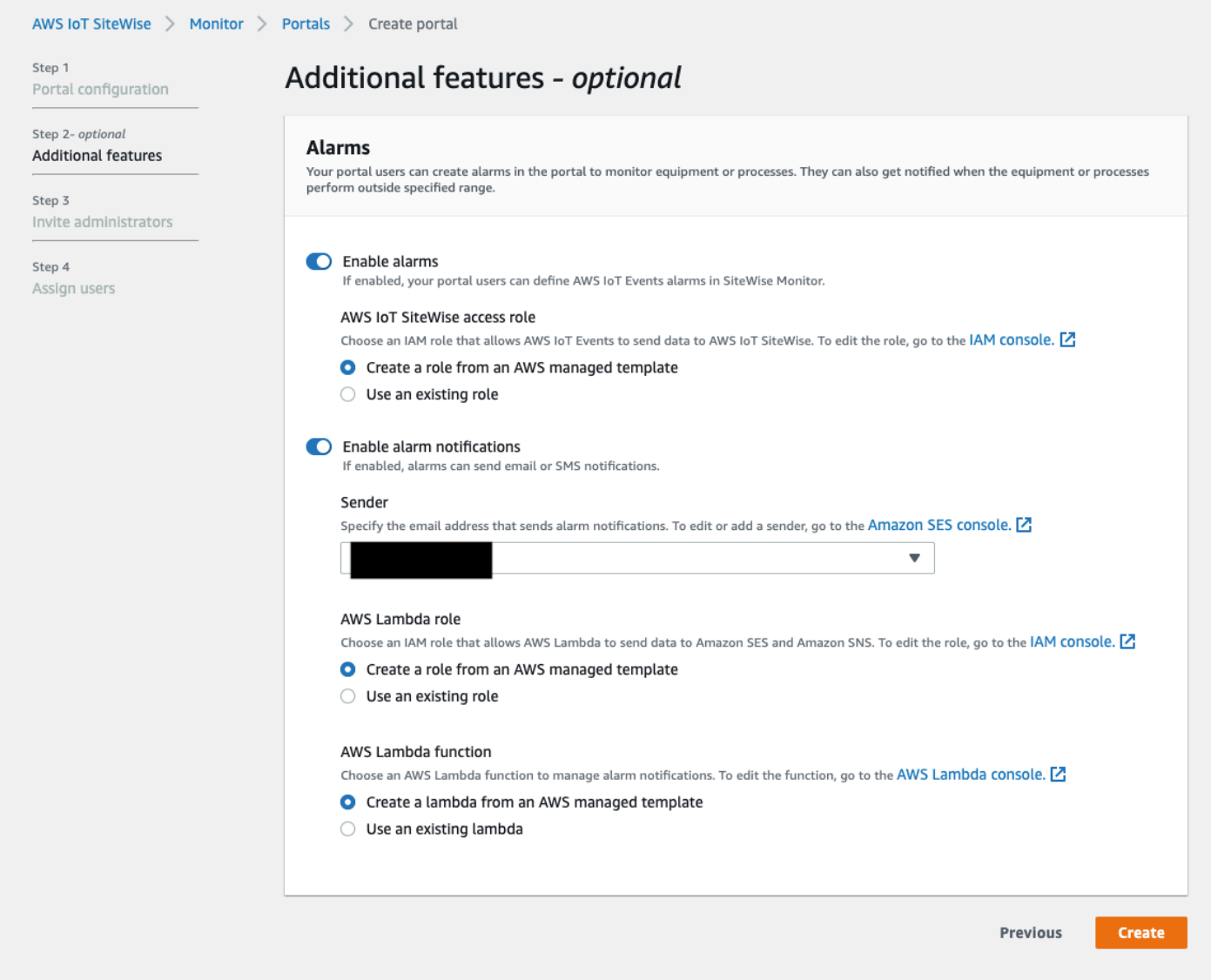
Sie können die von unterstützte Alarmfunktion AWS IoT Events für Ihre Portale aktivieren, sodass Portaladministratoren AWS IoT Events Alarmmodelle in Ihren SiteWise Monitor-Portalen erstellen, bearbeiten und löschen können. Projekteigentümer können Alarme konfigurieren. Projektbetrachter können Alarmdetails einsehen. In diesem Abschnitt wird erklärt, wie Sie die AWS IoT SiteWise Konsole verwenden können, um die Alarmfunktion für Ihre Portale zu aktivieren.

Important

- Sie können in Ihren Portalen keine externen Alarme erstellen.
- Wenn Sie Alarmbenachrichtigungen senden möchten, müssen Sie IAM Identity Center für den Benutzerauthentifizierungsdienst auswählen.
- Die Funktion für Alarmbenachrichtigungen ist in China (Peking) AWS-Region nicht verfügbar.

Wenn Sie ein Portal konfigurieren und erstellen, können Sie Alarme und Alarmbenachrichtigungen in Schritt 2 Zusätzliche Funktionen aktivieren. Wählen Sie je nach Benutzerauthentifizierungsdienst eine der folgenden Optionen aus:

IAM Identity Center



Um Alarme für ein Portal zu aktivieren

1. (Optional) Wählen Sie Alarme aktivieren.

    - Verwenden Sie für die AWS IoT SiteWise Zugriffsrolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Diese Rolle erfordert die `iotevents:BatchPutMessage` Erlaubnis und eine Vertrauensbeziehung, die es

ermöglicht `iot.amazonaws.com` und `iotevents.amazonaws.com` die Übernahme der Rolle ermöglicht.

2. (Optional) Wählen Sie Alarmbenachrichtigungen aktivieren.

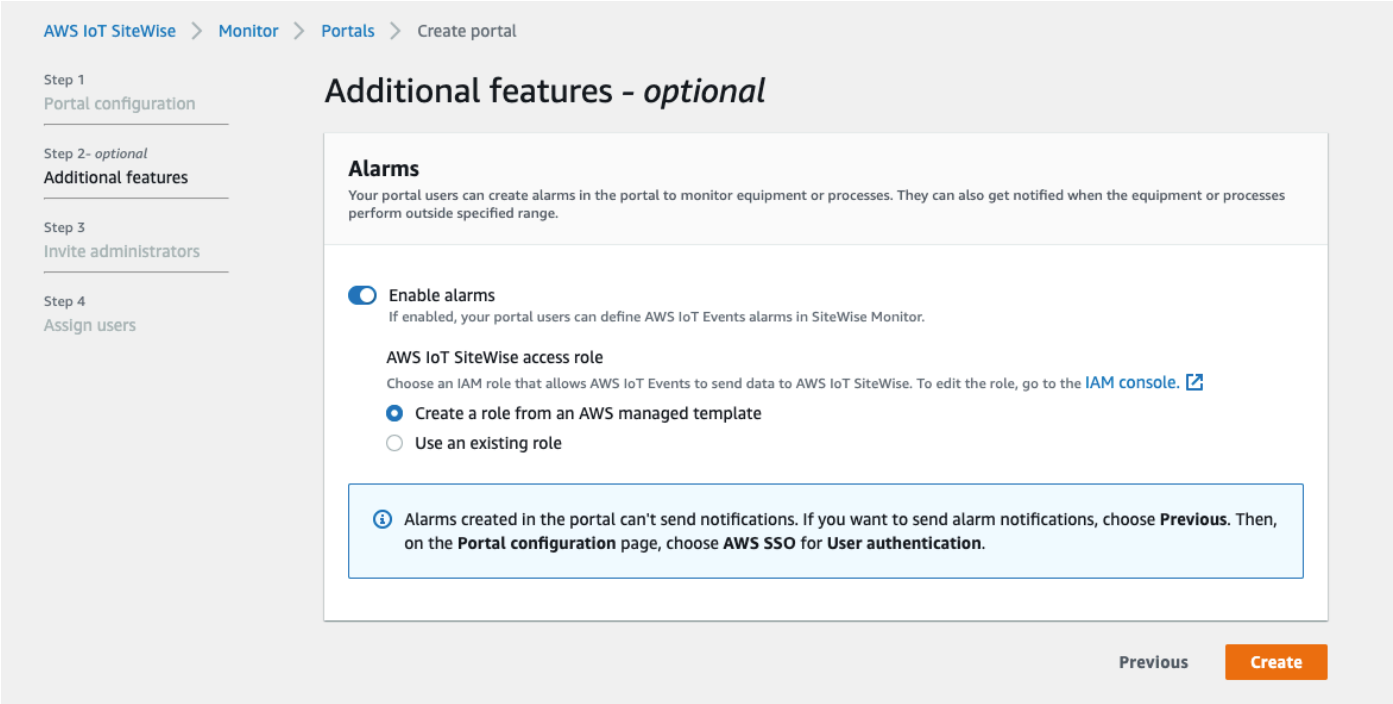
   a. Wählen Sie unter Absender den Absender aus.

   > **Important**
   >
   > Sie müssen die Absender-E-Mail-Adresse in Amazon SES verifizieren. Weitere Informationen finden Sie unter Verifizieren von E-Mail-Adressen in Amazon SES im Amazon Simple Email Service Developer Guide.

   b. Verwenden Sie für die AWS Lambda Rolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Für diese Rolle sind die `sso-directory:DescribeUser` Berechtigungen `lambda:InvokeFunction` und eine Vertrauensbeziehung erforderlich, die es ermöglicht `iotevents.amazonaws.com` und `lambda.amazonaws.com` die Übernahme der Rolle ermöglicht.

   c. Wählen Sie für AWS Lambda Funktionen eine vorhandene Lambda-Funktion aus oder erstellen Sie eine Funktion, die Alarmbenachrichtigungen verwaltet. Weitere Informationen finden Sie unter Verwaltung von Alarmbenachrichtigungen im AWS IoT Events Entwicklerhandbuch.

IAM



Um Alarme für ein Portal zu aktivieren

- (Optional) Wählen Sie Alarme aktivieren.
  - Verwenden Sie für die AWS IoT SiteWise Zugriffsrolle eine vorhandene Rolle oder erstellen Sie eine Rolle mit den erforderlichen Berechtigungen. Diese Rolle erfordert die `iotevents:BatchPutMessage` Erlaubnis und eine Vertrauensbeziehung, die es ermöglicht `iot.amazonaws.com` und `iotevents.amazonaws.com` die Übernahme der Rolle ermöglicht.

Weitere Informationen zu Alarmen in SiteWise Monitor finden Sie unter Überwachung mit Alarmen im AWS IoT SiteWise Anwendungshandbuch.

Aktivierung Ihres Portals am Edge

Nachdem Sie Ihr Portal am Edge aktiviert haben, ist dieses Portal auf allen SiteWise Edge-Gateways verfügbar, für die das Datenverarbeitungspaket in Ihrem Konto aktiviert ist.

Um das Portal am Edge zu aktivieren

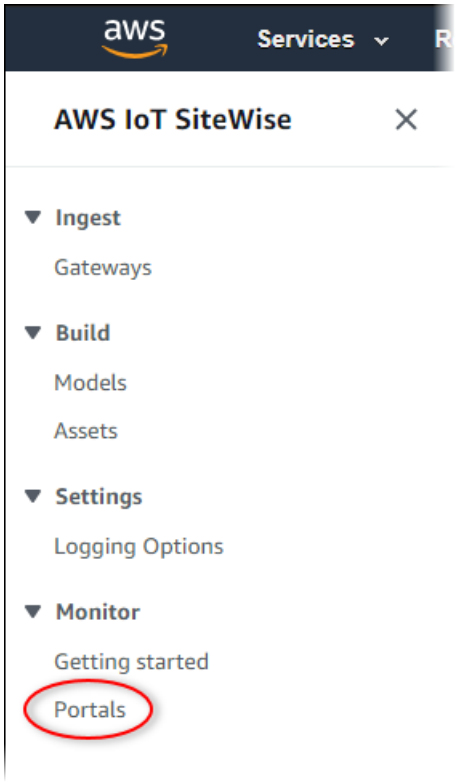
1. Aktivieren Sie im Abschnitt Edge-Konfiguration die Option Dieses Portal am Edge aktivieren.

2. Wählen Sie Create (Erstellen) aus.

Verwaltung Ihrer SiteWise Monitor-Portale

Möglicherweise müssen Sie Portaldetails aktualisieren, Administratoren ändern oder Benutzer zu Ihren Portalen hinzufügen. In diesem Abschnitt wird erklärt, wie Sie diese grundlegenden Verwaltungsaufgaben für Ihre SiteWise Monitor-Portale erledigen können.

1. Melden Sie sich an der AWS IoT SiteWise -Konsole an.
2. Wählen Sie im Navigationsbereich Monitor (Überwachen), Portals (Portale) aus.



3. Wählen Sie das Portal und dann View details (Details anzeigen) aus (oder wählen Sie den Namen des Portals aus).
4. Sie können eine der folgenden Verwaltungsaufgaben ausführen:

   - Änderung des Namens, der Beschreibung, des Brandings, der Support-E-Mail-Adresse und der Berechtigungen eines Portals
   - Hinzufügen oder Entfernen von Portaladministratoren
   - Senden von Einladungs-E-Mails an Portaladministratoren
   - Hinzufügen oder Entfernen von Portalbenutzern

- Löschen eines Portals

Weitere Informationen zum Erstellen eines Portals finden Sie unter Erste Schritte mit AWS IoT SiteWise Monitor.

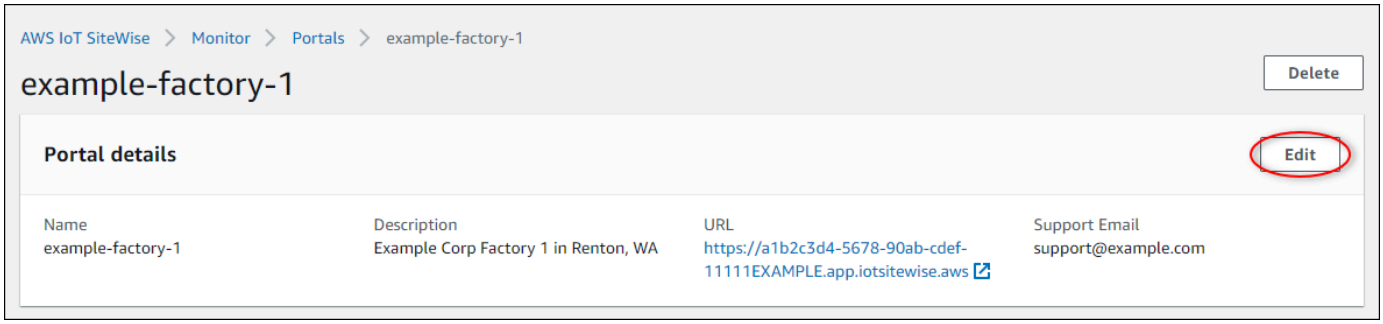
Themen

- Änderung des Namens, der Beschreibung, des Brandings, der Support-E-Mail-Adresse und der Berechtigungen eines Portals
- Hinzufügen oder Entfernen von Portaladministratoren
- Senden von Einladungs-E-Mails an Portaladministratoren
- Hinzufügen oder Entfernen von Portalbenutzern
- Löschen eines Portals

Änderung des Namens, der Beschreibung, des Brandings, der Support-E-Mail-Adresse und der Berechtigungen eines Portals

Sie können den Namen, die Beschreibung, das Branding, die Support-E-Mail-Adresse und die Berechtigungen eines Portals ändern.

1. Wählen Sie auf der Seite mit den Portaldetails im Abschnitt Portal details (Portaldetails) die Option Edit (Bearbeiten) aus.

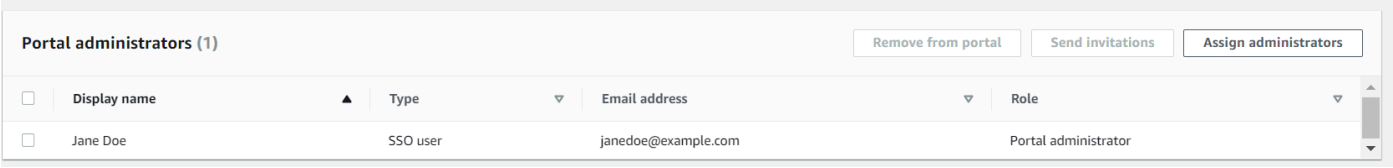


2. Aktualisieren Sie Name, Description (Beschreibung), Portal Branding, Support contact email (E-Mail-Adresse des Support-Kontakts) oder Permissions (Berechtigungen).
3. Wenn Sie fertig sind, wählen Sie Speichern.

Hinzufügen oder Entfernen von Portaladministratoren

Sie können mit wenigen Schritten Benutzer als Administratoren für ein Portal hinzufügen oder entfernen. Wählen Sie je nach Benutzerauthentifizierungsdienst eine der folgenden Optionen aus.

IAM Identity Center

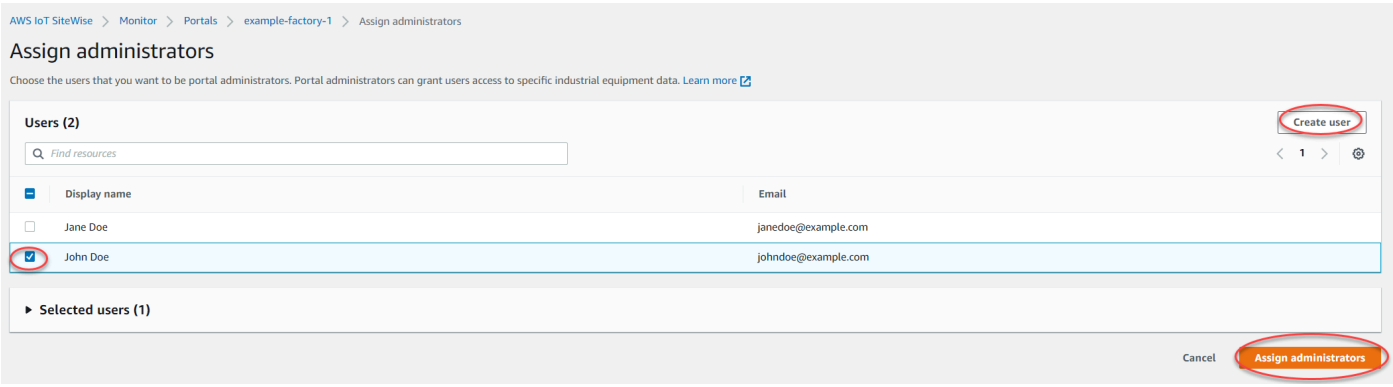


So fügen Sie Portaladministratoren hinzu

1. Wählen Sie auf der Seite mit den Portaldetails im Abschnitt Portaladministratoren die Option Administratoren zuweisen aus.
2. Aktivieren Sie auf der Seite Administratoren zuweisen die Kontrollkästchen für die Benutzer, die dem Portal als Administratoren hinzugefügt werden sollen.

> **Note**
>
> Wenn Sie IAM Identity Center als Identitätsspeicher verwenden und bei Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie Benutzer erstellen wählen, um einen IAM Identity Center-Benutzer zu erstellen. IAM Identity Center sendet dem neuen Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Anschließend können Sie den Benutzer dem Portal als Administrator zuweisen. Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.

3. Wählen Sie Administratoren zuweisen.

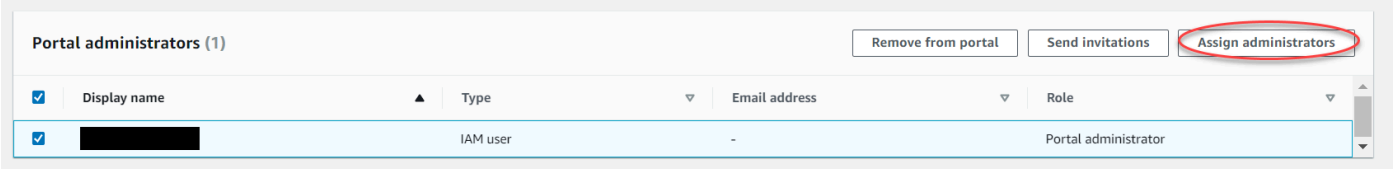


So entfernen Sie Portaladministratoren

- Aktivieren Sie auf der Seite „Portal details (Portaldetails)“ im Abschnitt Portal administrators (Portaladministratoren) das Kontrollkästchen für jeden zu entfernenden Benutzer und wählen Sie dann Remove from portal (Aus Portal entfernen) aus.

> **Note**
>
> Wir empfehlen, dass Sie mindestens einen Portaladministrator auswählen.

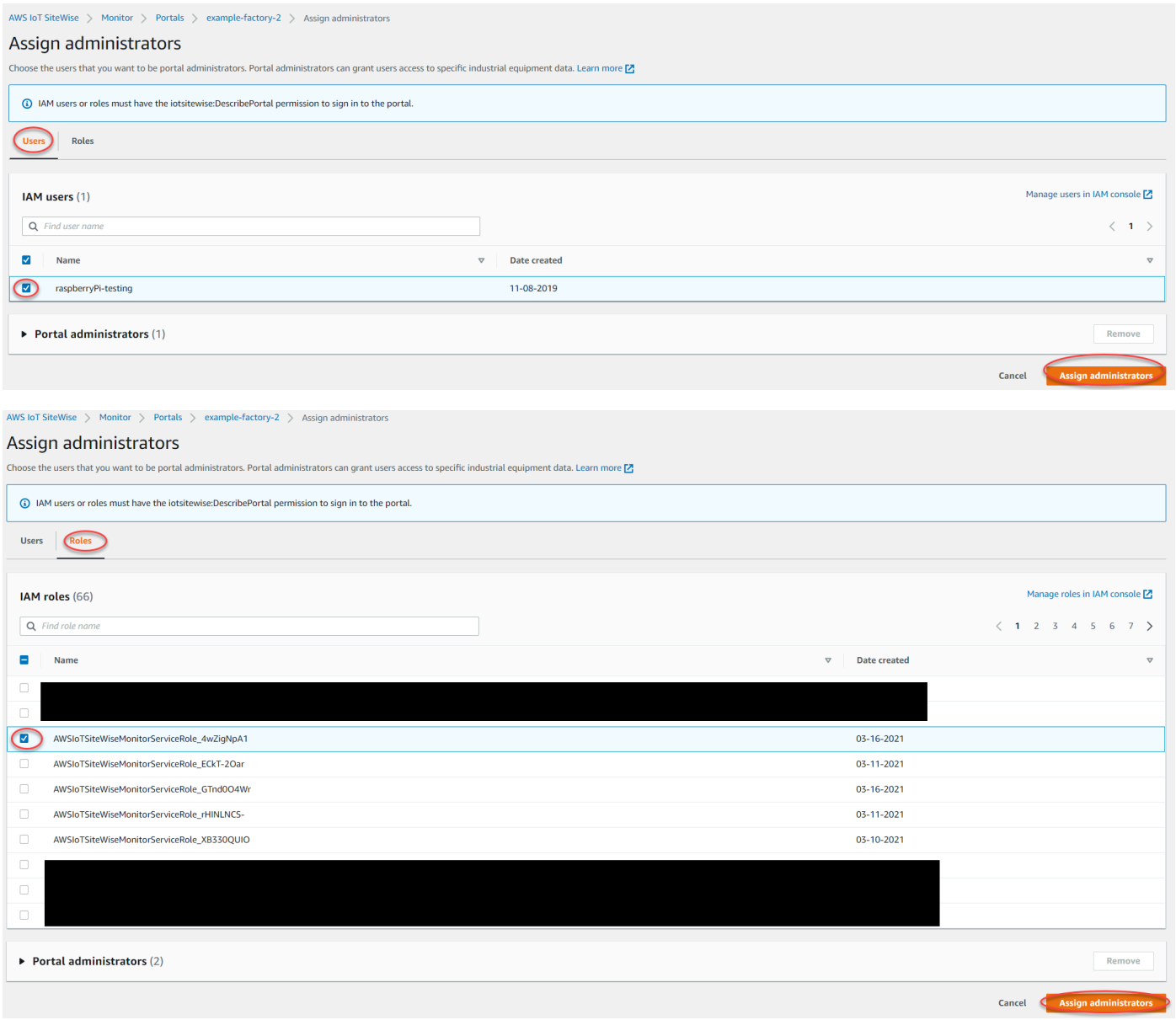
IAM



So fügen Sie Portaladministratoren hinzu

1. Wählen Sie auf der Seite mit den Portaldetails im Abschnitt Portaladministratoren die Option Administratoren zuweisen aus.
2. Gehen Sie auf der Seite Administratoren zuweisen wie folgt vor:
   - Wählen Sie IAM-Benutzer, wenn Sie einen IAM-Benutzer als Portaladministrator hinzufügen möchten.
   - Wählen Sie IAM-Rollen, wenn Sie eine IAM-Rolle als Portaladministrator hinzufügen möchten.
3. Aktivieren Sie die Kontrollkästchen für die Benutzer oder Rollen, die Sie als Portaladministratoren verwenden möchten. Dadurch werden die Benutzer oder Rollen zur Liste der Portaladministratoren hinzugefügt.
4. Wählen Sie Administratoren zuweisen aus.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.



So entfernen Sie Portaladministratoren

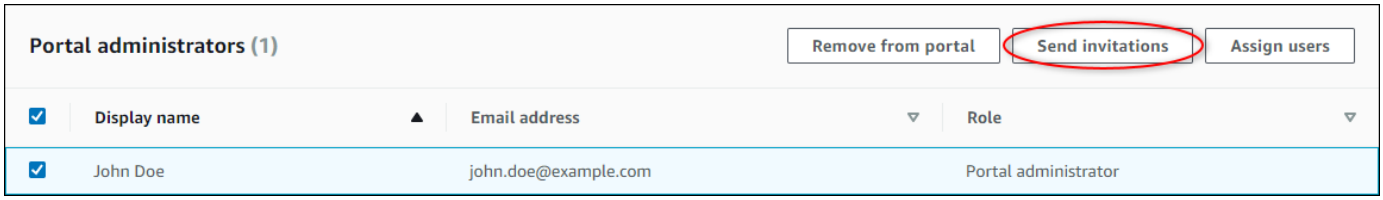
- Aktivieren Sie auf der Seite „Portal details (Portaldetails)“ im Abschnitt Portal administrators (Portaladministratoren) das Kontrollkästchen für jeden zu entfernenden Benutzer und wählen Sie dann Remove from portal (Aus Portal entfernen) aus.

> **Note**
>
> Es empfiehlt sich nicht, ein Portal ohne Portaladministrator zu belassen.

Senden von Einladungs-E-Mails an Portaladministratoren

Sie können E-Mail-Einladungen an Portaladministratoren senden.

1. Aktivieren Sie auf der Seite mit den Portaldetails im Abschnitt Portal administrators (Portaladministratoren) die Kontrollkästchen für die Portaladministratoren.



2. Wählen Sie Send invitations (Einladungen senden) aus. Ihr E-Mail-Client wird geöffnet und der Nachrichtentext wird mit einer Einladung gefüllt.

   Sie können die E-Mail anpassen, bevor Sie sie an die Portaladministratoren senden.

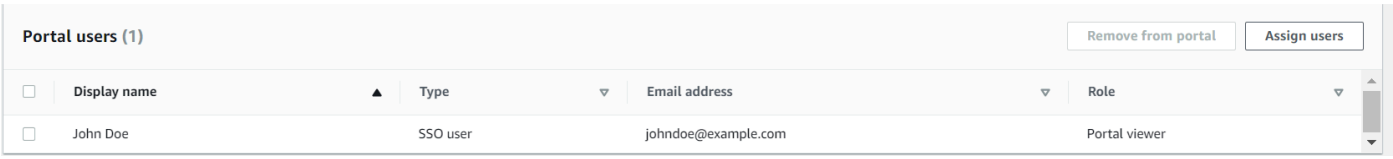
Hinzufügen oder Entfernen von Portalbenutzern

Sie wählen, welche Benutzer Zugriff auf Ihr Portal haben. Portalbenutzer werden in der Benutzerliste in einem SiteWise Monitor-Portal angezeigt. Aus dieser Liste können Portaladministratoren Projektbesitzer hinzufügen, und Projektbesitzer können Projektbetrachter hinzufügen.

> **Note**
>
> Ihre Portaladministratoren und Portalbenutzer wenden sich möglicherweise über die Support-E-Mail eines Portals an Sie, wenn Sie einen Benutzer hinzufügen oder entfernen müssen.

Wählen Sie je nach Benutzerauthentifizierungsdienst eine der folgenden Optionen aus.

IAM Identity Center

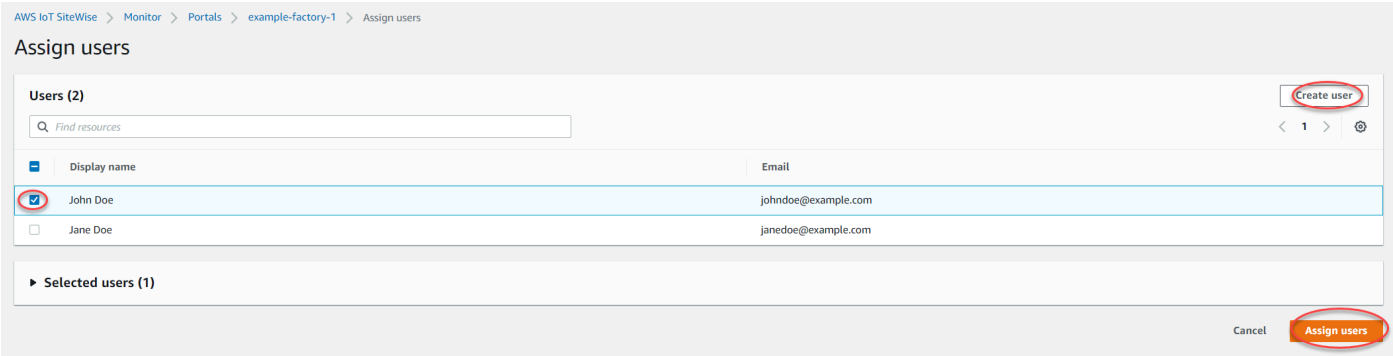


So fügen Sie Portalbenutzer hinzu

1. Wählen Sie auf der Seite „Portal details (Portaldetails)“ im Abschnitt Portal users (Portalbenutzer) die Option Assign users (Benutzer zuweisen) aus.
2. Aktivieren Sie auf der Seite Benutzer zuweisen das Kontrollkästchen für die Benutzer, die dem Portal hinzugefügt werden sollen.

> **Note**
>
> Wenn Sie IAM Identity Center als Identitätsspeicher verwenden und bei Ihrem AWS Organizations Verwaltungskonto angemeldet sind, können Sie Benutzer erstellen auswählen, um einen IAM Identity Center-Benutzer zu erstellen. IAM Identity Center sendet dem neuen Benutzer eine E-Mail, damit er sein Passwort einrichten kann. Anschließend können Sie den Benutzer dem Portal als Benutzer zuweisen. Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.

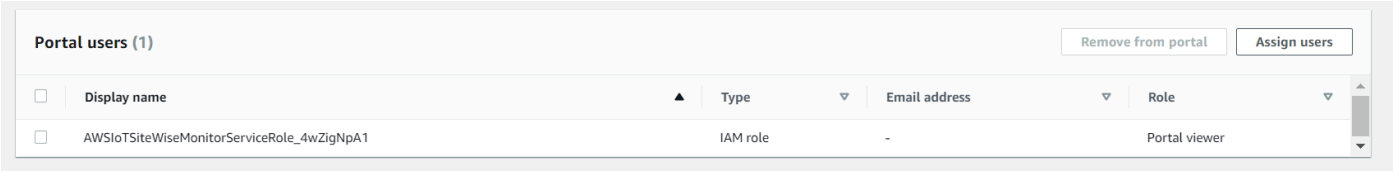
3. Wählen Sie Assign users (Benutzer zuweisen) aus.



So entfernen Sie Portalbenutzer

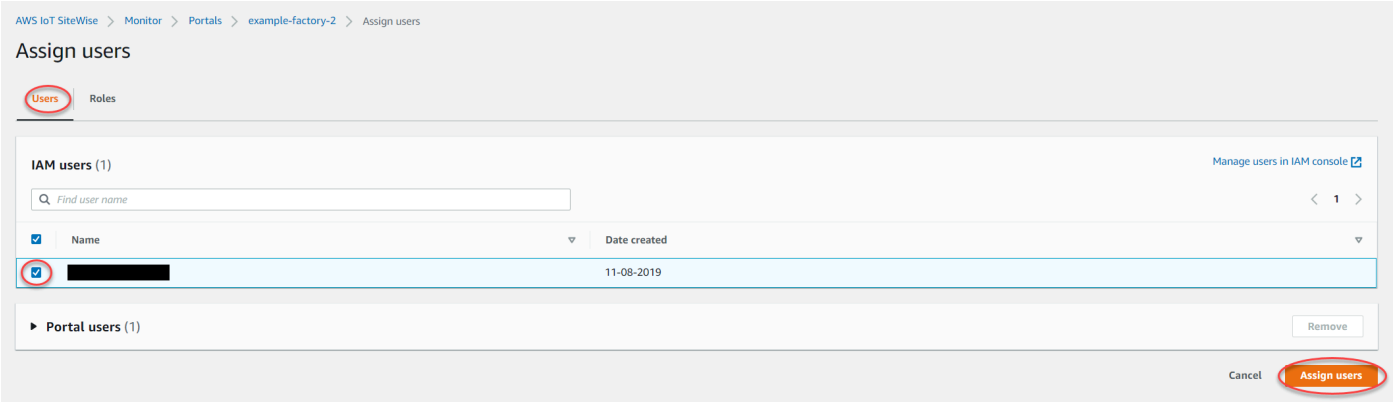
- Aktivieren Sie auf der Seite mit den Portaldetails im Abschnitt Portalbenutzer das Kontrollkästchen für die Benutzer, die aus dem Portal entfernt werden sollen, und wählen Sie dann Aus Portal entfernen aus.

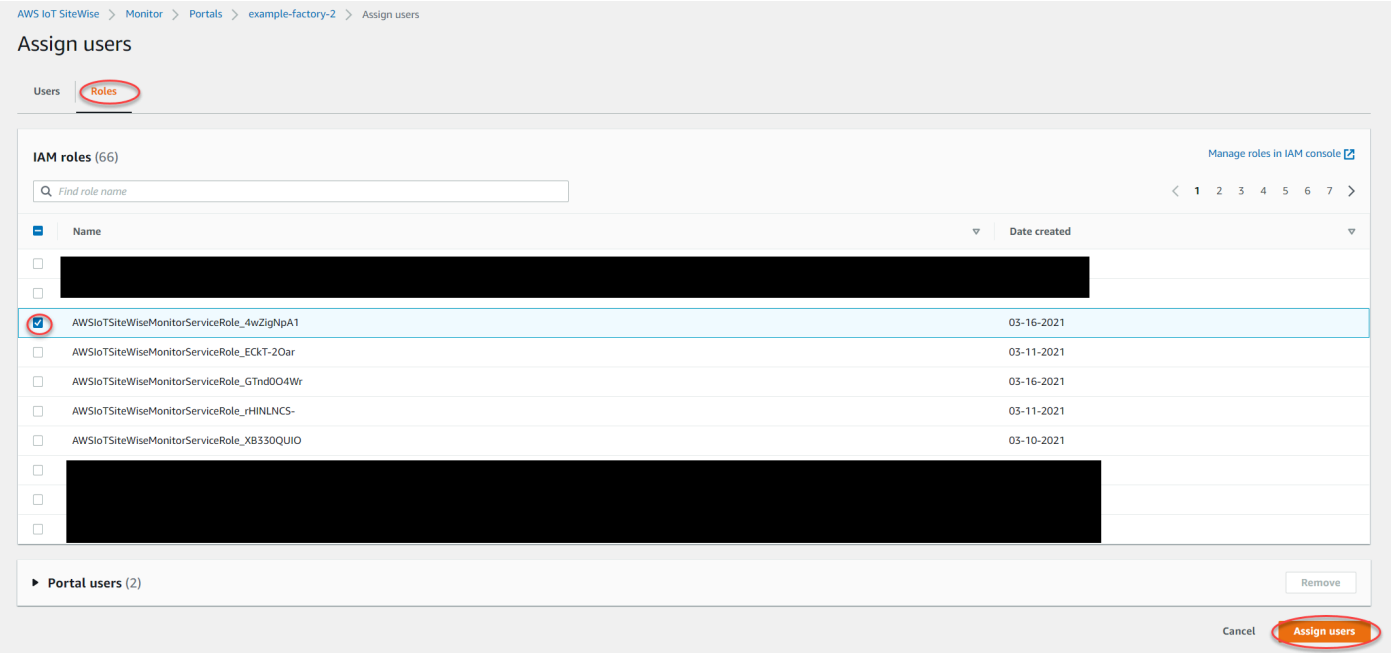
IAM



So fügen Sie Portalbenutzer hinzu

1. Wählen Sie auf der Seite „Portal details (Portaldetails)“ im Abschnitt Portal users (Portalbenutzer) die Option Assign users (Benutzer zuweisen) aus.
2. Gehen Sie auf der Seite Benutzer zuweisen wie folgt vor:
   - Wählen Sie IAM-Benutzer aus, um einen IAM-Benutzer als Ihren Portalbenutzer hinzuzufügen.
   - Wählen Sie IAM-Rollen aus, um eine IAM-Rolle als Portalbenutzer hinzuzufügen.
3. Aktivieren Sie die Kontrollkästchen für die Benutzer oder Rollen, die Sie als Portalbenutzer hinzufügen möchten. Dadurch werden die Benutzer oder Rollen zur Liste der Portalbenutzer hinzugefügt.
4. Wählen Sie Assign users (Benutzer zuweisen) aus.





So entfernen Sie Portalbenutzer

- Aktivieren Sie auf der Seite mit den Portaldetails im Abschnitt Portalbenutzer das Kontrollkästchen für die Benutzer, die aus dem Portal entfernt werden sollen, und wählen Sie dann Aus Portal entfernen aus.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.

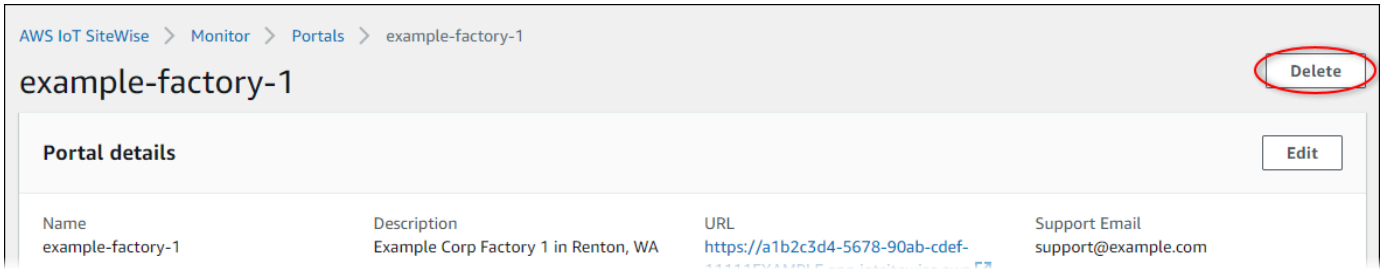
Löschen eines Portals

Sie können ein Portal löschen, wenn Sie es zu Testzwecken erstellt haben, oder wenn Sie ein Duplikat eines bereits erstellten Portals erstellt haben.

> **Note**
>
> Bevor Sie das Portal löschen können, müssen Sie zunächst alle Dashboards und Projekte in dem Portal manuell löschen. Weitere Informationen finden Sie unter Löschen von Projekten und Löschen von Dashboards im SiteWise Monitor-Anwendungshandbuch.

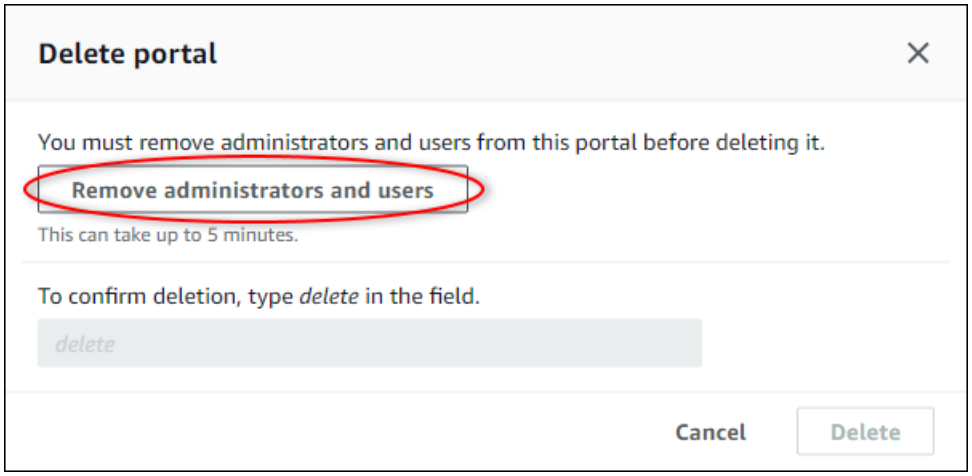
1. Wählen Sie auf der Seite „Portal details (Portaldetails)“ die Option Delete (Löschen) aus.

> **Important**
>
> Wenn Sie ein Portal löschen, gehen alle Projekte, die das Portal enthält, und alle Dashboards in den einzelnen Projekten verloren. Diese Aktion kann nicht mehr rückgängig gemacht werden. Ihre Komponentendaten sind nicht betroffen.

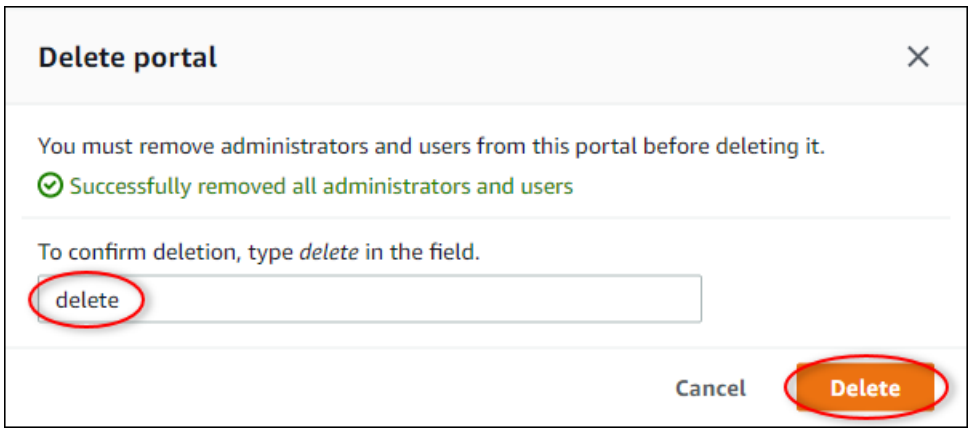


2. Wählen Sie im Dialogfeld Portale löschen die Option Admins and users entfernen aus.

   Sie müssen die Administratoren und Benutzer aus dem Portal entfernen, bevor Sie das Portal löschen können. Wenn es für Ihr Portal keine Administratoren oder Benutzer gibt, wird die Schaltfläche nicht angezeigt und Sie können mit dem nächsten Schritt fortfahren.



3. Wenn Sie sicher sind, dass Sie das gesamte Portal löschen möchten, geben Sie **`delete`** in das Feld ein, um das Löschen zu bestätigen.



4. Wählen Sie Löschen.

Überwachen von Daten mit IoT-Dashboard-Anwendung

Die IoT-Dashboard-Anwendung ist eine Open-Source-Dashboard-Anwendung, mit der Sie Betriebsdaten visualisieren und mit ihnen interagieren können. Sie können die verwendenAWS Cloud Development Kit (AWS CDK), um die IoT-Dashboard-Anwendung bereitzustellen.

Im Folgenden finden Sie Beispiele für anpassbare Datenvisualisierungsfunktionen in der IoT-Dashboard-Anwendung:

- Unterstützung für mehrere Eigenschaften in einem Einzelzeilendiagramm.
- Verbesserte Suche nach Komponenten und Eigenschaften.

Kunden aus den Bereichen Fertigung, Logistik, Energie und anderen Branchen können IoT-Dashboard-Anwendung verwenden, um bestimmte Herausforderungen zu bewältigen, z. B. die Nachverfolgung der Geräteleistung, die Optimierung der betrieblichen Effizienz und datengestützte Entscheidungen. Weitere Informationen finden Sie unter GitHub Repository für die IoT-Dashboard-Anwendung .

Daten abfragen von AWS IoT SiteWise

Sie können die AWS IoT SiteWise API-Operationen verwenden, um die aktuellen Werte, historischen Werte und Aggregate Ihrer Asset-Eigenschaften über bestimmte Zeitintervalle abzufragen.

Verwenden Sie diese Funktionen, um Einblick in Ihre Daten zu erhalten. Finden Sie beispielsweise alle Ihre Vermögenswerte mit einem bestimmten Immobilienwert heraus oder erstellen Sie eine benutzerdefinierte Darstellung Ihrer Daten. Sie können API-Operationen auch verwenden, um Softwarelösungen zu entwickeln, die sich in die in Ihren AWS IoT SiteWise Anlagen gespeicherten Industriedaten integrieren lassen. Sie können Ihre Komponentendaten auch live in AWS IoT SiteWise Monitor untersuchen. Informationen zur Konfiguration von SiteWise Monitor finden Sie unterDaten überwachen mit AWS IoT SiteWise Monitor.

Die in diesem Abschnitt beschriebenen Operationen geben Eigenschaftswertobjekte zurück, die Zeitstempel-, Qualitäts- und Wertstrukturen (TQV) enthalten:

- `timestamp` enthält die aktuelle Unix-Epoche in Sekunden mit Nanosekunden-Offset.
- `quality` enthält eine der folgenden Zeichenfolgen zur Angabe der Qualität des Datenpunkts:
  - `GOOD`— Die Daten sind von keinen Problemen betroffen.
  - `BAD`— Die Daten sind von einem Problem wie einem Sensorausfall betroffen.
  - `UNCERTAIN`— Die Daten sind von einem Problem wie einer Sensorungenauigkeit betroffen.
- `value` enthält abhängig vom Typ der Eigenschaft eines der folgenden Felder:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Themen

Immobilienwerte des aktuellen Vermögenswerts abfragen

Dieses Tutorial zeigt zwei Möglichkeiten, den aktuellen Wert einer Anlageneigenschaft zu ermitteln. Sie können die AWS IoT SiteWise Konsole oder die API in der AWS Command Line Interface (AWS CLI) verwenden.

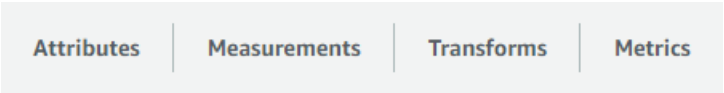
Themen

Fragen Sie den aktuellen Wert einer Asset-Eigenschaft ab (Konsole)

Sie können die AWS IoT SiteWise Konsole verwenden, um den aktuellen Wert einer Anlageneigenschaft anzuzeigen.

So erhalten Sie den aktuellen Wert einer Komponenteneigenschaft (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die Komponente mit der abzufragenden Eigenschaft aus.
4. Wählen Sie das Pfeilsymbol, um eine Asset-Hierarchie zu erweitern und Ihr Asset zu finden.
5. Wählen Sie die Registerkarte für den Eigenschaftstyp aus. Wählen Sie beispielsweise Messungen, um den aktuellen Wert einer Messungseigenschaft anzuzeigen.

6. Suchen Sie nach der anzuzeigenden Eigenschaft. Der aktuelle Wert wird in der Spalte Aktueller Wert angezeigt.

Fragen Sie den aktuellen Wert einer Anlageneigenschaft ab (AWS CLI)

Sie können das AWS Command Line Interface (AWS CLI) verwenden, um den aktuellen Wert einer Anlageneigenschaft abzufragen.

Verwenden Sie die GetAssetPropertyValueOperation, um den aktuellen Wert einer Anlageneigenschaft abzufragen.

Um eine Anlageneigenschaft zu identifizieren, geben Sie eine der folgenden Optionen an:

- Das `assetId` Ende `propertyId` der Anlageneigenschaft, an die Daten gesendet werden.
- The`propertyAlias`, bei dem es sich um einen Datenstream-Alias handelt (z. B.`/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Informationen zum Festlegen von Eigenschaftsaliasnamen finden Sie unterZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

So ermitteln Sie den aktuellen Wert einer Anlageneigenschaft ()AWS CLI

- Führen Sie den folgenden Befehl aus, um den aktuellen Wert der Komponenteneigenschaft abzurufen. Ersetzen Sie *`asset-id`* durch die ID der Komponente und *`property-id`* durch die ID der Eigenschaft.

  ```
  aws iotsitewise get-asset-property-value \
    --asset-id asset-id \
    --property-id property-id
  ```

  Die Operation gibt eine Antwort mit der aktuellen TQV der Eigenschaft im folgenden Format zurück.

  ```
  {
    "propertyValue": {
      "value": {
        "booleanValue": Boolean,
        "doubleValue": Number,
        "integerValue": Number,
        "stringValue": "String"
      },
      "timestamp": {
        "timeInSeconds": Number,
        "offsetInNanos": Number
      },
      "quality": "String"
    }
  }
  ```

Abfragen von historischen Komponenteneigenschaftswerten

Sie können den AWS IoT SiteWise GetAssetPropertyValueHistoryAPI-Vorgang verwenden, um die historischen Werte einer Anlageneigenschaft abzufragen.

Um eine Anlageneigenschaft zu identifizieren, geben Sie eine der folgenden Optionen an:

- Das `assetId` Ende `propertyId` der Anlageneigenschaft, an die Daten gesendet werden.
- The`propertyAlias`, bei dem es sich um einen Datenstream-Alias handelt (z. B.`/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Informationen zum Festlegen von Eigenschaftsaliasnamen finden Sie unterZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Übergeben Sie die folgenden Parameter, um Ihre Ergebnisse zu verfeinern:

- `startDate`— Der ausschließliche Anfang des Bereichs, aus dem historische Daten abgefragt werden sollen, ausgedrückt in Sekunden in der Unix-Epoche.
- `endDate`— Das inklusive Ende des Bereichs, aus dem historische Daten abgefragt werden sollen, ausgedrückt in Sekunden in der Unix-Epochenzeit.
- `maxResults`— Die maximale Anzahl von Ergebnissen, die in einer Anfrage zurückgegeben werden sollen. Standardmäßig werden `20` Ergebnisse verwendet.
- `nextToken`— Ein Paginierungstoken, das von einem früheren Aufruf dieser Operation zurückgegeben wurde.
- `timeOrdering`— Die Reihenfolge, die auf die zurückgegebenen Werte angewendet werden soll: `ASCENDING` oder`DESCENDING`.
- `qualities`— Die Qualität, nach der Ergebnisse gefiltert werden sollen nach: `GOODBAD`,, oder`UNCERTAIN`.

Themen

- Fragen Sie den Werteverlauf für eine Anlageeigenschaft ab (AWS CLI)

Fragen Sie den Werteverlauf für eine Anlageeigenschaft ab (AWS CLI)

Um den Werteverlauf für eine Anlageeigenschaft abzufragen (AWS CLI)

1. Führen Sie den folgenden Befehl aus, um den Wertverlauf für die Komponenteneigenschaft abzurufen. Dieser Befehl fragt den Verlauf der Eigenschaft über ein bestimmtes 10-Minuten-Intervall ab. Ersetzen Sie *asset-id* durch die ID der Komponente und *property-id* durch die ID der Eigenschaft. Ersetzen Sie die Datumsparameter durch das abzufragende Intervall.

   ```
   aws iotsitewise get-asset-property-value-history \
     --asset-id asset-id \
     --property-id property-id \
     --start-date 1575216000 \
     --end-date 1575216600
   ```

   Die Operation gibt eine Antwort zurück, die die historischen TQVs der Eigenschaft im folgenden Format enthält:

   ```
   {
     "assetPropertyValueHistory": [
       {
         "value": {
           "booleanValue": Boolean,
           "doubleValue": Number,
           "integerValue": Number,
           "stringValue": "String"
         },
         "timestamp": {
           "timeInSeconds": Number,
           "offsetInNanos": Number
         },
         "quality": "String"
       }
     ],
     "nextToken": "String"
   }
   ```

2. Wenn mehr Werteinträge vorhanden sind, können Sie das Paginierungstoken aus dem `nextToken` Feld an einen nachfolgenden Aufruf der GetAssetPropertyValueHistoryOperation übergeben.

Abfragen von Komponenteneigenschaften-Aggregaten

AWS IoT SiteWise berechnet automatisch aggregierte Immobilienwerte, bei denen es sich um eine Reihe von Basiskennzahlen handelt, die über mehrere Zeitintervalle berechnet werden. AWS IoT SiteWise berechnet jede Minute, Stunde und Tag die folgenden Aggregate für Ihre Anlageeigenschaften:

- Durchschnitt — Der Durchschnitt (Mittelwert) der Werte einer Immobilie über ein Zeitintervall.
- Anzahl — Die Anzahl der Datenpunkte für eine Eigenschaft über ein Zeitintervall.
- Maximum — Das Maximum der Werte einer Eigenschaft über ein Zeitintervall.
- Minimum — Das Minimum der Werte einer Eigenschaft über ein Zeitintervall.
- Standardabweichung — Die Standardabweichung der Werte einer Eigenschaft über ein Zeitintervall.
- Summe — Die Summe der Werte einer Eigenschaft über ein Zeitintervall.

Für nicht numerische Eigenschaften, wie Zeichenketten und Boolesche Werte, wird nur das Aggregat für die AWS IoT SiteWise Anzahl berechnet.

Sie können für Ihre Komponentendaten auch benutzerdefinierte Metriken berechnen. Mit metrischen Eigenschaften definieren Sie Aggregationen, die für Ihren Vorgang spezifisch sind. Metrische Eigenschaften bieten zusätzliche Aggregationsfunktionen und Zeitintervalle, die für die API nicht im Voraus berechnet wurden. AWS IoT SiteWise Weitere Informationen finden Sie unter Aggregieren von Daten aus Immobilien und anderen Vermögenswerten (Metriken).

Themen

Aggregate für eine Anlageneigenschaft (API)

Sie können die AWS IoT SiteWise API verwenden, um Aggregate für eine Anlageneigenschaft abzurufen.

Verwenden Sie den GetAssetPropertyAggregatesVorgang, um Aggregate einer Anlageneigenschaft abzufragen.

Um eine Anlageneigenschaft zu identifizieren, geben Sie eine der folgenden Optionen an:

- Das `assetId` Ende `propertyId` der Anlageneigenschaft, an die Daten gesendet werden.
- The`propertyAlias`, bei dem es sich um einen Datenstream-Alias handelt (z. B.`/company/windfarm/3/turbine/7/temperature`). Um diese Option verwenden zu können, müssen Sie zuerst den Alias der Komponenteneigenschaft festlegen. Informationen zum Festlegen von Eigenschaftsaliasnamen finden Sie unterZuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

Sie müssen auch die folgenden erforderlichen Parameter übergeben:

- `aggregateTypes`— Die Liste der abzurufenden Aggregate. Sie können `AVERAGE`, `COUNT`, `MAXIMUM`, `MINIMUM`, `STANDARD_DEVIATION` oder `SUM` angeben.
- `resolution`— Das Zeitintervall, für das die Metrik abgerufen werden soll: `1m` (1 Minute), `1h` (1 Stunde) oder `1d` (1 Tag).
- `startDate`— Der ausschließliche Anfang des Bereichs, aus dem historische Daten abgefragt werden sollen, ausgedrückt in Sekunden in der Unix-Epochenzeit.
- `endDate`— Das inklusive Ende des Bereichs, aus dem historische Daten abgefragt werden sollen, ausgedrückt in Sekunden in der Unix-Epochenzeit.

Sie können auch einen der folgenden Parameter übergeben, um Ihre Ergebnisse zu verfeinern:

- `maxResults`— Die maximale Anzahl von Ergebnissen, die in einer Anfrage zurückgegeben werden sollen. Standardmäßig werden `20` Ergebnisse verwendet.
- `nextToken`— Ein Paginierungstoken, das von einem früheren Aufruf dieser Operation zurückgegeben wurde.
- `timeOrdering`— Die Reihenfolge, die auf die zurückgegebenen Werte angewendet werden soll: `ASCENDING` oder`DESCENDING`.
- `qualities`— Die Qualität, nach der Ergebnisse gefiltert werden sollen nach: `GOODBAD`,, oder`UNCERTAIN`.

> **Note**
>
> Die GetAssetPropertyAggregatesOperation gibt ein TQV zurück, dessen Format sich von den anderen in diesem Abschnitt beschriebenen Operationen unterscheidet. Die `value`-Struktur

enthält ein Feld für jeden der `aggregateTypes` in der Anforderung. Der `timestamp` enthält die Zeit in Sekunden in Unix-Epoche-Zeit, zu der die Aggregation stattfand.

Aggregate für eine Anlageeigenschaft ()AWS CLI

Um Aggregate für eine Anlageneigenschaft abzufragen ()AWS CLI

1. Führen Sie den folgenden Befehl aus, um Aggregate für die Komponenteneigenschaft abzurufen. Dieser Befehl fragt den Durchschnitt und die Summe mit einer Auflösung von 1 Stunde für ein bestimmtes Intervall von 1 Stunde ab. Ersetzen Sie *`asset-id`* durch die ID der Komponente und *`property-id`* durch die ID der Eigenschaft. Ersetzen Sie die Parameter durch die Aggregate und das abzufragende Intervall.

```
aws iotsitewise get-asset-property-aggregates \
  --asset-id asset-id \
  --property-id property-id \
  --start-date 1575216000 \
  --end-date 1575219600 \
  --aggregate-types AVERAGE SUM \
  --resolution 1h
```

Die Operation gibt eine Antwort mit den historischen TQVs der Eigenschaft im folgenden Format zurück. Die Antwort enthält nur die angeforderten Aggregate.

```
{
  "aggregatedValues": [
    {
      "timestamp": Number,
      "quality": "String",
      "value": {
        "average": Number,
        "count": Number,
        "maximum": Number,
        "minimum": Number,
        "standardDeviation": Number,
        "sum": Number
      }
    }
  ],
  "nextToken": "String"
```

```
}
```

2. Wenn mehr Werteinträge vorhanden sind, können Sie das Paginierungstoken aus dem `nextToken` Feld an einen nachfolgenden Aufruf der GetAssetPropertyAggregatesOperation übergeben.

AWS IoT SiteWise Abfragesprache

Mit dem ExecuteQueryAPI-Vorgang zum AWS IoT SiteWise Datenabruf können Sie Informationen zu deklarativen Strukturdefinitionen und den damit verbundenen Zeitreihendaten aus folgenden Quellen abrufen:

- Modelle
- Vermögenswerte
- Messungen
- Kennzahlen
- wandelt um
- Aggregate

Dies kann mit SQL-ähnlichen Abfrageanweisungen in einer einzigen API-Anfrage erfolgen.

> **Note**
>
> Diese Funktion ist in allen Regionen verfügbar, in denen AWS IoT SiteWise sowohl als auch verfügbar AWS IoT TwinMaker sind, außer in AWS GovCloud (USA West).

Themen

Voraussetzungen

AWS IoT SiteWise benötigt Genehmigungen für die Integration, AWS IoT TwinMaker damit industrielle Daten organisiert und modelliert werden können.

Bevor Sie Informationen über Modelle, Anlagen, Messungen, Metriken, Transformationen und Aggregate abrufen können, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Serviceverknüpfte Rollen für beide AWS IoT SiteWise und AWS IoT TwinMaker Einrichtung in Ihrem. AWS-Konto Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen im IAM-Benutzerhandbuch.
- Eine aktivierte AWS IoT SiteWise Integration für Ihre IAM-Rolle. Weitere Informationen finden Sie unter Integration von AWS IoT SiteWise und AWS IoT TwinMaker.
- Ein AWS IoT TwinMaker Workspace mit ID `IoTSiteWiseDefaultWorkspace` in deinem Konto in der Region. Weitere Informationen finden Sie unter Using the IoTSiteWiseDefaultWorkspace im AWS IoT TwinMaker -Benutzerhandbuch.
- Entweder der Standard - oder der gestaffelte Paketpreismodus für AWS IoT TwinMaker aktiviert. Weitere Informationen finden Sie im AWS IoT TwinMaker Benutzerhandbuch unter AWS IoT TwinMaker Preismodus wechseln.

Sprachreferenz abfragen

AWS IoT SiteWise unterstützt eine umfangreiche Abfragesprache für die Arbeit mit Ihren Daten. Die verfügbaren Datentypen, Operatoren, Funktionen und Konstrukte werden in den folgenden Themen beschrieben.

Informationen Beispielabfragen zum Schreiben von Abfragen mit der AWS IoT SiteWise Abfragesprache finden Sie unter.

Themen

- Ansichten verstehen
- Unterstützte Datentypen
- Rufen Sie Daten mit einer SELECT-Anweisung ab
- Logische Operatoren
- Vergleichsoperatoren
- Beispielabfragen

Ansichten verstehen

Dieser Abschnitt enthält Informationen, die Ihnen helfen sollen, die Ansichten in zu verstehen AWS IoT SiteWise, z. B. Prozessmetadaten und Telemetriedaten.

Die folgenden Tabellen enthalten die Namen und Beschreibungen der Ansichten.

Datenmodell

Name der Ansicht	Ansichtsbeschreibung
Komponente	Enthält Informationen zur Anlage- und Modellableitung.
asset_property	Enthält Informationen über die Struktur der Anlageeigenschaft.
raw_time_series	Enthält die historischen Daten der Zeitreihe.
latest_value_time_series	Enthält den neuesten Wert der Zeitreihe.
precomputed_aggregates	Enthält die automatisch berechneten aggregier ten Eigenschaftswerte von Vermögens werten. Es handelt sich um eine Reihe von Basiskennzahlen, die über mehrere Zeitinter valle berechnet wurden.

In den folgenden Ansichten sind die Spaltennamen für Abfragen zusammen mit Beispieldaten aufgeführt.

Ansicht: Anlage

asset_id	Name der Anlage	Beschreibung der Anlage	Asset_Modell-ID
88898498-0b8b-42b5-bf57-16180bc3d3a0	WindTurbine EIN	WindTurbine Anlage A	17847250-5bf0-4f74-b775-cc03f05e7cb8
17847250-5bf0-4f74-b775-cc03f05e7cb8	Anlagenmodell einer Windkraftanlage	Stellt eine Turbine in einem Windpark dar.	

Ansicht: ASSET_PROPERTY

property_id	Objekt-ID	Eigenschaftsname	Eigenschaft_Datentyp	Eigenschaftsalias	Asset_Composite_Modell-ID
b29be434-b000-4d74-b809-75287d83bcd6	88898498-0b8b-42b5-bf57-16180bc3d3a0	Motortemperatur	Double	`Rochester 2/44///Line-5/Bus-2/Machine-5/Temperature`	
3b458f00-24e7-458a-b4e8-c6026eff654a	88898498-0b8b-42b5-bf57-16180bc3d3a0	Windrichtung	Double	`/company/windfarm/3/turbine/7/winddirection`	2f458n00-56e7-458h-b4e8-c6026eff985g

Ansicht: RAW_TIME_SERIES

asset_id	Eigenschafts-ID	Eigenschaftsalias	Zeitstempel des Ereignisses	Qualität	boolescher_Wert	int_wert	doppelter Wert	Zeichenkettenwert
88898498-0b8b-42b5-bf57-16180bc3d3a	b29be434-b000-4d74-b809-75287d83bcd	`Rochester 2/44///Line-5/Bus-2/Machine-5/Temperature`	1575219600	GUT			115,0	

asset_id	Eigenscha fts-ID	Eigenscha ftsalias	Zeitstemp el des Ereigniss es	Qualität	boolesche r_Wert	int_wert	doppelter Wert	Zeichenke ttenwert
88898498 0b8b-42b5 - bf57-161 80bc3d3a	3b458f00- 24e7-458a -b4e8- c60 26eff654a	/ company, windfarı 3/ turbine /7/ winddi rection	15752193 7	GUT			348,75	

> **Note**
>
> Sie müssen eine Filterklausel in die `event_timestamp` Spalte aufnehmen, um die Ansicht abzufragen. `raw_time_series` Dies ist ein erforderlicher Filter, und ohne ihn schlägt die Abfrage fehl.
>
> Example query
>
> ```
> SELECT event_timestamp, double_value FROM raw_time_series WHERE event_timestamp
>  > 1234567890
> ```

Ansicht: Latest_Value_Time_Series

asset_id	Eigenscha fts-ID	Eigenscha ftsalias	Zeitstemp el des Ereigniss es	Qualität	boolesche r_Wert	int_wert	doppelter Wert	Zeichenke ttenwert
88898498 0b8b-42b5 - bf57-161	3b458f00- 24e7-458a -b4e8- c60	/ company, windfarı	15752196 0	GUT			355,39	

asset_id	Eigenscha fts-ID	Eigenscha ftsalias	Zeitstemp el des Ereigniss es	Qualität	boolesche r_Wert	int_wert	doppelter Wert	Zeichenke ttenwert
80bc3d3a	26eff654a	3/ turbine /7/ winddi rection						

Ansicht: precomputed_aggregates

asset_ic	Eigensc fts-ID	Eigensc ftsalias	Zeitsten el des Ereignis es	Auflösu	Summe t	Anzahl_ rt	Durchsc ittswert	maxima ert	minimal ert	Standardw ert
888984 0b8b-42 - bf57-16 80bc3d	b29be4 b000-4c - b809-75 87d83b	Roches 2/44// Li ne-5/ Bus- 2/ Machin -5/ Temper ature	157521 0	15m	1105,48	15	73,4	80,6	68	3,64

Unterstützte Datentypen

AWS IoT SiteWise Die Abfragesprache unterstützt die folgenden Datentypen.

Ansicht: Anlage

Datentyp	Beschreibung
`STRING`	Eine Zeichenfolge mit einer maximalen Länge von 1024 Byte.
`INTEGER`	Eine 32-Bit-Ganzzahl mit Vorzeichen und einem Bereich von`-2,147,483,648 to 2,147,483,647` .
`DOUBLE`	Eine Fließkommazahl mit einem Bereich von `-10^100 to 10^100` und `IEEE 754` doppelter Genauigkeit.
`BOOLEAN`	`true` oder `false`.

> **Note**
>
> Die Daten mit doppelter Genauigkeit sind nicht exakt. Einige Werte werden nicht exakt konvertiert und stellen aufgrund der begrenzten Genauigkeit nicht alle reellen Zahlen dar. Gleitkommadaten in der Abfrage sind möglicherweise nicht derselbe Wert, der intern dargestellt wird. Der Wert wird gerundet, wenn die Genauigkeit einer eingegebenen Zahl zu hoch ist.

Rufen Sie Daten mit einer SELECT-Anweisung ab

Die `SELECT` Anweisung wird verwendet, um Daten aus einer oder mehreren Ansichten abzurufen. AWS IoT SiteWise unterstützt eine implizite `JOIN` Ansicht. Sie können die Ansichten, die verknüpft werden sollen, auflisten (in der `FROM` Klausel der `SELECT` Anweisung), indem Sie sie durch Kommas trennen.

Example

Verwenden Sie die folgende `SELECT` Anweisung:

```
SELECT select_expr [, ...]
```

```
[ FROM from_item [, ...] ]
[ WHERE [LIKE condition ESCAPE condition] ]
```

Im vorherigen Beispiel spezifiziert die `LIKE` Klausel die Such- und Filterbedingungen mithilfe von Platzhaltern. AWS IoT SiteWise unterstützt `percentage (%)` als Platzhalterzeichen.

Example zur Verwendung **%** unter bestimmten Bedingungen:

```
Prefix search: String%
Infix search: %String%
Suffix search: %String
```

Example um nach einem Asset zu suchen:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'Wind%'
```

Example um mithilfe einer ESCAPE-Bedingung nach einem Asset zu suchen:

```
SELECT asset_name, asset_description FROM asset WHERE asset_name LIKE 'room\%' ESCAPE
 '\'
```

Logische Operatoren

AWS IoT SiteWise unterstützt die folgenden logischen Operatoren.

Logische Operatoren

Operator	Beschreibung	Beispiel
`AND`	`TRUE`wenn beide Werte wahr sind	a `AND` b

Wenn entweder a oder b zutrifft`FALSE`, wird der vorherige Ausdruck als falsch ausgewertet. Damit ein `AND` Operator als wahr ausgewertet werden kann, müssen sowohl a als auch b wahr sein.

Example

```
SELECT a.asset_name
```

```
FROM asset as a, latest_value_time_series as t
WHERE t.int_value > 30 AND t.event_timestamp > 1234567890
```

Vergleichsoperatoren

AWS IoT SiteWise unterstützt die folgenden Vergleichsoperatoren.

Logische Operatoren

Operator	Beschreibung
<	kleiner als
>	größer als
<=	kleiner als oder gleich
>=	größer als oder gleich
=	Gleichheitszeichen
!=	Ungleich

Beispielabfragen

Filterung von Metadaten

Das folgende Beispiel bezieht sich auf die Metadatenfilterung mit einer `SELECT` Anweisung in der AWS IoT SiteWise Abfragesprache:

```
SELECT a.asset_name, p.property_name
FROM asset a, asset_property p
WHERE a.asset_id = p.asset_id AND a.asset_name LIKE '%windmill%'
```

Filterung von Werten

Im Folgenden finden Sie ein Beispiel für die Wertfilterung mithilfe einer `SELECT` Anweisung in der AWS IoT SiteWise Abfragesprache:

```
SELECT a.asset_name FROM asset a, raw_time_series r
WHERE a.asset_id = r.asset_id AND r.int_value > 30  AND r.event_timestamp > 1234567890
 AND r.event_timestamp < 1234567891
```

Interaktion mit anderen AWS Diensten

AWS IoT SiteWise kann Asset-Daten im Publish-Subscribe-Nachrichtenbroker von AWS IoT MQTT veröffentlichen, sodass Sie mit Ihren Asset-Daten aus anderen Diensten interagieren können. AWS AWS IoT SiteWise weist jeder Asset-Eigenschaft ein eindeutiges MQTT-Thema zu, das Sie verwenden können, um Ihre Asset-Daten mithilfe von Core-Regeln an andere AWS Dienste weiterzuleiten. AWS IoT Sie können beispielsweise AWS IoT Core-Regeln für die folgenden Aufgaben konfigurieren:

- Ermittlung von Anlagenausfällen und Benachrichtigung der entsprechenden Mitarbeiter durch Senden von Daten an AWS IoT Events.
- Historisieren Sie ausgewählte Asset-Daten zur Verwendung in externen Softwarelösungen, indem Sie Daten an Amazon DynamoDB senden.
- Generieren wöchentlicher Berichte durch Auslösen einer AWS Lambda-Funktion.

Sie können einem Tutorial folgen, das die Schritte beschreibt, die zum Einrichten einer Regel zum Speichern von Eigenschaftswerten in DynamoDB erforderlich sind. Weitere Informationen finden Sie unter Veröffentlichung von Eigenschaftswertaktualisierungen in Amazon DynamoDB.

Weitere Informationen zur Konfiguration einer Regel finden Sie unter Regeln im AWS IoT Entwicklerhandbuch.

Sie können auch Daten aus anderen AWS Diensten wieder in das System einlesen AWS IoT SiteWise. Informationen zum Aufnehmen von Daten mithilfe der AWS IoT SiteWise Regelaktion finden Sie unterDaten mithilfe AWS IoT Core von Regeln aufnehmen.

Themen

- Grundlegendes zu Komponenteneigenschafts-MQTT-Themen
- Mit Benachrichtigungen über Vermögenseigenschaften arbeiten
- Exportieren Sie Daten mit Benachrichtigungen über Vermögenseigenschaften nach Amazon S3
- Integration in Grafana
- Integration von AWS IoT SiteWise und AWS IoT TwinMaker
- Erkennung von Geräteanomalien mit Amazon Lookout for Equipment

Grundlegendes zu Komponenteneigenschafts-MQTT-Themen

Jede Komponenteneigenschaft verfügt über einen eindeutigen MQTT-Themenpfad im folgenden Format.

```
$aws/sitewise/asset-models/assetModelId/assets/assetId/properties/propertyId
```

> **Note**
>
> AWS IoT SiteWise unterstützt den Platzhalter für den # (mehrstufigen) Themenfilter in der AWS IoT Core Rules Engine nicht. Sie können den (einstufigen) Platzhalter + verwenden. So können Sie beispielsweise den folgenden Themenfilter verwenden, um alle Aktualisierungen für ein bestimmtes Komponentenmodell abzugleichen.
>
> ```
> $aws/sitewise/asset-models/assetModelId/assets/+/properties/+
> ```
>
> Weitere Informationen zu Platzhaltern für Themenfilter finden Sie unter Themen im AWS IoT Core Developer Guide.

Mit Benachrichtigungen über Vermögenseigenschaften arbeiten

Sie können Eigenschaftsbenachrichtigungen aktivieren AWS IoT Core, um Aktualisierungen der Objektdaten zu veröffentlichen und anschließend Abfragen für Ihre Daten durchzuführen. AWS IoT SiteWise Bietet mit Benachrichtigungen über Vermögenseigenschaften eine AWS CloudFormation Vorlage, mit der Sie AWS IoT SiteWise Daten nach Amazon S3 exportieren können.

> **Note**
>
> Objektdaten werden bei AWS IoT Core jedem Empfang an gesendet AWS IoT SiteWise, unabhängig davon, ob sich der Wert geändert hat.

Themen

- Aktivieren der Benachrichtigungen zu Komponenteneigenschaften (Konsole)
- Benachrichtigungen über Vermögenseigenschaften aktivieren (AWS CLI)
- Abfragen von Benachrichtigungsmeldungen für Komponenteneigenschaften

Aktivieren der Benachrichtigungen zu Komponenteneigenschaften (Konsole)

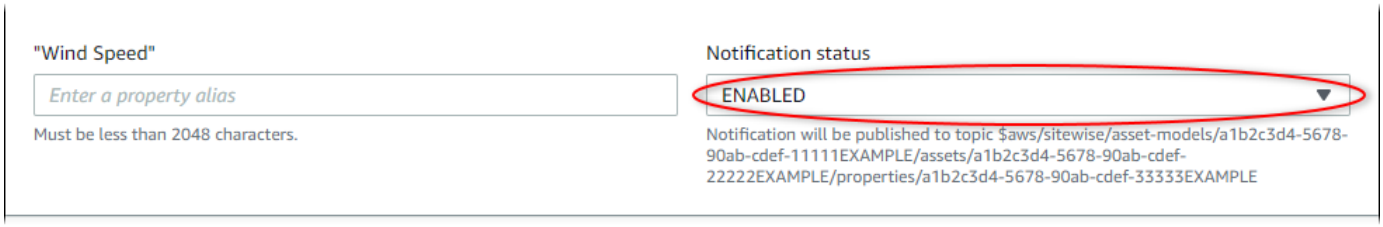
Veröffentlicht standardmäßig AWS IoT SiteWise keine Aktualisierungen des Immobilienwerts. Sie können die AWS IoT SiteWise Konsole verwenden, um Benachrichtigungen für eine Objekteigenschaft zu aktivieren.

So aktivieren oder deaktivieren Sie Benachrichtigungen für eine Komponenteneigenschaft (Konsole)

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Komponenten aus.
3. Wählen Sie die Komponente aus, um die Benachrichtigungen einer Eigenschaft zu aktivieren.

   > **Tip**
   >
   > Sie können eine Komponentenhierarchie mithilfe des Pfeilsymbols erweitern, um nach Ihrer Komponente zu suchen.

4. Wählen Sie Bearbeiten aus.
5. Wählen Sie für den Benachrichtigungsstatus der Komponenteneigenschaft AKTIVIERT aus.

   Sie können auch DEAKTIVIERT wählen, um Benachrichtigungen für die Komponenteneigenschaft zu deaktivieren.
6. Wählen Sie Speichern.

Benachrichtigungen über Vermögenseigenschaften aktivieren (AWS CLI)

Veröffentlicht standardmäßig AWS IoT SiteWise keine Aktualisierungen von Eigenschaftswerten. Sie können das AWS Command Line Interface (AWS CLI) verwenden, um Benachrichtigungen für eine Asset-Eigenschaft zu aktivieren oder zu deaktivieren.

Um dieses Verfahren abzuschließen, müssen Sie die `assetId` Ihrer Komponenten und die `propertyId` Ihrer Eigenschaft kennen. Sie können auch die externe ID verwenden. Wenn Sie ein Asset erstellt haben und es nicht kennen`assetId`, verwenden Sie die ListAssetsAPI, um alle Assets für ein bestimmtes Modell aufzulisten. Verwenden Sie den DescribeAssetVorgang, um die Eigenschaften Ihres Assets einschließlich der Eigenschafts-IDs anzuzeigen.

Verwenden Sie den UpdateAssetPropertyVorgang, um Benachrichtigungen für eine Vermögenseigenschaft zu aktivieren oder zu deaktivieren. Geben Sie die folgenden Parameter an:

- `assetId`— Die ID des Vermögenswerts.
- `propertyId`— Die ID des Vermögenswerts.
- `propertyNotificationState`— Status der Benachrichtigung über den Immobilienwert: `ENABLED` oder`DISABLED`.
- `propertyAlias`— Der Alias der Immobilie. Geben Sie den vorhandenen Alias der Eigenschaft an, wenn Sie den Benachrichtigungsstatus aktualisieren. Wenn Sie diesen Parameter auslassen, wird der vorhandene Alias der Eigenschaft entfernt.

So aktivieren oder deaktivieren Sie Benachrichtigungen für eine Komponenteneigenschaft (CLI)

1. Führen Sie den folgenden Befehl aus, um den Alias der Komponenteneigenschaft abzurufen. Ersetzen Sie *`asset-id`* durch die ID der Komponente und *`property-id`* durch die ID der Eigenschaft.

   ```
   aws iotsitewise describe-asset-property \
     --asset-id asset-id \
     --property-id property-id
   ```

   Die Operation gibt eine Antwort zurück, die Informationen zur Komponenteneigenschaft im folgenden Format enthält. Der Eigenschaftenalias befindet sich in `assetProperty.alias` im JSON-Objekt.

   ```
   {
     "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
     "assetName": "Wind Turbine 7",
     "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
     "assetProperty": {
       "id": "a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
       "name": "Wind Speed",
   ```

```
    "alias": "/company/windfarm/3/turbine/7/windspeed",
    "notification": {
      "topic": "$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/
assets/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/properties/a1b2c3d4-5678-90ab-
cdef-33333EXAMPLE",
      "state": "DISABLED"
    },
    "dataType": "DOUBLE",
    "unit": "m/s",
    "type": {
      "measurement": {}
    }
  }
}
```

2. Führen Sie den folgenden Befehl aus, um Benachrichtigungen für die Komponenteneigenschaft zu aktivieren. Ersetzen Sie *property-alias* durch den Eigenschaftenalias aus der Antwort des vorherigen Befehls, oder lassen Sie `--property-alias` weg, um die Eigenschaft ohne einen Alias zu aktualisieren.

   ```
   aws iotsitewise update-asset-property \
     --asset-id asset-id \
     --property-id property-id \
     --property-notification-state ENABLED \
     --property-alias property-alias
   ```

   Sie können auch `--property-notification-state DISABLED` übergeben, um Benachrichtigungen für die Komponenteneigenschaft zu deaktivieren.

Abfragen von Benachrichtigungsmeldungen für Komponenteneigenschaften

Um Benachrichtigungen über Vermögenseigenschaften abzufragen, erstellen Sie AWS IoT Core Regeln, die aus SQL-Anweisungen bestehen.

AWS IoT SiteWise veröffentlicht Aktualisierungen von Objektdaten in AWS IoT Core im folgenden Format.

```
{
  "type": "PropertyValueUpdate",
  "payload": {
    "assetId": "String",
```

```
    "propertyId": "String",
    "values": [
      {
        "timestamp": {
          "timeInSeconds": Number,
          "offsetInNanos": Number
        },
        "quality": "String",
        "value": {
          "booleanValue": Boolean,
          "doubleValue": Number,
          "integerValue": Number,
          "stringValue": "String"
        }
      }
    ]
  }
}
```

Jede Struktur in der `values` Liste ist eine timestamp-quality-value (TQV-) Struktur.

- `timestamp` enthält die aktuelle Unix-Epoche in Sekunden mit Nanosekunden-Offset.
- `quality` enthält eine der folgenden Zeichenfolgen zur Angabe der Qualität des Datenpunkts:
  - `GOOD`— Die Daten sind von keinen Problemen betroffen.
  - `BAD`— Die Daten sind von einem Problem wie einem Sensorausfall betroffen.
  - `UNCERTAIN`— Die Daten sind von einem Problem wie einer Sensorungenauigkeit betroffen.
- `value` enthält abhängig vom Typ der Eigenschaft eines der folgenden Felder:
  - `booleanValue`
  - `doubleValue`
  - `integerValue`
  - `stringValue`

Um Werte aus dem `values`-Array zu analysieren, müssen Sie in den SQL-Anweisungen Ihrer Regeln komplexe verschachtelte Objektabfragen verwenden. Weitere Informationen finden Sie im AWS IoT Entwicklerhandbuch unter Abfragen verschachtelter Objekte. Ein konkretes Beispiel für das Analysieren von Benachrichtigungen über Asset-Eigenschaften finden Sie im Veröffentlichung von Eigenschaftswertaktualisierungen in Amazon DynamoDB Tutorial.

Example Beispielabfrage zum Extrahieren des Werte-Arrays

Die folgende Anweisung veranschaulicht, wie das Array aktueller Eigenschaftswerte für eine bestimmte Eigenschaft vom doppelten Typ für alle Komponenten mit dieser Eigenschaft abgefragt wird.

```
SELECT
  (SELECT VALUE (value.doubleValue) FROM payload.values) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
WHERE
  type = 'PropertyValueUpdate'
```

Die vorherige Anweisung zur Regelabfrage gibt Daten im folgenden Format aus.

```
{
  "windspeed": [
    26.32020195042838,
    26.282584572975477,
    26.352566977372508,
    26.283084346171442,
    26.571883739599322,
    26.60684140743005,
    26.628738636715045,
    26.273486932802125,
    26.436379105473964,
    26.600590095377303
  ]
}
```

Example Beispielabfrage zum Extrahieren eines einzelnen Wertes

Die folgende Anweisung veranschaulicht, wie der erste Wert aus dem Array von Eigenschaftswerten für eine bestimmte Eigenschaft vom doppelten Typ für alle Komponenten mit dieser Eigenschaft abgefragt wird.

```
SELECT
  get((SELECT VALUE (value.doubleValue) FROM payload.values), 0) AS windspeed
FROM
  '$aws/sitewise/asset-models/a1b2c3d4-5678-90ab-cdef-11111EXAMPLE/assets/+/
properties/a1b2c3d4-5678-90ab-cdef-33333EXAMPLE'
```

```
WHERE
  type = 'PropertyValueUpdate'
```

Die vorherige Anweisung zur Regelabfrage gibt Daten im folgenden Format aus.

```
{
  "windspeed": 26.32020195042838
}
```

> **Important**
>
> Diese Regelabfrageanweisung ignoriert Wertaktualisierungen, abgesehen vom ersten in jedem Stapel. Jeder Stapel kann bis zu 10 Werte enthalten. Wenn Sie die verbleibenden Werte einschließen müssen, ist es erforderlich, eine komplexere Lösung einzurichten, um Eigenschaftswerte der Komponenten an andere Services auszugeben. Sie können beispielsweise eine Regel mit einer AWS Lambda Aktion einrichten, um jeden Wert im Array erneut in einem anderen Thema zu veröffentlichen, und eine weitere Regel einrichten, um dieses Thema abzufragen und jeden Wert in der gewünschten Regelaktion zu veröffentlichen.

Exportieren Sie Daten mit Benachrichtigungen über Vermögenseigenschaften nach Amazon S3

Sie können eingehende Daten aus AWS IoT SiteWise einem Amazon S3 S3-Bucket in Ihrem Konto exportieren. Sie können Ihre Daten in einem Format sichern, das Sie verwenden können, um historische Berichte zu erstellen oder Ihre Daten mit komplexen Methoden zu analysieren.

> **Note**
>
> AWS IoT SiteWise unterstützt auch Cold-Tier-Speicher, mit dem Sie Daten in einem vom Kunden verwalteten Amazon S3 S3-Bucket speichern können. Weitere Informationen zu unterstützten Speicherstufen finden Sie unterVerwaltung des Datenspeichers.

AWS IoT SiteWise stellt diese Funktion als AWS CloudFormation Vorlage bereit. Wenn Sie aus der Vorlage einen Stack erstellen, werden die erforderlichen AWS Ressourcen AWS CloudFormation erstellt, um eingehende Daten aus einem S3-Bucket AWS IoT SiteWise zu streamen.

Anschließend empfängt der S3-Bucket alle Ihre Objektdaten, die aus Nachrichten zur Aktualisierung des AWS IoT SiteWise Immobilienwerts gesendet wurden. Der S3-Bucket empfängt auch Ihre Komponenten,etadaten, die Komponenten- und Eigenschaftsnamen und weitere Informationen enthalten.

Weitere Informationen darüber, wie Sie Eigenschaftswert-Aktualisierungsnachrichten für die Asset-Eigenschaften für den Export nach Amazon S3 aktivieren, finden Sie unterInteraktion mit anderen AWS Diensten.

Diese Funktion speichert Ihre Objektdaten und Asset-Metadaten im Apache Parquet-Format in Amazon S3. Parquet ist ein in Spalten organisiertes Datenformat, das Platz spart und im Vergleich zu zeilenorientierten Formaten wie JSON schnellere Abfragen ermöglicht.

> **Note**
>
> Wenn diese Funktion Asset-Metadaten abruft, unterstützt sie bis zu etwa 1.500 Assets. Diese Einschränkung gilt nur für Komponentenmetadaten. Diese Beschränkung gilt nicht für die Anzahl der Assets, die unterstützt werden, wenn die Funktion Asset-Eigenschaftsdaten exportiert.

Der Name jeder Ressource enthält ein Präfix, das Sie beim Erstellen des Stacks anpassen können. Ressourcen sind:

- Ein Amazon-S3-Bucket
- AWS Lambda Funktionen
- Eine AWS IoT Core Regel
- AWS Identity and Access Management Rollen
- Ein Amazon Data Firehose-Stream
- Eine Datenbank AWS Glue

Eine vollständige Liste finden Sie hier: Ressourcen, die aus der Vorlage erstellt wurden.

> **Important**
>
> Die Ressourcen, die mit dieser AWS CloudFormation Vorlage erstellt und verbraucht werden, werden Ihnen in Rechnung gestellt. Diese Gebühren beinhalten Datenspeicherung und Datenübertragung für mehrere AWS Dienste.

Themen

Erstellen Sie den AWS CloudFormation Stapel

Sie müssen einen Stack erstellen AWS CloudFormation , um Ihre Asset-Daten nach Amazon S3 zu exportieren.

Um Daten nach Amazon S3 zu exportieren

1. Öffnen Sie die AWS CloudFormation -Vorlage, und melden Sie sich bei AWS Management Console an.
2. Wählen Sie auf der Seite Create stack (Stack erstellen) unten auf der Seite Next (Weiter) aus.
3. Geben Sie auf der Seite „Stack-Details angeben“ einen Wert BucketNamefür den S3-Bucket ein, den diese Vorlage für den Empfang von Asset-Daten erstellt. Dieser Bucket-Name muss global eindeutig sein. Weitere Informationen finden Sie unter Regeln für die Bucket-Benennung im Amazon Simple Storage Service-Benutzerhandbuch.
4. (Optional) Ändern Sie andere Parameter der Vorlage:
   - GlobalResourcePrefix— Ein Präfix für Namen globaler Ressourcen, wie z. B. IAM-Rollen, die anhand dieser Vorlage erstellt wurden.
   - LocalResourcePrefix— Ein Präfix für Namen von Ressourcen, die anhand dieser Vorlage in der aktuellen Region erstellt wurden.

> **Note**
>
> Wenn Sie diese Vorlage mehrmals erstellen, sollten Sie die Parameter für den Bucket-Namen und das Ressourcenpräfix ändern, um Konflikte mit Ressourcennamen zu vermeiden.

5. Wählen Sie Weiter aus.
6. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
7. Aktivieren Sie unten auf der Seite das Kontrollkästchen Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
8. Wählen Sie Stack erstellen aus.

   Das Erstellen des -Stacks nimmt einige Minuten in Anspruch. Wenn der Stack nicht erstellt werden kann, verfügt Ihr Konto möglicherweise über unzureichende Berechtigungen, oder Sie haben einen Bucket-Namen eingegeben, der bereits vorhanden ist. Führen Sie die folgenden Schritte aus, um den Stack zu löschen, und versuchen Sie es erneut:

   a. Wählen Sie Löschen in der oberen rechten Ecke aus.

      Das Löschen des Stacks nimmt einige Minuten in Anspruch.

      > **Note**
      >
      > AWS CloudFormation löscht keine S3-Buckets oder CloudWatch Protokollgruppen. Sie können diese Ressourcen in den Konsolen für diese Services löschen.

   b. Wenn der Stack nicht gelöscht werden kann, wählen Sie erneut Delete (Löschen) .
   c. Wenn der Stack erneut nicht gelöscht werden kann, folgen Sie den Schritten in der AWS CloudFormation Konsole, um die Ressourcen zu überspringen, die nicht gelöscht werden konnten, und versuchen Sie es erneut.
9. Nachdem der AWS CloudFormation Stack erfolgreich erstellt wurde, folgen Sie dem nächsten Verfahren, um Ihre Objektdaten in Amazon S3 zu untersuchen.

> **Important**
>
> Nachdem Sie den Stack erstellt haben, können Sie die neuen Ressourcen in Ihrem AWS Konto sehen. Die Funktion funktioniert möglicherweise nicht mehr ordnungsgemäß, wenn Sie diese Ressourcen löschen oder ändern. Es wird empfohlen, diese Ressourcen nicht zu ändern, es sei denn, Sie möchten das Senden von Daten an den Bucket beenden oder diese Funktion anpassen.

Ihre Daten in Amazon S3 anzeigen

Nachdem Sie die Funktion erstellt haben, können Sie Ihre Objektdaten und Asset-Metadaten in Amazon S3 anzeigen.

> **Note**
>
> Die Asset-Metadaten werden alle sechs Stunden aktualisiert. Möglicherweise müssen Sie bis zu sechs Stunden warten, bis die Asset-Metadaten im S3-Bucket angezeigt werden.

Diese Funktion speichert Komponenteneigenschaftsdaten in den folgenden Spalten, wobei jede Zeile einen Datenpunkt enthält:

- type — Der Typ der Eigenschaftsbenachrichtigung (`PropertyValueUpdate`).
- asset_id — Die ID des Assets, das einen Datenpunkt empfangen hat.
- asset_property_id — Die ID der Immobilie, die einen Datenpunkt für das Asset erhalten hat.
- time_in_seconds — Die Zeit, zu der die Daten empfangen wurden, ausgedrückt in Sekunden in der Unix-Epoche.
- offset_in_nanos — Der Nanosekunden-Offset von. `timeInSeconds`
- asset_property_quality — Die Qualität des Datenpunkts:,, oder. `GOOD` `UNCERTAIN` `BAD`
- asset_property_value — Der Wert des Datenpunkts.
- asset_property_data_type — Der Datentyp der Asset-Eigenschaft:,, oder. `boolean` `double` `integer` `string`

Diese Funktion speichert KomponentenmMetadaten in den folgenden Spalten, wobei jede Zeile eine Komponenteneigenschaft enthält:

- asset_id — Die ID des Assets.
- asset_name — Der Name des Assets.
- asset_model_id — Die ID des Modells des Assets.
- asset_property_id — Die ID der Vermögenseigenschaft.
- asset_property_name — Der Name der Vermögenseigenschaft.
- asset_property_data_type — Der Datentyp der Anlageneigenschaft:,, oder. `BOOLEAN` `DOUBLE` `INTEGER` `STRING`
- asset_property_unit — Die Einheit der Anlageeigenschaft.
- asset_property_alias — Der Alias der Vermögenseigenschaft.

So zeigen Sie Ihre AWS IoT SiteWise Daten in Amazon S3 an

1. Navigieren Sie zur Amazon S3 S3-Konsole.
2. Wählen Sie aus der Liste der Buckets den Bucket mit dem Namen aus, den Sie beim Erstellen der Vorlage ausgewählt haben.
3. Wählen Sie in dem Bucket einen der folgenden Ordner aus:
   - `asset-property-updates`— Dieser Ordner enthält Objektdaten, aus denen exportiert wurde AWS IoT SiteWise.
   - `asset-metadata`— Dieser Ordner enthält Asset-Details, aus denen exportiert wurde AWS IoT SiteWise.
4. Wählen Sie das Objekt aus, das Sie anzeigen möchten.
5. Führen Sie auf der Seite des Objekts die folgenden Schritte aus:
   a. Wählen Sie die Registerkarte Select from (Auswählen aus) .

      In diesem Fenster können Sie eine Vorschau von Datensätzen aus Parquet-Dateien anzeigen.

   b. Wählen Sie für File format (Dateiformat) Parquet.

   c. Um den Inhalt der Datei im JSON-Format anzuzeigen, wählen Sie Dateivorschau anzeigen.

> **Note**
>
> Wenn keine neuen Daten in dem Bucket angezeigt werden, überprüfen Sie, ob Sie die Benachrichtigungen zur Aktualisierung von Eigenschaftenwerten für Ihre Komponenteneigenschaften aktiviert haben. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten.

Weitere Informationen zum Analysieren der im S3-Bucket gespeicherten Komponentendaten finden Sie unter Analysieren Sie die exportierten Daten mit Amazon Athena.

Analysieren Sie die exportierten Daten mit Amazon Athena

Nachdem Sie Ihre Objektdaten in Amazon S3 gespeichert haben, können Sie verschiedene AWS Dienste verwenden, um Berichte zu erstellen oder Ihre Daten zu analysieren und abzufragen:

- Führen Sie mit Amazon Athena SQL-Abfragen für Ihre Daten aus.
- Führen Sie Big-Data-Analysen mit Amazon EMR durch.
- Suchen und analysieren Sie Ihre Daten mit Amazon OpenSearch Service.

Weitere AWS Dienste, die mit Ihren Daten in Amazon S3 interagieren können, finden Sie unter Analytics in der AWS Management Console.

> **Note**
>
> Der Stack erstellt eine AWS Glue Datenbank zur Formatierung von Objektdaten. Sie können diese Datenbank nicht nach Komponentendaten abfragen. Folgen Sie den Schritten in diesem Abschnitt, um eine AWS Glue Datenbank zu erstellen, die Sie abfragen können.

In diesem Tutorial erfahren Sie, wie Sie die Voraussetzungen für die Verwendung von Amazon Athena konfigurieren und wie Sie Athena verwenden, um SQL-Abfragen für Ihre exportierten AWS IoT SiteWise Asset-Daten auszuführen. Um Daten mit Athena abzufragen, müssen Sie die zuerst AWS Glue Data Catalog mit Ihren Asset-Daten füllen. Der Datenkatalog enthält Datenbanken und Tabellen, und Athena kann auf Daten im Datenkatalog zugreifen. Sie können einen AWS Glue Crawler erstellen, der den Datenkatalog regelmäßig mit Ihren exportierten Asset-Daten aktualisiert.

Themen

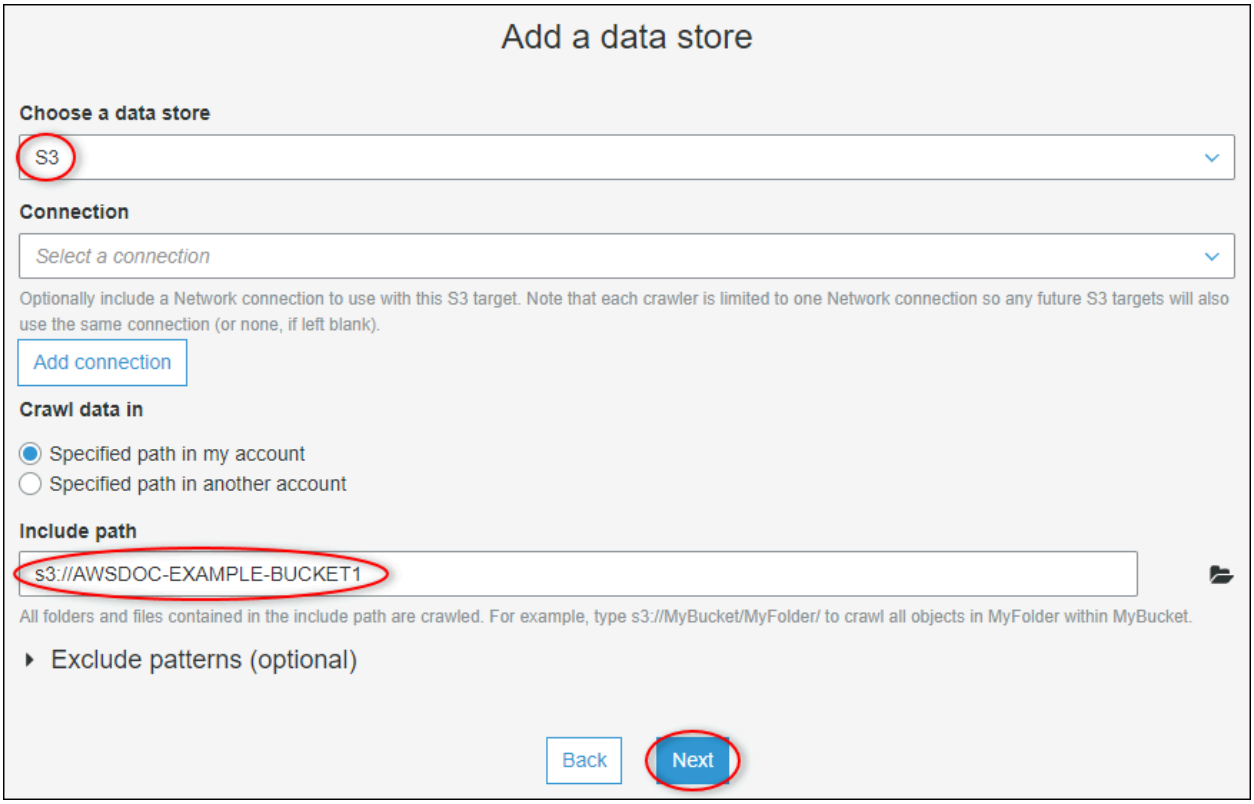
- Konfigurieren eines Crawlers zum Auffüllen der AWS Glue Data Catalog
- Daten mit Athena abfragen

Konfigurieren eines Crawlers zum Auffüllen der AWS Glue Data Catalog

AWS Glue Crawler durchsuchen Datenspeicher, um Tabellen in der zu füllen. AWS Glue Data Catalog In diesem Verfahren erstellen und führen Sie einen AWS Glue Crawler für Ihren S3-Bucket aus, der exportierte Asset-Daten enthält. Der Crawler erstellt eine Tabelle für Aktualisierungen von Komponenteneigenschaften und eine Tabelle für Komponentenmetadaten. Anschließend können Sie mit Athena SQL-Abfragen für diese Tabellen durchführen. Weitere Informationen finden Sie unter Auffüllen der Crawler AWS Glue Data Catalog und Definieren von Crawlern im AWS Glue Entwicklerhandbuch.

So erstellen Sie einen Crawler AWS Glue

1. Navigieren Sie zur AWS Glue -Konsole.
2. Wählen Sie im Navigationsbereich Crawlers (Crawler) aus.
3. Wählen Sie Add crawler (Crawler hinzufügen).
4. Führen Sie auf der Seite Add crawler (Crawler hinzufügen) die folgenden Schritte aus:
    a. Geben Sie einen Namen für den Crawler ein, z. B. **`IoTSiteWiseDataCrawler`**, und wählen Sie dann Next (Weiter).
    b. Wählen Sie in Crawler source type (Crawler-Quelltyp) die Option Data stores (Datenspeicher) und anschließend Next (Weiter) aus.
    c. Führen Sie auf der Seite Add a data store (Datenspeicher hinzufügen die folgenden Schritte aus:
        i. Wählen Sie in Choose a data store (Datenspeicher auswählen) die Option S3 aus.
        ii. Geben Sie Include path (Pfad einschließen) **`s3://DOC-EXAMPLE-BUCKET1`** ein, um den Komponentendaten-Bucket als Datenspeicher hinzuzufügen. Ersetzen Sie DOC-EXAMPLE-BUCKET1 durch den Bucket-Namen, den Sie bei der Erstellung des Stacks ausgewählt haben.
        iii. Wählen Sie Weiter aus.



d. Wählen Sie auf der Seite Add another data store (Einen weiteren Datenspeicher hinzufügen) die Option No (Nein) und anschließend Next (Weiter) aus.

e. Gehen Sie auf der Seite „IAM-Rolle auswählen“ wie folgt vor:

   i. Um eine neue Servicerolle zu erstellen, die den AWS Glue Zugriff auf den S3-Bucket ermöglicht, wählen Sie Create an IAM-Rolle.

   ii. Geben Sie ein Suffix für den Namen Ihrer Rolle ein, z. B. **`IoTSiteWiseDataCrawler`**.

   iii. Wählen Sie Weiter aus.

f. Wählen Sie in Frequency (Häufigkeit) die Option Hourly (Stündlich) und anschließend Next (Weiter) aus. Der Crawler aktualisiert die Tabellen bei jeder Ausführung mit neuen Daten, sodass Sie eine beliebige Häufigkeit genau für Ihren Anwendungsfall auswählen können.

g. Führen Sie auf der Seite Configure the crawler's output (Crawler-Ausgabe konfigurieren) die folgenden Schritte aus:

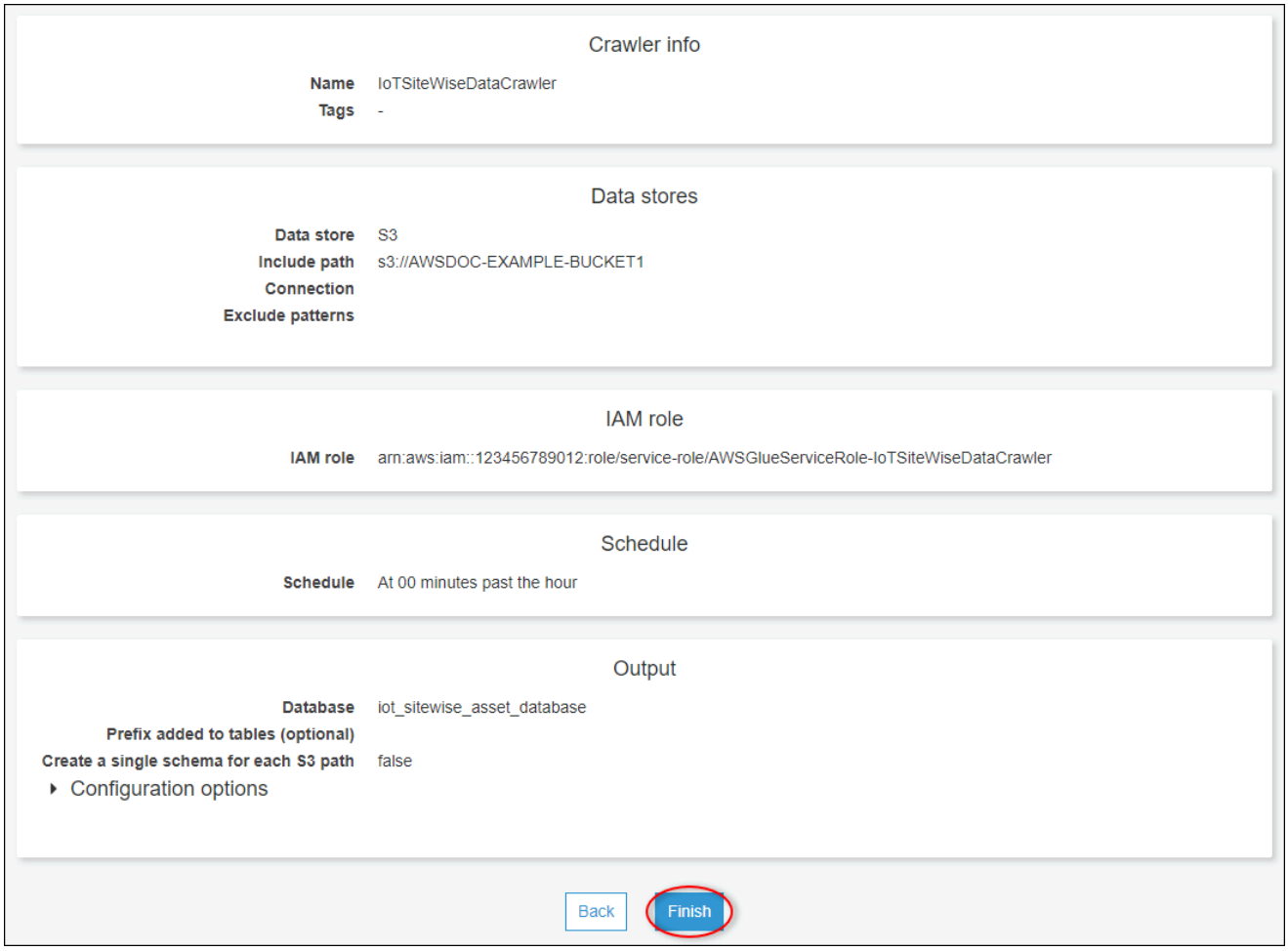
   i. Wählen Sie Datenbank hinzufügen, um eine AWS Glue Datenbank für Ihre Asset-Daten zu erstellen.

   ii. Geben Sie einen Namen für die Datenbank ein, z. B. **`iot_sitewise_asset_database`**.

iii. Wählen Sie Erstellen.

iv. Wählen Sie Weiter aus.

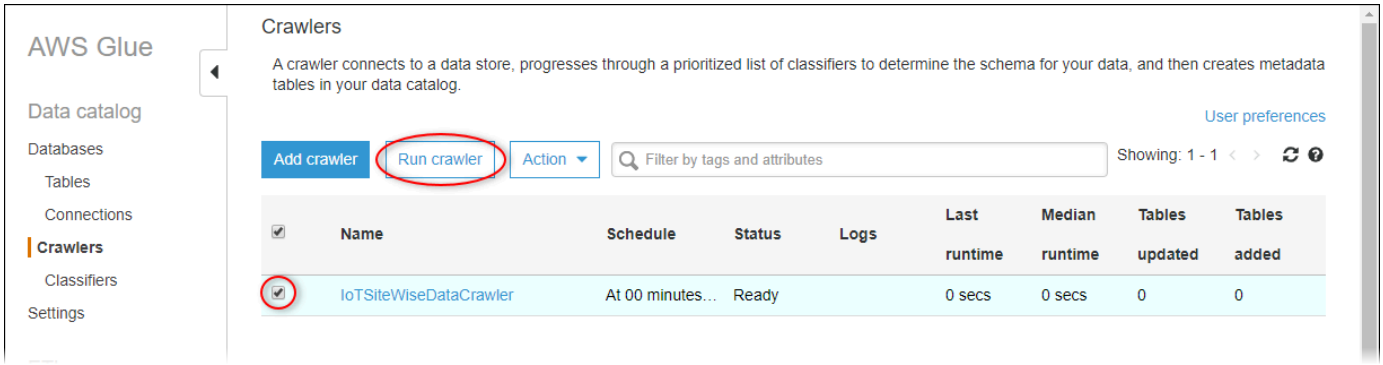
h. Überprüfen Sie die Crawler-Details, und wählen Sie dann Finish (Fertig stellen).



Der neue Crawler wird standardmäßig nicht sofort ausgeführt. Sie müssen ihn manuell ausführen oder warten, bis der Crawler nach dem konfigurierten Zeitplan ausgeführt wird.

So führen Sie einen Crawler aus

1. Aktivieren Sie auf der Seite Crawler das Kontrollkästchen für den neuen Crawler und wählen Sie anschließend Run Crawler (Crawler ausführen) aus.



2. Warten Sie, bis der Crawler die Startsequenz beendet und den Status Ready (Bereit) hat.

   Das Starten des Crawlers kann mehrere Minuten dauern, und sein Status wird automatisch aktualisiert.

3. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.

   Sie sollten zwei neue Tabellen sehen: asset_metadata und asset_property_updates.

Daten mit Athena abfragen

Athena entdeckt automatisch Ihre Asset-Datentabellen in der. AWS Glue Data Catalog Um Abfragen über Schnittmengen dieser Tabellen durchzuführen, können Sie eine Ansicht erstellen, also eine logische Datentabelle. Weitere Informationen finden Sie unter Arbeiten mit Ansichten im Amazon Athena Athena-Benutzerhandbuch.

Nachdem Sie eine Ansicht mit Komponenteneigenschaftsdaten und Metadaten erstellt haben, können Sie Abfragen ausführen, die Eigenschaftswerte mit angefügten Komponenten- und Eigenschaftsnamen ausgeben. Weitere Informationen finden Sie unter Ausführen von SQL-Abfragen mit Amazon Athena im Amazon Athena Athena-Benutzerhandbuch.

Um Asset-Daten mit Athena abzufragen

1. Navigieren Sie zur Athena-Konsole.

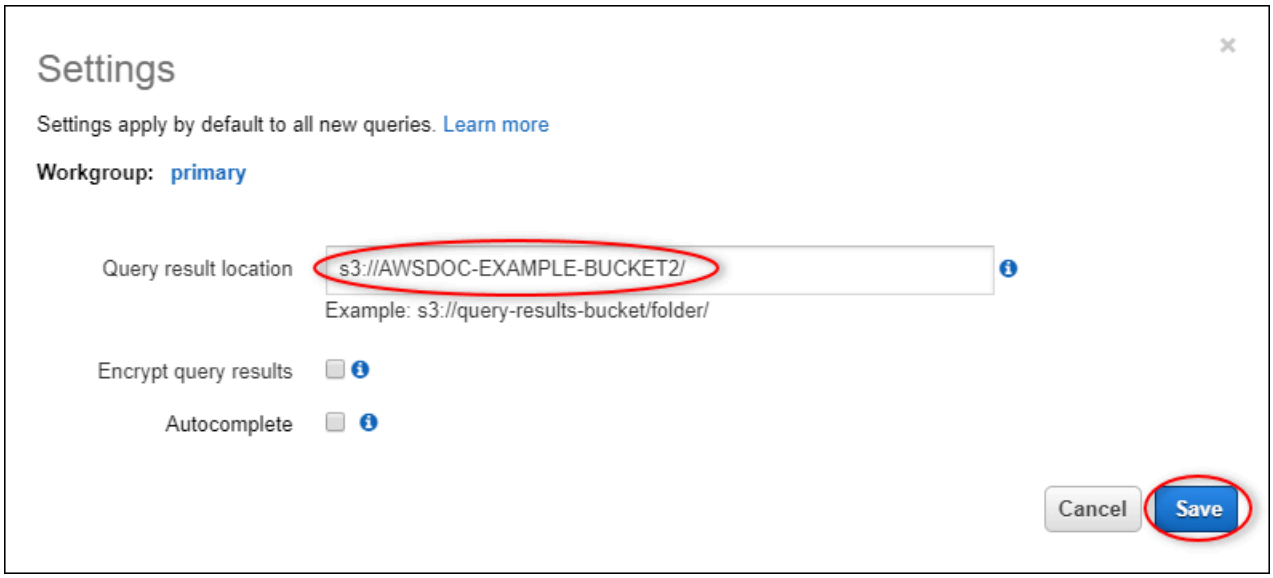
   Wenn die Seite Getting started (Erste Schritte) angezeigt wird, wählen Sie Getting started (Erste Schritte) aus.

2. Wenn Sie Athena zum ersten Mal verwenden, führen Sie die folgenden Schritte aus, um einen S3-Bucket für Abfrageergebnisse zu konfigurieren. Athena speichert die Ergebnisse Ihrer Abfragen in diesem Bucket.

> **Important**
>
> Verwenden Sie einen anderen Bucket als Ihren Komponentendaten-Bucket, damit der Crawler, den Sie zuvor erstellt haben, keine Abfrageergebnisse durchforstet. Wir empfehlen, dass Sie einen Bucket erstellen, der nur für Athena-Abfrageergebnisse verwendet wird. Weitere Informationen finden Sie unter Wie erstelle ich einen S3-Bucket? im Amazon Simple Storage Service-Benutzerhandbuch.

a. Wählen Sie Settings (Einstellungen) aus.

b. Geben Sie im Feld Speicherort der Abfrageergebnisse den S3-Bucket für Athena-Abfrageergebnisse ein. Der Bucket muss mit / enden.

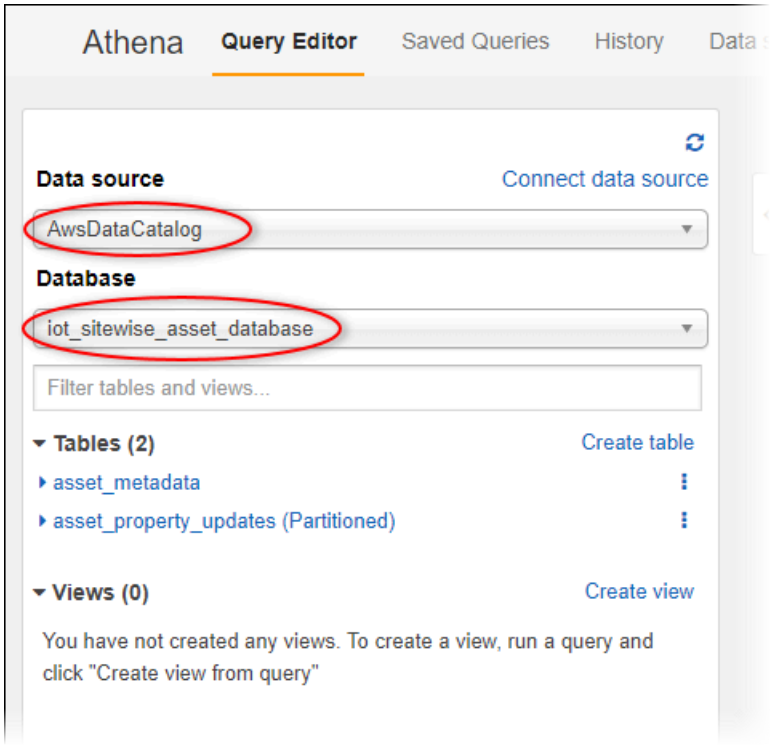


c. Wählen Sie Speichern.

3. Der linke Bereich enthält die Datenquelle, die abgefragt werden soll. Gehen Sie wie folgt vor:

a. Wählen Sie als Datenquelle AwsDataCatalogdie AWS Glue Data Catalog Verwendung von.

b. Wählen Sie für Datenbank die AWS Glue Datenbank aus, die Sie mit dem Crawler erstellt haben.



Sie sollten zwei Tabellen sehen: asset_metadata und asset_property_updates.

4. Um eine kombinierte Ansicht der Komponenteneigenschaftsdaten und der Metadaten zu erstellen, geben Sie die folgende Abfrage ein, und wählen Sie dann Run query (Abfrage ausführen)aus.

```
CREATE
        OR REPLACE VIEW iot_sitewise_asset_data AS
SELECT "from_unixtime"("time_in_seconds" + ("offset_in_nanos" / 1000000000))
 "timestamp",
         "metadata"."asset_name",
         "metadata"."asset_property_name",
         "data"."asset_property_value",
         "metadata"."asset_property_unit",
         "metadata"."asset_property_alias"
FROM ( "iot_sitewise_asset_database".asset_property_updates data
INNER JOIN "iot_sitewise_asset_database".asset_metadata metadata
    ON ( ("data"."asset_id" = "metadata"."asset_id")
        AND ("data"."asset_property_id" = "metadata"."asset_property_id") ) );
```

Diese Abfrage erstellt eine Ansicht, in dem ein Join der Komponentendateneigenschaftsdaten und der Metadatentabellen über die Komponenten-ID und Eigenschaften-ID durchgeführt wird.

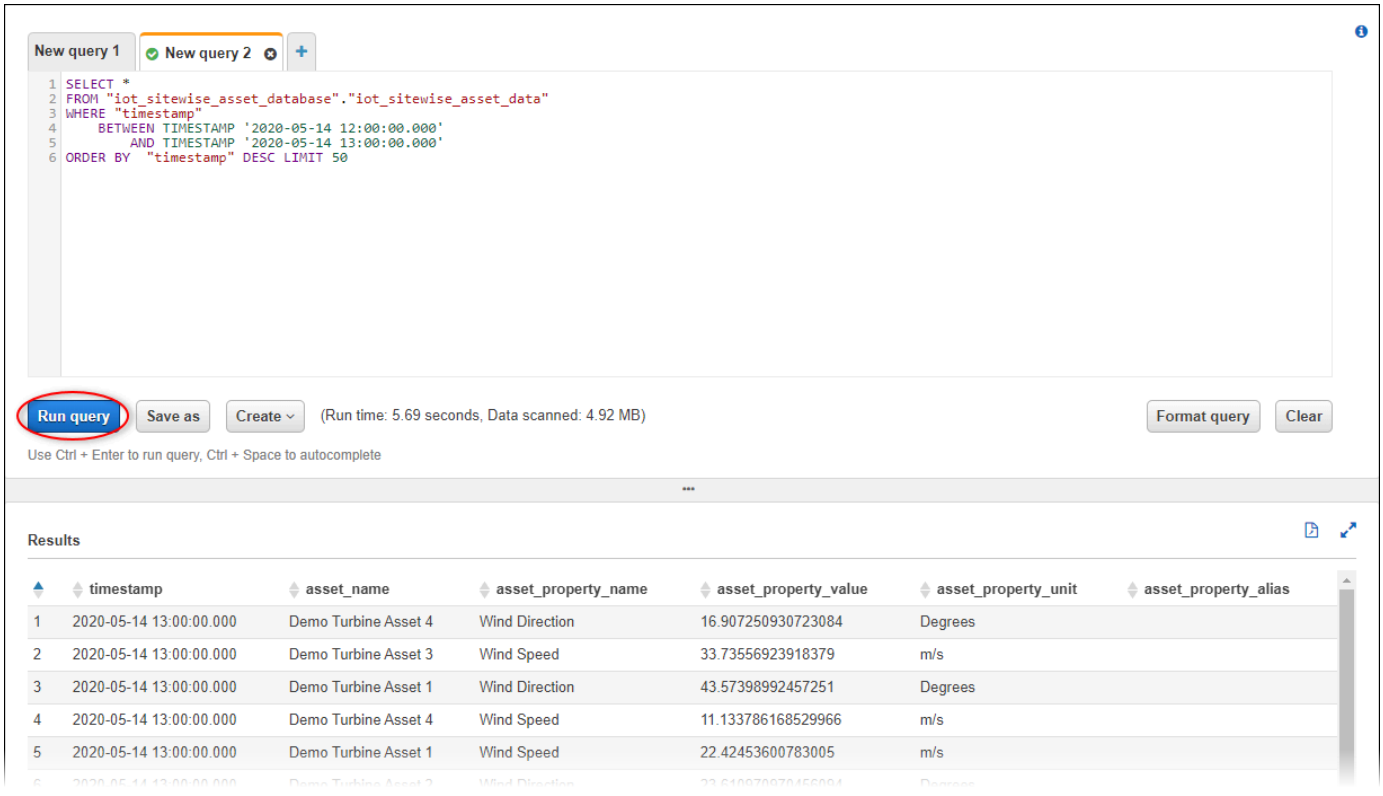
Sie können diese Abfrage mehrmals ausführen, da sie eine ggf. bereits vorhandene Ansicht ersetzt.

5. Um eine neue Abfrage hinzuzufügen, wählen Sie das +-Symbol.
6. Um ein Beispiel für Komponentendaten anzuzeigen, geben Sie die folgende Abfrage ein und wählen anschließend Run query (Abfrage ausführen) aus. Ersetzen Sie die Zeitstempel durch ein Intervall, für das Ihr Bucket Daten enthält.

```
SELECT *
FROM "iot_sitewise_asset_database"."iot_sitewise_asset_data"
WHERE "timestamp"
    BETWEEN TIMESTAMP '2020-05-14 12:00:00.000'
        AND TIMESTAMP '2020-05-14 13:00:00.000'
ORDER BY  "timestamp" DESC LIMIT 50;
```

Diese Abfrage gibt bis zu 50 Datenpunkte zwischen zwei Zeitstempeln aus, wobei die letzten Einträge zuerst angezeigt werden.

Ihre Abfrageausgabe könnte den folgenden Ergebnissen ähnlich aussehen.



Sie können jetzt Abfragen ausführen, die für Ihre AWS IoT SiteWise Anwendung nützlich sind. Weitere Informationen finden Sie unter SQL-Referenz für Amazon Athena im Amazon Athena Athena-Benutzerhandbuch.

Ressourcen, die aus der Vorlage erstellt wurden

Wenn Sie einen Stapel aus der Vorlage erstellen, werden die folgenden Ressourcen AWS CloudFormation erstellt. Die Namen der meisten Ressourcen enthalten ein Präfix, das Sie beim Erstellen des Stacks anpassen können.

Ressourcennamen-Parameter

- `BucketName`— Der Name des S3-Buckets, der anhand dieser Vorlage erstellt wurde und Asset-Daten empfängt.
- `GlobalResourcePrefix`— Ein Präfix für Namen globaler Ressourcen, die anhand dieser Vorlage erstellt wurden. Standardeinstellung: `sitewise-export-to-s3`.
- `LocalResourcePrefix`— Ein Präfix für Namen von Ressourcen, die anhand dieser Vorlage in der aktuellen Region erstellt wurden. Standardeinstellung: `sitewise_export_to_s3`.

Mit der AWS CloudFormation Vorlage erstellte Ressourcen

Ressource	Beschreibung	Name
S3-Bucket für verarbeitete Daten	Dieser Bucket enthält zwei Ordner. Ein Ordner empfängt die reduzierten, formatierten Daten aus dem Firehose-Lieferstream, und der andere Ordner empfängt Asset-Met adaten.	`${BucketName}`
AWS Glue-Datenbank	Diese Datenbank enthält die AWS Glue Tabelle, die dieser Stapel erstellt.	`${LocalResourcePrefix}_firehose_glue_database`
AWS Glue-Tabelle	Der Firehose-Lieferstream verwendet diese Tabelle, um	`${LocalResourcePrefix}_firehose_glue_table`

Ressource	Beschreibung	Name
	Daten im Parquet-Format zu formatieren.	
AWS Lambda Funktion, die Daten transformiert	Diese Funktion reduziert das Wertearray in Benachrichtigungen über Eigenschaftswerte, die von gesendet werden. AWS IoT SiteWise	`${LocalResourcePrefix}_lambda_transform_function`
IAM-Rolle für die Lambda-Funktion Transform	Diese Rolle ermöglicht es Lambda, Laufzeitprotokolle für die Transformationsfunktion zu speichern.	`${GlobalResourcePrefix}-lambda-transform-role`
IAM-Richtlinie für die Lambda-Funktionsrolle „Transform“	Diese Richtlinie ermöglicht es Lambda, Ausführungsprotokolle für die Transformationsfunktion zu speichern.	`${GlobalResourcePrefix}-lambda-transform-policy`
CloudWatch Logs, Protokollgruppe für die Transformationsfunktion	Diese Protokollgruppe enthält Protokolle für die Transformationsfunktion.	`/aws/lambda/${LocalResourcePrefix}_lambda_transform_function`
Lambda-Funktion, die Asset-Metadaten sammelt	Diese Funktion ruft Details zu Assets in einem Amazon S3-Bucket ab AWS IoT SiteWise und speichert die Details in einem Amazon S3 S3-Bucket, den dieser Stack erstellt.	`${LocalResourcePrefix}_lambda_metadata_function`
Lambda-Schicht für die Metadatenfunktion	Diese Ebene stellt ein AWS SDK bereit, das AWS IoT SiteWise Operationen enthält, die von der Metadatenfunktion verwendet werden.	`${LocalResourcePrefix}_lambda_metadata_layer`

Ressource	Beschreibung	Name
IAM-Rolle für die Metadaten-Lambda-Funktion	Diese Rolle ermöglicht es Lambda, Details zu Assets in AWS IoT SiteWise abzurufen.	`${GlobalResourcePrefix}-lambda-metadata-role`
IAM-Richtlinie für die Lambda-Funktionsrolle für Metadaten	Diese Richtlinie ermöglicht es Lambda, Details zu Vermögenswerten in AWS IoT SiteWise abzurufen.	`${GlobalResourcePrefix}-lambda-metadata-policy`
EventBridgegeplantes Ereignis für die Metadaten-Lambda-Funktion	Dieses geplante Ereignis führt das Metadaten-Lambda alle 6 Stunden aus, um den Asset-Metadaten-Bucket zu aktualisieren.	`${LocalResourcePrefix}-metadata-event`
CloudWatch Protokolliert die Protokollgruppe für die Metadatenfunktion	Diese Protokollgruppe enthält Protokolle für die Metadatenfunktion.	`/aws/lambda/${LocalResourcePrefix}_lambda_metadata_function`
AWS IoT Regel	Diese Regel fragt Benachrichtigungen über Immobilienwerte ab und sendet Asset-Daten an einen Amazon Data Firehose-Lieferstream.	`${LocalResourcePrefix}_iot_topic_rule`
IAM-Rolle für die Regel AWS IoT	Diese Rolle ermöglicht AWS IoT das Senden von Daten an den Firehose-Lieferstream.	`${GlobalResourcePrefix}-core-firehose-role`
IAM-Richtlinie für die Regelrolle AWS IoT	Diese Richtlinie ermöglicht AWS IoT das Senden von Daten an den Firehose-Lieferstream.	`${GlobalResourcePrefix}-core-firehose-policy`

Ressource	Beschreibung	Name
Firehose-Lieferstrom	Dieser Lieferstream verwendet Daten aus der AWS IoT Regel, glättet die Daten mit einer Lambda-Funktion und übermittelt die Daten an Amazon S3.	`${LocalResourcePrefix}_firehose_delivery_stream`
IAM-Rolle für den Lieferstream	Diese Rolle ermöglicht es Firehose, Operationen mit dem S3-Bucket, der AWS Glue Tabelle, den Lambda-Funktionen und der CloudWatch Logs-Protokollgruppe durchzuführen.	`${GlobalResourcePrefix}-firehose-delivery-role`
CloudWatch Logs, Protokollgruppe für den Lieferstream	Diese Protokollgruppe enthält einen Protokollstream,`S3 Delivery`, der Protokolle über den Firehose-Lieferstream empfängt.	`/aws/kinesisfirehose/${LocalResourcePrefix}_firehose_delivery_stream`

Integration in Grafana

Grafana ist eine Datenvisualisierungsplattform, mit der Sie Daten in Dashboards visualisieren und überwachen können. In Grafana Version 7.3.0 und höher können Sie das AWS IoT SiteWise Plugin verwenden, um Ihre AWS IoT SiteWise Komponentendaten in Grafana-Dashboards zu visualisieren. Sie können Daten aus mehreren AWS Quellen (wie AWS IoT SiteWise, Amazon Timestream und Amazon CloudWatch) und anderen Datenquellen mit einem einzigen Grafana-Dashboard visualisieren.

Sie haben zwei Möglichkeiten, das AWS IoT SiteWise Plugin zu verwenden:

- Lokale Grafana-Server

Sie können das AWS IoT SiteWise Plugin auf einem von Ihnen verwalteten Grafana-Server einrichten. Weitere Informationen zum Hinzufügen und Verwenden des Plugins finden Sie in der AWS IoT SiteWise Datasource-README-Datei auf der - GitHub Website.

- AWS Managed Service für Grafana

  Sie können das AWS IoT SiteWise Plugin im AWS Managed Service for Grafana (AMG) verwenden. verwaltet Grafana-Server für Sie, sodass Sie Ihre Daten visualisieren können, ohne Hardware oder eine andere Grafana-Infrastruktur erstellen, verpacken oder bereitstellen zu müssen. Weitere Informationen finden Sie in den folgenden Themen im AWS Benutzerhandbuch zu Managed Service für Grafana:

  - Was ist Amazon Managed Service for Grafana (AMG)?
  - Verwenden der AWS IoT SiteWise Datenquelle

Example Beispiel für ein Grafana-Dashboard

Das folgende Grafana-Dashboard visualisiert die Demo-Vorkommensfarm . Sie können auf dieses Demo-Dashboard auf der Grafana Play-Website zugreifen.

Integration von AWS IoT SiteWise und AWS IoT TwinMaker

Durch die Integration mit AWS IoT TwinMaker wird Zugriff auf robuste Funktionen in gewährtAWS IoT SiteWise, z. B. AWS IoT SiteWise Datenabruf`ExecuteQuery`-API und erweiterte Komponentensuche in der -AWS IoT SiteWiseKonsole. Um die Services zu integrieren und diese Funktionen zu nutzen, müssen Sie zuerst die Integration aktivieren.

Themen

- Aktivierung der Integration
- Integration von AWS IoT SiteWise und AWS IoT TwinMaker

Aktivierung der Integration

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen. Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Weitere Informationen zu AWS IoT SiteWise unterstützten Aktionen finden Sie unter Von definierte Aktionen AWS IoT SiteWise in der Service-Autorisierungs-Referenz.

Weitere Informationen zur AWS IoT TwinMaker serviceverknüpften Rolle finden Sie unter Serviceverknüpfte Rollen für AWS IoT TwinMaker im AWS IoT TwinMaker -Benutzerhandbuch.

Bevor Sie AWS IoT SiteWise und integrieren könnenAWS IoT TwinMaker, müssen Sie die folgenden Berechtigungen erteilen, die AWS IoT SiteWise die Integration in einen AWS IoT TwinMaker verknüpften Workspace ermöglichen:

- `iotsitewise:EnableSiteWiseIntegration` – Ermöglicht AWS IoT SiteWise die Integration in einen verknüpften AWS IoT TwinMaker Workspace. Diese Integration ermöglicht es AWS IoT TwinMaker, alle Ihre Modellierungsinformationen in AWS IoT SiteWise über eine AWS IoT TwinMaker serviceverknüpfte Rolle zu lesen. Um diese Berechtigung zu aktivieren, fügen Sie Ihrer IAM-Rolle die folgende Richtlinie hinzu:

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

Integration von AWS IoT SiteWise und AWS IoT TwinMaker

Um AWS IoT SiteWise und zu integrierenAWS IoT TwinMaker, benötigen Sie Folgendes:

- AWS IoT SiteWise -serviceverknüpfte Rolle, die in Ihrem Konto eingerichtet wurde

- AWS IoT TwinMaker -serviceverknüpfte Rolle, die in Ihrem Konto eingerichtet wurde
- AWS IoT TwinMaker Workspace mit der ID `IoTSiteWiseDefaultWorkspace` in Ihrem Konto in der Region.

So integrieren Sie mithilfe der AWS IoT SiteWise Konsole

Wenn Sie das Banner Integration mit AWS IoT TwinMaker in der Konsole sehen, wählen Sie Berechtigung erteilen aus. Die Voraussetzungen werden in Ihrem Konto erstellt.

So integrieren Sie mithilfe der AWS CLI

Um AWS IoT SiteWise und AWS IoT TwinMaker mithilfe der zu integrierenAWS CLI, geben Sie die folgenden Befehle ein:

1. Rufen Sie `CreateServiceLinkedRole` mit einem `AWSServiceName` von auf`iotsitewise.amazonaws.com`.

   ```
   aws iam create-service-linked-role --aws-service-name iotsitewise.amazonaws.com
   ```

2. Rufen Sie `CreateServiceLinkedRole` mit einem `AWSServiceName` von auf `iottwinmaker.amazonaws.com`.

   ```
   aws iam create-service-linked-role --aws-service-name iottwinmaker.amazonaws.com
   ```

3. Rufen Sie `CreateWorkspace` mit einem `ID` von auf`IoTSiteWiseDefaultWorkspace`.

   ```
   aws iottwinmaker create-workspace --workspace-id IoTSiteWiseDefaultWorkspace
   ```

Erkennung von Geräteanomalien mit Amazon Lookout for Equipment

> **Note**
>
> Die Erkennung von Anomalien ist nur in den Regionen verfügbar, in denen Amazon Lookout for Equipment verfügbar ist.

Sie können Amazon Lookout for Equipment integrieren AWS IoT SiteWise , um mithilfe von Anomalieerkennung und vorausschauender Wartung von Industrieanlagen Einblicke in Ihre Industrieanlagen zu gewinnen. Lookout for Equipment ist ein Service für maschinelles Lernen (ML) zur Überwachung von Industrieanlagen, der abnormales Geräteverhalten erkennt und potenzielle Ausfälle identifiziert. Mit Lookout for Equipment können Sie prädiktive Wartungsprogramme implementieren und suboptimale Geräteprozesse identifizieren. Weitere Informationen zu Lookout for Equipment finden Sie unter Was ist Amazon Lookout for Equipment? im Amazon Lookout for Equipment Equipment-Benutzerhandbuch.

Wenn Sie eine Prognose erstellen, um ein ML-Modell zu trainieren, um anomales Geräteverhalten zu erkennen, AWS IoT SiteWise sendet es die Werte der Anlageneigenschaften an Lookout for Equipment, um ein ML-Modell zur Erkennung von anomalem Geräteverhalten zu trainieren. Um eine Prognosedefinition für ein Asset-Modell zu definieren, geben Sie die IAM-Rollen an, die Lookout for Equipment benötigt, um auf Ihre Daten zuzugreifen, und die Eigenschaften, die an Lookout for Equipment gesendet und verarbeitete Daten an Amazon S3 gesendet werden sollen. Weitere Informationen finden Sie unter Erstellen von Komponentenmodellen.

Um Lookout for Equipment zu integrieren AWS IoT SiteWise und Lookout for Equipment zu integrieren, führen Sie die folgenden allgemeinen Schritte aus:

- Fügen Sie einem Asset-Modell eine Prognosedefinition hinzu, die beschreibt, welche Eigenschaften Sie verfolgen möchten. Die Vorhersagedefinition ist eine wiederverwendbare Sammlung von Messungen, Transformationen und Metriken, die verwendet wird, um Vorhersagen für die Anlagen zu erstellen, die auf diesem Anlagenmodell basieren.
- Trainieren Sie die Vorhersage auf der Grundlage der von Ihnen bereitgestellten historischen Daten.
- Planen Sie Inferenz, die angibt, AWS IoT SiteWise wie oft eine bestimmte Vorhersage ausgeführt werden soll.

Sobald die Inferenz geplant ist, überwacht das Modell Lookout for Equipment die Daten, die es von Ihren Geräten empfängt, und sucht nach Anomalien im Geräteverhalten. Sie können die Ergebnisse in SiteWise Monitor mithilfe der AWS IoT SiteWise GET-API-Operationen oder der Lookout for Equipment Equipment-Konsole anzeigen und analysieren. Sie können auch Alarme mithilfe von Alarmmeldern aus dem Anlagenmodell erstellen, um Sie über abnormales Geräteverhalten zu informieren.

Themen

- Hinzufügen einer Vorhersagedefinition (Konsole)

- Eine Vorhersage trainieren (Konsole)
- Inferenz für eine Vorhersage starten oder beenden (Konsole)
- Hinzufügen einer Vorhersagedefinition (CLI)
- Eine Vorhersage trainieren und Inferenz starten (CLI)
- Eine Vorhersage trainieren (CLI)
- Inferenz aus einer Vorhersage starten oder beenden (CLI)

Hinzufügen einer Vorhersagedefinition (Konsole)

Um mit dem Senden der von gesammelten Daten AWS IoT SiteWise an Lookout for Equipment zu beginnen, müssen Sie einem Anlagenmodell eine AWS IoT SiteWise Prognosedefinition hinzufügen.

Um einem AWS IoT SiteWise Anlagenmodell eine Vorhersagedefinition hinzuzufügen

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Modelle und dann das Assetmodell aus, dem Sie die Vorhersagedefinition hinzufügen möchten.
3. Wählen Sie Prognosen aus.
4. Wählen Sie Vorhersagedefinition hinzufügen.
5. Definieren Sie Details zur Vorhersagedefinition.

    a. Geben Sie einen eindeutigen Namen und eine Beschreibung für Ihre Prognosedefinition ein. Wählen Sie den Namen sorgfältig aus, da Sie den Namen der Vorhersagedefinition nicht mehr ändern können, nachdem Sie sie erstellt haben.

    b. Erstellen oder wählen Sie eine IAM-Berechtigungsrolle aus, die es AWS IoT SiteWise ermöglicht, Ihre Asset-Daten mit Amazon Lookout for Equipment zu teilen. Die Rolle sollte die folgenden IAM- und Vertrauensrichtlinien haben. Hilfe zum Erstellen der Rolle finden Sie unter Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole).

    IAM-Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "L4EPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "lookoutequipment:CreateDataset",
                "lookoutequipment:CreateModel",
                "lookoutequipment:CreateInferenceScheduler",
                "lookoutequipment:DescribeDataset",
                "lookoutequipment:DescribeModel",
                "lookoutequipment:DescribeInferenceScheduler",
                "lookoutequipment:ListInferenceExecutions",
                "lookoutequipment:StartDataIngestionJob",
                "lookoutequipment:StartInferenceScheduler",
                "lookoutequipment:UpdateInferenceScheduler",
                "lookoutequipment:StopInferenceScheduler"
            ],
            "Resource": [
                "arn:aws:lookoutequipment:Region:Account_ID:inference-
scheduler/IoTSiteWise_*",
                "arn:aws:lookoutequipment:Region:Account_ID:model/
IoTSiteWise_*",
                "arn:aws:lookoutequipment:Region:Account_ID:dataset/
IoTSiteWise_*"
            ]
        },
        {
            "Sid": "L4EPermissions2",
            "Effect": "Allow",
            "Action": [
                "lookoutequipment:DescribeDataIngestionJob"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": ["arn:aws:s3:::iotsitewise-*"]
        },
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::Account_ID:role/Role_name"
        }
    ]
}
```

Vertrauensrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Principal": {
                "Service": "iotsitewise.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "Account_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:iotsitewise:Region:Account_ID:asset/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lookoutequipment.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "Account_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:lookoutequipment:Region:Account_ID:*"
                }
            }
```

```
        }
    ]
}
```

c. Wählen Sie Weiter aus.

6. Wählen Sie Datenattribute (Messungen, Transformationen und Metriken) aus, die Sie an Lookout for Equipment senden möchten.

   a. (Optional) Wählen Sie Messungen aus.

   b. (Optional) Wählen Sie Transformationen aus.

   c. (Optional) Wählen Sie Metriken aus.

   d. Wählen Sie Weiter aus.

7. Überprüfen Sie Ihre Auswahl. Um die Prognosedefinition zum Asset-Modell hinzuzufügen, wählen Sie auf der Übersichtsseite die Option Vorhersagedefinition hinzufügen aus.

Sie können auch eine bestehende Vorhersagedefinition bearbeiten oder löschen, der aktive Vorhersagen angehängt sind.

Eine Vorhersage trainieren (Konsole)

Nachdem Sie einem Anlagenmodell eine Prognosedefinition hinzugefügt haben, können Sie die Vorhersagen trainieren, die sich auf Ihre Anlagen beziehen.

Um eine Vorhersage zu trainieren in AWS IoT SiteWise

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Assets und dann das Asset aus, das Sie überwachen möchten.
3. Wählen Sie Prognosen aus.
4. Wählen Sie die Vorhersagen aus, die Sie trainieren möchten.
5. Wählen Sie unter Aktionen die Option Training starten aus und gehen Sie wie folgt vor:

   a. Wählen Sie unter Prognosedetails eine IAM-Berechtigungsrolle aus, mit der Sie Ihre Asset-Daten mit Lookout for Equipment teilen können AWS IoT SiteWise . Wenn Sie eine neue Rolle erstellen müssen, wählen Sie Neue Rolle erstellen aus.

   b. Geben Sie unter Einstellungen für Trainingsdaten einen Zeitraum für Trainingsdaten ein, um auszuwählen, welche Daten zum Trainieren der Vorhersage verwendet werden sollen.

c. (Optional) Wählen Sie die Samplerate für die Daten nach der Nachverarbeitung aus.

d. (Optional) Geben Sie für Datenlabels einen Amazon S3 S3-Bucket und ein Präfix an, das Ihre Kennzeichnungsdaten enthält. Weitere Informationen zur Kennzeichnung von Daten finden Sie unter Kennzeichnen Ihrer Daten im Amazon Lookout for Equipment Equipment-Benutzerhandbuch.

e. Wählen Sie Weiter aus.

6. (Optional) Wenn Sie möchten, dass die Vorhersage aktiv ist, sobald das Training abgeschlossen ist, wählen Sie unter Erweiterte Einstellungen die Option Vorhersage nach dem Training automatisch aktivieren aus, und gehen Sie dann wie folgt vor:

   a. Definieren Sie unter Eingabedaten für Häufigkeit des Daten-Uploads, wie oft Daten hochgeladen werden, und definieren Sie für Offset-Verzögerungszeit, wie viel Puffer verwendet werden soll.

   b. Wählen Sie Weiter aus.

7. Überprüfen Sie die Details der Prognose und wählen Sie Speichern und starten aus.

Inferenz für eine Vorhersage starten oder beenden (Konsole)

> **Note**
>
> Die Gebühren von Lookout for Equipment fallen für geplante Inferenzen mit den Daten an, die zwischen AWS IoT SiteWise und Lookout for Equipment übertragen werden. Weitere Informationen finden Sie unter Amazon Lookout for Equipment Pricing.

Wenn Sie eine Prognose „blookoutequipment:CreateDataset“ hinzugefügt, diese aber nach dem Training nicht aktiviert haben, müssen Sie sie aktivieren, damit sie mit der Überwachung Ihrer Anlagen beginnen kann.

Um die Inferenz für eine Vorhersage zu starten

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Assets und dann das Asset aus, zu dem die Prognose hinzugefügt werden soll.
3. Wählen Sie Prognosen aus.
4. Wählen Sie die Prognosen aus, die Sie aktivieren möchten.

5. Wählen Sie unter Aktionen die Option Inferenz starten aus und gehen Sie wie folgt vor:

    a. Definieren Sie unter Eingabedaten für Häufigkeit des Daten-Uploads, wie oft Daten hochgeladen werden, und definieren Sie für Offset-Verzögerungszeit, wie viel Puffer verwendet werden soll.

    b. Wählen Sie Speichern und starten.

Um die Inferenz für eine Vorhersage zu beenden

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Assets und dann das Asset aus, zu dem die Prognose hinzugefügt werden soll.
3. Wählen Sie Prognosen aus.
4. Wählen Sie die Vorhersagen aus, die Sie beenden möchten.
5. Wählen Sie unter Aktionen die Option Inferenz beenden aus.

Hinzufügen einer Vorhersagedefinition (CLI)

Um eine Vorhersagedefinition für ein neues oder vorhandenes Asset-Modell zu definieren, können Sie die AWS Command Line Interface (AWS CLI) verwenden. Nachdem Sie die Prognosedefinition für das Anlagenmodell definiert haben, trainieren Sie eine Vorhersage für eine Anlage und planen die Inferenz für diese, AWS IoT SiteWise um Anomalieerkennung mit Lookout for Equipment durchzuführen.

Voraussetzungen

Um diese Schritte ausführen zu können, müssen Sie ein Anlagenmodell und mindestens eine Anlage erstellt haben. Weitere Informationen finden Sie unter Ein Asset-Modell erstellen (AWS CLI) und Ein Asset erstellen (AWS CLI).

Wenn Sie noch nicht damit vertraut sind AWS IoT SiteWise, müssen Sie den `CreateBulkImportJob` API-Vorgang aufrufen, in AWS IoT SiteWise den die Eigenschaftswerte der Anlage importiert werden. Dieser Vorgang wird dann zum Trainieren des Modells verwendet. Weitere Informationen finden Sie unter Erstellen Sie einen Massenimportauftrag ()AWS CLI.

Um eine Vorhersagedefinition hinzuzufügen

1. Erstellen Sie eine Datei mit dem Namen `asset-model-payload.json`. Folgen Sie den Schritten in diesen anderen Abschnitten, um der Datei die Details Ihres Asset-Modells hinzuzufügen, reichen Sie aber nicht die Anfrage zur Erstellung oder Aktualisierung des Asset-Modells ein.

   - Weitere Informationen zum Erstellen eines Vermögensmodells finden Sie unter Ein Asset-Modell erstellen (AWS CLI)
   - Weitere Informationen zum Aktualisieren eines vorhandenen Asset-Modells finden Sie unter Aktualisierung eines Asset- oder Komponentenmodells (AWS CLI)
2. Fügen Sie dem Asset-Modell ein Verbundmodell von Lookout for Equipment (`assetModelCompositeModels`) hinzu, indem Sie den folgenden Code hinzufügen.

   - *`Property`*Ersetzen Sie es durch die ID der Eigenschaften, die Sie einbeziehen möchten. Rufen Sie an, um diese IDs zu erhalten `DescribeAssetModel`.
   - *`RoleARN`*Ersetzen Sie es durch den ARN einer IAM-Rolle, die Lookout for Equipment den Zugriff auf Ihre AWS IoT SiteWise Daten ermöglicht.

```
{
  ...
  "assetModelCompositeModels": [
    {
      "name": "L4Epredictiondefinition",
      "type": "AWS/L4E_ANOMALY",
      "properties": [
          {
            "name": "AWS/L4E_ANOMALY_RESULT",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_RESULT",
            "unit": "none",
            "type": {
              "measurement": {}
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INPUT",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INPUT",
            "type": {
```

```
            "attribute": {
              "defaultValue": "{\"properties\": [\"Property1\", \"Property2\"]}"
            }
          }
        },
        {
          "name": "AWS/L4E_ANOMALY_PERMISSIONS",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/L4E_ANOMALY_PERMISSIONS",
          "type": {
            "attribute": {
              "defaultValue": "{\"roleArn\": \"RoleARN\"}"
            }
          }
        },
        {
          "name": "AWS/L4E_ANOMALY_DATASET",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/L4E_ANOMALY_DATASET",
          "type": {
              "attribute": {}
          }
        },
        {
          "name": "AWS/L4E_ANOMALY_MODEL",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/L4E_ANOMALY_MODEL",
          "type": {
            "attribute": {}
          }
        },
        {
          "name": "AWS/L4E_ANOMALY_INFERENCE",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE",
          "type": {
            "attribute": {}
          }
        },
        {
          "name": "AWS/L4E_ANOMALY_TRAINING_STATUS",
          "dataType": "STRUCT",
          "dataTypeSpec": "AWS/L4E_ANOMALY_TRAINING_STATUS",
          "type": {
```

```
              "attribute": {
                "defaultValue": "{}"
              }
            }
          },
          {
            "name": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "dataType": "STRUCT",
            "dataTypeSpec": "AWS/L4E_ANOMALY_INFERENCE_STATUS",
            "type": {
              "attribute": {
                "defaultValue": "{}"
              }
            }
          }
    ]
}
```

3. Erstellen Sie das Asset-Modell oder aktualisieren Sie das bestehende Asset-Modell. Führen Sie eine der folgenden Aktionen aus:

   - Führen Sie den folgenden Befehl aus, um das Asset-Modell zu erstellen:

     ```
     aws iotsitewise create-asset-model --cli-input-json file://asset-model-
     payload.json
     ```

   - Führen Sie den folgenden Befehl aus, um das bestehende Asset-Modell zu aktualisieren. *asset-model-id*Ersetzen Sie es durch die ID des Asset-Modells, das Sie aktualisieren möchten.

     ```
     aws iotsitewise update-asset-model \
       --asset-model-id asset-model-id \
       --cli-input-json file://asset-model-payload.json
     ```

Nachdem Sie den Befehl ausgeführt haben, notieren Sie sich das `assetModelId` in der Antwort.

Eine Vorhersage trainieren und Inferenz starten (CLI)

Nachdem die Vorhersagedefinition definiert ist, können Sie Assets auf dieser Grundlage trainieren und mit der Inferenz beginnen. Wenn Sie Ihre Vorhersage trainieren, aber keine Inferenz starten

möchten, fahren Sie mit fort. Eine Vorhersage trainieren (CLI) Um die Vorhersage zu trainieren und die Inferenz für das Asset zu starten, benötigen Sie die `assetId` der Zielressource.

Um die Vorhersage zu trainieren und mit der Inferenz zu beginnen

1. Führen Sie den folgenden Befehl aus, um das `assetModelCompositeModelId` `assetModelCompositeModelSummaries` Under zu finden. *`asset-model-id`*Ersetzen Sie es durch die ID des Asset-Modells, in dem Sie es erstellt habenAktualisierung eines Asset- oder Komponentenmodells (AWS CLI).

   ```
   aws iotsitewise describe-asset-model \
     --asset-model-id asset-model-id \
   ```

2. Führen Sie den folgenden Befehl aus, um `actionDefinitionId` die `TrainingWithInference` Aktion zu finden. *`asset-model-id`*Ersetzen Sie durch die im vorherigen Schritt verwendete ID und *`asset-model-composite-model-id`*ersetzen Sie sie durch die im vorherigen Schritt zurückgegebene ID.

   ```
   aws iotsitewise describe-asset-model-composite-model \
     --asset-model-id asset-model-id \
     --asset-model-composite-model-id asset-model-composite-model-id \
   ```

3. Erstellen Sie eine Datei mit dem Namen `train-start-inference-prediction.json` und fügen Sie den folgenden Code hinzu, der den folgenden ersetzt:

   - *`asset-id`*mit der ID des Ziel-Assets
   - *`action-definition-id`*mit der ID der TrainingWithInference Aktion
   - *`StartTime`*mit dem Beginn der Trainingsdaten, angegeben in Epochensekunden
   - *`EndTime`*mit dem Ende der Trainingsdaten, angegeben in Epochensekunden
   - *`TargetSamplingRate`*mit der Abtastrate der Daten nach der Nachbearbeitung durch Lookout for Equipment. Zulässige Werte sind:`PT1S | PT5S | PT10S | PT15S | PT30S | PT1M | PT5M | PT10M | PT15M | PT30M | PT1H`.

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
     },
     "actionDefinitionId": "action-definition-Id",
   ```

```
  "actionPayload":{
    "stringValue": "{\"l4ETrainingWithInference\":{\"trainingWithInferenceMode
\":\"START\",\"trainingPayload\":{\"exportDataStartTime\":StartTime,
\"exportDataEndTime\":EndTime},\"targetSamplingRate\":\"TargetSamplingRate\"},
\"inferencePayload\":{\"dataDelayOffsetInMinutes\":0,\"dataUploadFrequency\":\"PT5M
\"}}}"
  }
}
```

4. Führen Sie den folgenden Befehl aus, um das Training und die Inferenz zu starten:

```
aws iotsitewise execute-action --cli-input-json file://train-start-inference-
prediction.json
```

Eine Vorhersage trainieren (CLI)

Nachdem die Definition der Vorhersage nun definiert ist, können Sie Ressourcen auf dieser Grundlage trainieren. Um die Vorhersage auf der Anlage zu trainieren, benötigen Sie die `assetId` der Zielressource.

Um die Vorhersage zu trainieren

1. Führen Sie den folgenden Befehl aus, um das `assetModelCompositeModelId` Under zu finden`assetModelCompositeModelSummaries`. *`asset-model-id`*Ersetzen Sie es durch die ID des Asset-Modells, in dem Sie es erstellt habenAktualisierung eines Asset- oder Komponentenmodells (AWS CLI).

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Führen Sie den folgenden Befehl aus, um `actionDefinitionId` die `Training` Aktion zu finden. *`asset-model-id`*Ersetzen Sie durch die im vorherigen Schritt verwendete ID und *`asset-model-composite-model-id`*ersetzen Sie sie durch die im vorherigen Schritt zurückgegebene ID.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Erstellen Sie eine Datei mit dem Namen `train-prediction.json` und fügen Sie den folgenden Code hinzu, der den folgenden ersetzt:

   - *`asset-id`*mit der ID des Ziel-Assets
   - *`action-definition-id`*mit der ID der Trainingsaktion
   - *`StartTime`*mit dem Beginn der Trainingsdaten, angegeben in Epochensekunden
   - *`EndTime`*mit dem Ende der Trainingsdaten, angegeben in Epochensekunden
   - (Optional) *`BucketName`* mit dem Namen des Amazon S3 S3-Buckets, der Ihre Etikettendaten enthält
   - (Optional) *`Prefix`* mit dem Präfix, das dem Amazon S3 S3-Bucket zugeordnet ist.
   - *`TargetSamplingRate`*mit der Abtastrate der Daten nach der Nachbearbeitung durch Lookout for Equipment. Zulässige Werte sind:`PT1S | PT5S | PT10S | PT15S | PT30S | PT1M | PT5M | PT10M | PT15M | PT30M | PT1H`.

   > **Note**
   >
   > Geben Sie sowohl den Bucket-Namen als auch das Präfix oder keines von beiden an.

   ```
   {
     "targetResource": {
       "assetId": "asset-id"
     },
     "actionDefinitionId": "action-definition-Id",
     "actionPayload":{ "stringValue": "{\"l4ETraining\": {\"trainingMode\":
   \"START\",\"exportDataStartTime\": StartTime, \"exportDataEndTime\": EndTime,
    \"targetSamplingRate\":\"TargetSamplingRate\"}, \"labelInputConfiguration\":
    {\"bucketName\": \"BucketName\", \"prefix\": \"Prefix\"}}}"
   }
   }
   ```

4. Führen Sie den folgenden Befehl aus, um das Training zu starten:

   ```
   aws iotsitewise execute-action --cli-input-json file://train-prediction.json
   ```

Bevor Sie mit der Inferenz beginnen können, muss das Training abgeschlossen sein. Gehen Sie wie folgt vor, um den Status der Schulung zu überprüfen:

- Navigieren Sie in der Konsole zu dem Asset, für das sich die Prognose bezieht.
- Rufen Sie von der AWS CLI aus `BatchGetAssetPropertyValue` über `propertyId` die `trainingStatus` Eigenschaft auf.

Inferenz aus einer Vorhersage starten oder beenden (CLI)

Sobald die Vorhersage trainiert ist, können Sie mit der Inferenz beginnen und Lookout for Equipment anweisen, mit der Überwachung Ihrer Anlagen zu beginnen. Um die Inferenz zu starten oder zu beenden, benötigen Sie die Daten `assetId` der Zielressource.

Um die Inferenz zu starten

1. Führen Sie den folgenden Befehl aus, um das `assetModelCompositeModelId` `assetModelCompositeModelSummaries` Under zu finden. *`asset-model-id`*Ersetzen Sie es durch die ID des Asset-Modells, in dem Sie es erstellt habenAktualisierung eines Asset- oder Komponentenmodells (AWS CLI).

   ```
   aws iotsitewise describe-asset-model \
     --asset-model-id asset-model-id \
   ```

2. Führen Sie den folgenden Befehl aus, um `actionDefinitionId` die `Inference` Aktion zu finden. *`asset-model-id`*Ersetzen Sie durch die im vorherigen Schritt verwendete ID und *`asset-model-composite-model-id`*ersetzen Sie sie durch die im vorherigen Schritt zurückgegebene ID.

   ```
   aws iotsitewise describe-asset-model-composite-model \
     --asset-model-id asset-model-id \
     --asset-model-composite-model-id asset-model-composite-model-id \
   ```

3. Erstellen Sie eine Datei mit dem Namen `start-inference.json` und fügen Sie den folgenden Code hinzu, der den folgenden ersetzt:

   - *`asset-id`*mit der ID des Ziel-Assets
   - *`action-definition-id`*mit der ID der Start-Inferenzaktion
   - *`Offset`*mit der Menge des zu verwendenden Puffers
   - *`Frequency`*mit wie oft Daten hochgeladen werden

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4EInference\": {\"inferenceMode\":\"START
\",\"dataDelayOffsetInMinutes\": Offset, \"dataUploadFrequency\": \"Frequency\"}}"
}}
```

4. Führen Sie den folgenden Befehl aus, um die Inferenz zu starten:

```
aws iotsitewise execute-action --cli-input-json file://start-inference.json
```

Um die Inferenz zu beenden

1. Führen Sie den folgenden Befehl aus, um das `assetModelCompositeModelId` `assetModelCompositeModelSummaries` Under zu finden. *`asset-model-id`*Ersetzen Sie es durch die ID des Asset-Modells, in dem Sie es erstellt habenAktualisierung eines Asset- oder Komponentenmodells (AWS CLI).

```
aws iotsitewise describe-asset-model \
  --asset-model-id asset-model-id \
```

2. Führen Sie den folgenden Befehl aus, um `actionDefinitionId` die `Inference` Aktion zu finden. *`asset-model-id`*Ersetzen Sie durch die im vorherigen Schritt verwendete ID und *`asset-model-composite-model-id`*ersetzen Sie sie durch die im vorherigen Schritt zurückgegebene ID.

```
aws iotsitewise describe-asset-model-composite-model \
  --asset-model-id asset-model-id \
  --asset-model-composite-model-id asset-model-composite-model-id \
```

3. Erstellen Sie eine Datei mit dem Namen `stop-inference.json` und fügen Sie den folgenden Code hinzu, der den folgenden ersetzt:

   - *`asset-id`*mit der ID des Ziel-Assets
   - *`action-definition-id`*mit der ID der Start-Inferenzaktion

```
{
  "targetResource": {
    "assetId": "asset-id"
  },
  "actionDefinitionId": "action-definition-Id",
  "actionPayload":{ "stringValue": "{\"l4EInference\":{\"inferenceMode\":\"STOP
\"}}"
}}
```

4. Führen Sie den folgenden Befehl aus, um die Inferenz zu beenden:

```
aws iotsitewise execute-action --cli-input-json file://stop-inference.json
```

Verwaltung des Datenspeichers

Sie können so konfigurieren AWS IoT SiteWise , dass Ihre Daten in den folgenden Speicherstufen gespeichert werden:

Heiße Stufe

Bei der Hot-Storage-Tier handelt es sich um einen AWS IoT SiteWise verwalteten Zeitreihenspeicher. Hot Tier ist am effektivsten für Daten, auf die häufig zugegriffen wird, und hat eine geringe write-to-read Latenz. Im Hot-Tier gespeicherte Daten werden von Industrieanwendungen verwendet, die schnellen Zugriff auf die neuesten Messwerte in Ihren Geräten benötigen. Dazu gehören Anwendungen, die Echtzeit-Metriken mit einem interaktiven Dashboard visualisieren, oder Anwendungen, die den Betrieb überwachen und Alarme auslösen, um Leistungsprobleme zu identifizieren.

Standardmäßig werden die AWS IoT SiteWise aufgenommenen Daten im Hot-Tier gespeichert. Sie können einen Aufbewahrungszeitraum für das Hot-Tier definieren. Danach werden die Daten auf dem Hot-Tier je nach Konfiguration entweder in den Warm- oder Cold-Tier-Speicher AWS IoT SiteWise verschoben. Um optimale Leistung und Kosteneffizienz zu erzielen, sollten Sie die Aufbewahrungsdauer für die Hot-Tier-Stufe so festlegen, dass sie länger ist als die Zeit, die häufig für das Abrufen von Daten benötigt wird. Dies wird für Echtzeit-Metriken, Alarme und Überwachungsszenarien verwendet. Wenn kein Aufbewahrungszeitraum festgelegt ist, werden Ihre Daten auf unbestimmte Zeit im Hot-Tier gespeichert.

Warme Stufe

Bei der Warm-Storage-Tier handelt AWS IoT SiteWise es sich um eine verwaltete Stufe, die sich für die kosteneffiziente Speicherung historischer Daten eignet. Sie eignet sich am besten zum Abrufen großer Datenmengen mit mittleren write-to-read Latenzeigenschaften. Verwenden Sie die warme Ebene, um historische Daten zu speichern, die für große Workloads benötigt werden. Es wird beispielsweise für den Datenabruf für Analysen, Business Intelligence-Anwendungen (BI), Berichtstools und das Training von Modellen für maschinelles Lernen (ML) verwendet. Wenn Sie die Cold-Storage-Stufe aktivieren, können Sie eine Aufbewahrungsfrist für die warme Stufe definieren. AWS IoT SiteWise Löscht nach Ablauf der Aufbewahrungsfrist Daten aus der warmen Stufe.

Kalte Stufe

Die Kühlspeicherebene verwendet einen Amazon S3 S3-Bucket zum Speichern von Daten, die selten verwendet werden. Bei aktiviertem Cold Tier werden die Zeitreihen,

einschließlich Messungen, Metriken, Transformationen und Aggregaten sowie Definitionen von Anlagenmodellen, alle 6 Stunden AWS IoT SiteWise repliziert. Cold Tier wird verwendet, um Daten zu speichern, die eine hohe Leselatenz für historische Berichte und Backups tolerieren.

Themen

Speichereinstellungen konfigurieren

Sie können Speichereinstellungen so konfigurieren, dass Sie sich für die Wartung von verwaltetem Speicher auf der warmen Ebene entscheiden und Daten auch auf das kalte Tier replizieren. Weitere Informationen zur Aufbewahrungsdauer für die Warm- und Hot-Tarife finden Sie unterAuswirkungen auf die Datenspeicherung. Gehen Sie bei der Konfiguration der Speichereinstellungen wie folgt vor:

- Aufbewahrung auf hoher Ebene — Legen Sie einen Aufbewahrungszeitraum fest, in dem Ihre Daten auf der heißen Ebene gespeichert werden, bevor sie gelöscht und je nach Ihren Speichereinstellungen in den vom Service verwalteten Speicher auf der warmen oder kalten Ebene verschoben werden. AWS IoT SiteWise löscht alle Daten in der Hot-Tier, die vor Ablauf der Aufbewahrungsfrist vorhanden waren. Wenn Sie keinen Aufbewahrungszeitraum festlegen, werden Ihre Daten auf unbestimmte Zeit im Hot-Tier gespeichert.
- Aufbewahrung auf warmer Ebene — Legen Sie einen Aufbewahrungszeitraum fest, in dem Ihre Daten auf der Warm-Tier-Ebene gespeichert werden, bevor sie aus dem AWS IoT SiteWise Speicher gelöscht und in den vom Kunden verwalteten Cold-Tier-Speicher verschoben werden. AWS IoT SiteWise löscht alle Daten aus der Warm-Tier, die vor Ablauf der Aufbewahrungsfrist vorhanden waren. Wenn kein Aufbewahrungszeitraum festgelegt ist, werden Ihre Daten auf unbestimmte Zeit in der Warm-Tier gespeichert.

> **Note**
>
> Um die Abfrageleistung zu verbessern, legen Sie mit Warm-Tier-Speicher einen Hot-Tier-Aufbewahrungszeitraum fest.

Auswirkungen der Datenspeicherung bei Speichern auf heißer und warmer Ebene

- Wenn Sie die Aufbewahrungsdauer des Hot-Tier-Speichers verkürzen, werden Daten dauerhaft vom Hot-Tier in das Warm- oder Cold-Tier verschoben. Wenn Sie die Aufbewahrungsdauer der warmen Schicht verkürzen, werden Daten in die kalte Schicht verschoben und aus der warmen Schicht dauerhaft gelöscht.
- Wenn Sie die Aufbewahrungsdauer des Speichers der heißen oder warmen Ebene verlängern, wirkt sich die Änderung auf Daten aus, an die AWS IoT SiteWise ab diesem Zeitpunkt gesendet werden. AWS IoT SiteWise ruft keine Daten aus dem warmen oder kalten Speicher ab, um den heißen Speicher zu füllen. Wenn beispielsweise die Aufbewahrungsdauer des Hot-Tier-Speichers zunächst auf 30 Tage festgelegt und dann auf 60 Tage erhöht wird, dauert es 30 Tage, bis der Hot-Tier-Speicher Daten im Wert von 60 Tagen enthält.

Themen

Konfigurieren Sie die Speichereinstellungen für die Warm-Stufe (Konsole)

Das folgende Verfahren zeigt Ihnen, wie Sie die Speichereinstellungen so konfigurieren, dass Daten in der AWS IoT SiteWise Konsole auf das warme Tier repliziert werden.

So konfigurieren Sie die Speichereinstellungen in der Konsole

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Speicher aus.
3. Wählen Sie rechts oben die Option Edit (Bearbeiten) aus.
4. Gehen Sie auf der Seite Speicher bearbeiten wie folgt vor:
5. Gehen Sie für Hot-Tier-Einstellungen wie folgt vor:

- Wenn Sie einen Aufbewahrungszeitraum für die Dauer festlegen möchten, für die Ihre Daten auf dem Hot-Tier gespeichert werden, bevor sie gelöscht und in den vom Service verwalteten Warm-Tier-Speicher verschoben werden, wählen Sie Aufbewahrungszeitraum aktivieren.
- Um einen Aufbewahrungszeitraum zu konfigurieren, geben Sie eine ganze Zahl ein und wählen Sie eine Einheit aus. Die Aufbewahrungsfrist muss mindestens 30 Tage betragen.

AWS IoT SiteWise löscht alle Daten im Hot-Tier, die älter als die Aufbewahrungsfrist sind. Wenn Sie keinen Aufbewahrungszeitraum festlegen, werden Ihre Daten auf unbestimmte Zeit gespeichert.

6. (Empfohlen) Gehen Sie für die Warm-Tier-Einstellungen wie folgt vor:

- Um sich für den Warm-Tier-Speicher zu entscheiden, wählen Sie Ich bestätige die Option Ich bestätige die Option Warm-Tier-Speicher, um sich für den Warm-Tier-Speicher zu entscheiden.
- (Optional) Um einen Aufbewahrungszeitraum zu konfigurieren, geben Sie eine ganze Zahl ein und wählen Sie eine Einheit aus. Die Aufbewahrungsdauer muss mindestens 365 Tage betragen.

AWS IoT SiteWise löscht Daten in der Warm-Tier, die vor dem Aufbewahrungszeitraum existierten. Wenn Sie keinen Aufbewahrungszeitraum festlegen, werden Ihre Daten auf unbestimmte Zeit gespeichert.

> **Note**
>
> - Wenn Sie sich für die Warm-Stufe entscheiden, wird die Konfiguration nur einmal angezeigt.
> - Um die Aufbewahrung auf der heißen Ebene festzulegen, müssen Sie entweder über einen warmen oder einen kalten Speicher verfügen. Aus Gründen der Kosteneffizienz und des Abrufs historischer Daten AWS IoT SiteWise empfiehlt es sich, Langzeitdaten im Warm-Tier zu speichern.
> - Um die Aufbewahrung auf der Warm-Tier-Ebene festzulegen, müssen Sie über einen Cold-Tier-Speicher verfügen.

7. Wählen Sie Speichern, um Ihre Speichereinstellungen zu speichern.

Im AWS IoT SiteWise Speicherbereich befindet sich der Warm Tier-Speicher in einem der folgenden Zustände:

- Aktiviert — Wenn Ihre Daten bereits vor dem Aufbewahrungszeitraum für das heiße Tier vorhanden waren, werden die Daten auf das Warm-Tier AWS IoT SiteWise verschoben.“
- Deaktiviert — Der Warm-Tier-Speicher ist deaktiviert.

Konfigurieren Sie die Speichereinstellungen für die Warmstufe (AWS CLI)

Mit den und den folgenden Befehlen können Sie Speichereinstellungen so konfigurieren, dass Daten auf die AWS CLI Warm-Tier verschoben werden.

Um zu verhindern, dass die bestehende Konfiguration überschrieben wird, rufen Sie die aktuellen Speicherkonfigurationsinformationen ab, indem Sie den folgenden Befehl ausführen:

```
aws iotsitewise describe-storage-configuration
```

Example Antwort ohne bestehende Cold-Tier-Konfiguration

```
{
          "storageType": "SITEWISE_DEFAULT_STORAGE",
          "disassociatedDataStorage": "ENABLED",
          "configurationStatus": {
              "state": "ACTIVE"
          },
          "lastUpdateDate": "2021-10-14T15:53:35-07:00",
          "warmTier": "DISABLED"
}
```

Example Antwort mit vorhandener Cold-Tier-Konfiguration

```
{
      "storageType": "MULTI_LAYER_STORAGE",
          "multiLayerStorage": {
            "customerManagedS3Storage": {
            "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
            "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
            }
          },
      "disassociatedDataStorage": "ENABLED",
```

```
      "retentionPeriod": {
      "numberOfDays": retention-in-days
      },
       "configurationStatus": {
       "state": "ACTIVE"
      },
      "lastUpdateDate": "2023-10-25T15:59:46-07:00",
      "warmTier": "DISABLED"
}
```

Konfigurieren Sie die Speichereinstellungen für die warme Stufe mit AWS CLI

Führen Sie den folgenden Befehl aus, um die Speichereinstellungen zu konfigurieren. `file-name`Ersetzen Sie es durch den Namen der Datei, die die AWS IoT SiteWise Speicherkonfiguration enthält.

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise Konfiguration mit heißer und warmer Stufe

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "disassociatedDataStorage": "ENABLED",
            "warmTier": "ENABLED",
            "retentionPeriod": {
               "numberOfDays": hot-tier-retention-in-days
             }

}
```

`hot-tier-retention-in-days`muss eine ganze Zahl größer oder gleich 30 Tagen sein.

Example response

```
{
            "storageType": "SITEWISE_DEFAULT_STORAGE",
            "configurationStatus": {
            "state": "UPDATE_IN_PROGRESS"
            }
}
```

Wenn Sie Cold-Tier-Speicher aktiviert haben, finden Sie weitere Informationen unterKonfigurieren Sie Speichereinstellungen mit einem AWS CLI vorhandenen Cold-Tier.

Konfigurieren Sie Speichereinstellungen mit einem AWS CLI vorhandenen Cold-Tier

Konfigurieren Sie die Speichereinstellungen AWS CLI mithilfe des vorhandenen Cold-Tier-Speichers

- Führen Sie den folgenden Befehl aus, um die Speichereinstellungen zu konfigurieren. Ersetzen Sie *file-name* durch den Namen der Datei, die die AWS IoT SiteWise Speicherkonfiguration enthält.

```
aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
```

Example AWS IoT SiteWise Speicherkonfiguration

- Ersetzen Sie *bucket-name* durch Ihren Amazon S3 S3-Bucket-Namen.
- Ersetzen Sie das *Präfix* durch Ihr Amazon S3 S3-Präfix.
- *aws-account-id*Ersetzen Sie es durch Ihre AWS Konto-ID.
- Ersetzen Sie *role-name* durch den Namen der Amazon S3-Zugriffsrolle, die das Senden von Daten AWS IoT SiteWise an Amazon S3 ermöglicht.
- Ersetzen Sie *hot-tier-retention-in-days* durch eine ganze Zahl, die größer oder gleich 30 Tagen ist.
- Ersetze *warm-tier-retention-in-days* durch eine ganze Zahl, die größer oder gleich 365 Tagen ist.

> **Note**
>
> AWS IoT SiteWise löscht alle Daten in der warmen Stufe, die älter sind als die Aufbewahrungsfrist der kalten Stufe. Wenn Sie keinen Aufbewahrungszeitraum festlegen, werden Ihre Daten auf unbestimmte Zeit gespeichert.

```
{
      "storageType": "MULTI_LAYER_STORAGE",
        "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
```

```
            "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
            }
        },
    "disassociatedDataStorage": "ENABLED",
    "retentionPeriod": {
      "numberOfDays": hot-tier-retention-in-days
    },
    "warmTier": "ENABLED",
    "warmTierRetentionPeriod": {
      "numberOfDays": warm-tier-retention-in-days
    }
}
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
       }
}
```

Konfigurieren Sie die Speichereinstellungen für das Cold-Tier (Konsole)

Das folgende Verfahren zeigt Ihnen, wie Sie die Speichereinstellungen für die Replikation von Daten auf das Cold-Tier in der AWS IoT SiteWise Konsole konfigurieren.

So konfigurieren Sie die Speichereinstellungen in der Konsole

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Speicher aus.
3. Wählen Sie rechts oben die Option Edit (Bearbeiten) aus.
4. Gehen Sie auf der Seite Speicher bearbeiten wie folgt vor:

    a. Wählen Sie unter Speichereinstellungen die Option Cold-Tier-Speicher aktivieren aus. Der Cold-Tier-Speicher ist standardmäßig deaktiviert.

    b. Geben Sie für S3-Bucket-Standort den Namen eines vorhandenen Amazon S3 S3-Buckets und ein Präfix ein.

> **Note**
>
> - Amazon S3 verwendet das Präfix als Ordnernamen im Amazon S3 S3-Bucket. Das Präfix muss 1—255 Zeichen lang sein und mit einem Schrägstrich (/) enden. Ihre AWS IoT SiteWise Daten werden in diesem Ordner gespeichert.
> - Wenn Sie keinen Amazon S3 S3-Bucket haben, wählen Sie View und erstellen Sie dann einen in der Amazon S3 S3-Konsole. Weitere Informationen finden Sie unter Erstellen Sie Ihren ersten S3-Bucket im Amazon S3 S3-Benutzerhandbuch.

c. Gehen Sie für die S3-Zugriffsrolle wie folgt vor:

- Wählen Sie Create a role from an AWS managed template. Dadurch AWS wird automatisch eine IAM-Rolle erstellt, die das Senden von Daten AWS IoT SiteWise an Amazon S3 ermöglicht.
- Wählen Sie Bestehende Rolle verwenden und wählen Sie dann die Rolle, die Sie erstellt haben, aus der Liste aus.

> **Note**
>
> - Sie müssen denselben Amazon S3 S3-Bucket-Namen für den S3-Bucket-Speicherort verwenden, den Sie im vorherigen Schritt und in Ihrer IAM-Richtlinie verwendet haben.
> - Stellen Sie sicher, dass Ihre Rolle über die im folgenden Beispiel gezeigten Berechtigungen verfügt.
>
>   Example Berechtigungsrichtlinie:
>
> ```
> {
>       "Version": "2012-10-17",
>       "Statement": [
>           {
>               "Effect": "Allow",
>               "Action": [
>                   "s3:PutObject",
>                   "s3:GetObject",
>                   "s3:DeleteObject",
>                   "s3:GetBucketLocation",
>                   "s3:ListBucket"
> ```

```
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Ersetzen Sie *bucket-name* durch den Namen Ihres Amazon S3 S3-Buckets.

d. Informationen zur Einrichtung von Hot Tier finden Sie unter Schritt 5 unter. Konfigurieren Sie die Speichereinstellungen für die Warm-Stufe (Konsole)

e. (Optional) Gehen Sie zur AWS IoT Analytics Integration wie folgt vor.

   i. Wenn Sie Ihre Daten abfragen AWS IoT Analytics möchten, wählen Sie Enabled AWS IoT Analytics data store aus.

   ii. AWS IoT SiteWise generiert einen Namen für Ihren Datenspeicher, oder Sie können einen anderen Namen eingeben.

   AWS IoT SiteWise erstellt automatisch einen Datenspeicher AWS IoT Analytics zum Speichern Ihrer Daten. Um die Daten abzufragen, können Sie sie verwenden, AWS IoT Analytics um Datensätze zu erstellen. Weitere Informationen finden Sie im AWS IoT Analytics Benutzerhandbuch unter Arbeiten mit AWS IoT SiteWise Daten.

f. Wählen Sie Speichern.

Im Bereich AWS IoT SiteWise Speicher kann der Cold-Tier-Speicher einen der folgenden Werte annehmen:

- Aktiviert — AWS IoT SiteWise repliziert Ihre Daten in den angegebenen Amazon S3 S3-Bucket.
- Aktiviert — AWS IoT SiteWise verarbeitet Ihre Anfrage zur Aktivierung des Cold-Tier-Speichers. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.
- Enable_Failed — Ihre Anfrage zur Aktivierung des Cold-Tier-Speichers AWS IoT SiteWise konnte nicht verarbeitet werden. Wenn Sie AWS IoT SiteWise das Senden von Protokollen an Amazon CloudWatch Logs aktiviert haben, können Sie diese Protokolle zur Behebung von Problemen verwenden. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch Logs.
- Deaktiviert — Der Cold-Tier-Speicher ist deaktiviert.

Konfigurieren Sie die Speichereinstellungen für Cold Tier (AWS CLI)

Das folgende Verfahren zeigt Ihnen, wie Sie die Speichereinstellungen für die Replikation von Daten auf das Cold-Tier mithilfe von AWS CLI konfigurieren.

Um Speichereinstellungen zu konfigurieren mit AWS CLI

1. Um Daten in einen Amazon S3 S3-Bucket in Ihrem Konto zu exportieren, führen Sie den folgenden Befehl aus, um die Speichereinstellungen zu konfigurieren. Ersetzen Sie *file-name* durch den Namen der Datei, die die AWS IoT SiteWise Speicherkonfiguration enthält.

   ```
   aws iotsitewise put-storage-configuration --cli-input-json file://file-name.json
   ```

   Example AWS IoT SiteWise Speicherkonfiguration

   - Ersetzen Sie *bucket-name* durch Ihren Amazon S3 S3-Bucket-Namen.
   - Ersetzen Sie das *Präfix* durch Ihr Amazon S3 S3-Präfix.
   - *aws-account-id*Ersetzen Sie es durch Ihre AWS Konto-ID.
   - Ersetzen Sie *role-name* durch den Namen der Amazon S3-Zugriffsrolle, die das Senden von Daten AWS IoT SiteWise an Amazon S3 ermöglicht.
   - *retention-in-days*Ersetzen Sie es durch eine ganze Zahl, die größer oder gleich 30 Tagen ist.

   ```
   {
         "storageType": "MULTI_LAYER_STORAGE",
         "multiLayerStorage": {
             "customerManagedS3Storage": {
                 "s3ResourceArn": "arn:aws:s3:::bucket-name/prefix/",
                 "roleArn": "arn:aws:iam::aws-account-id:role/role-name"
             }
         },
         "retentionPeriod": {
             "numberOfDays": retention-in-days,
             "unlimited": false
         }
     }
   ```

Note

- Sie müssen denselben Amazon S3 S3-Bucket-Namen in der AWS IoT SiteWise Speicherkonfiguration und in der IAM-Richtlinie verwenden.
- Stellen Sie sicher, dass Ihre Rolle über die im folgenden Beispiel gezeigten Berechtigungen verfügt.

  Example Berechtigungsrichtlinie:

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [
                  "s3:PutObject",
                  "s3:GetObject",
                  "s3:DeleteObject",
                  "s3:GetBucketLocation",
                  "s3:ListBucket"
              ],
              "Resource": [
                  "arn:aws:s3:::bucket-name",
                  "arn:aws:s3:::bucket-name/*"
              ]
          }
      ]
  }
```

  Ersetzen Sie *bucket-name* durch den Namen Ihres Amazon S3 S3-Buckets.

Example response

```
{
    "storageType": "MULTI_LAYER_STORAGE",
    "retentionPeriod": {
        "numberOfDays": 100,
        "unlimited": false
```

```
    },
    "configurationStatus": {
        "state": "UPDATE_IN_PROGRESS"
    }
}
```

> **Note**
>
> Es kann einige Minuten dauern, AWS IoT SiteWise bis die Speicherkonfiguration aktualisiert ist.

2. Führen Sie den folgenden Befehl aus, um die Informationen zur Speicherkonfiguration abzurufen.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "MULTI_LAYER_STORAGE",
      "multiLayerStorage": {
          "customerManagedS3Storage": {
              "s3ResourceArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/torque/",
              "roleArn": "arn:aws:iam::123456789012:role/SWAccessS3Role"
          }
      },
      "retentionPeriod": {
          "numberOfDays": 100,
          "unlimited": false
      },
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:54:14-07:00"
  }
```

3. Um den Export von Daten in den Amazon S3 S3-Bucket zu beenden, führen Sie den folgenden Befehl aus, um die Speichereinstellungen zu konfigurieren.

```
aws iotsitewise put-storage-configuration --storage-type SITEWISE_DEFAULT_STORAGE
```

> **Note**
>
> Standardmäßig werden Ihre Daten nur im Hot-Tier von gespeichert AWS IoT SiteWise.

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "UPDATE_IN_PROGRESS"
      }
  }
```

4. Führen Sie den folgenden Befehl aus, um die Informationen zur Speicherkonfiguration abzurufen.

```
aws iotsitewise describe-storage-configuration
```

Example response

```
{
      "storageType": "SITEWISE_DEFAULT_STORAGE",
      "configurationStatus": {
          "state": "ACTIVE"
      },
      "lastUpdateDate": "2021-03-30T15:57:14-07:00"
  }
```

(Optional) Erstellen Sie einen AWS IoT Analytics Datenspeicher (AWS CLI)

Ein AWS IoT Analytics Datenspeicher ist ein skalierbares und abfragbares Repository, das Daten empfängt und speichert. Sie können die AWS IoT SiteWise Konsole oder AWS IoT Analytics APIs verwenden, um einen AWS IoT Analytics Datenspeicher zum Speichern Ihrer AWS IoT SiteWise Daten zu erstellen. Um die Daten abzufragen, erstellen Sie Datensätze mithilfe AWS IoT Analytics von. Weitere Informationen finden Sie im AWS IoT Analytics Benutzerhandbuch unter Arbeiten mit AWS IoT SiteWise Daten.

Die folgenden Schritte dienen AWS CLI zum Erstellen eines Datenspeichers in AWS IoT Analytics.

Führen Sie den folgenden Befehl aus, um einen Datenspeicher zu erstellen. Ersetzen Sie *file-name* durch den Namen der Datei, die die Datenspeicherkonfiguration enthält.

```
aws iotanalytics create-datastore --cli-input-json file://file-name.json
```

> **Note**
>
> - Sie müssen den Namen eines vorhandenen Amazon S3 S3-Buckets angeben. Wenn Sie keinen Amazon S3 S3-Bucket haben, erstellen Sie zuerst einen. Weitere Informationen finden Sie unter Erstellen Ihres ersten S3-Buckets im Amazon S3 S3-Benutzerhandbuch.
> - Sie müssen denselben Amazon S3 S3-Bucket-Namen in der AWS IoT SiteWise Speicherkonfiguration, der IAM-Richtlinie und der AWS IoT Analytics Datenspeicherkonfiguration verwenden.

Example AWS IoT Analytics Datenspeicher-Konfiguration

Ersetzen Sie *data-store-name*und *s3-bucket-name durch Ihren AWS IoT Analytics Datenspeicher-Namen* und den Amazon S3 S3-Bucket-Namen.

```
{
      "datastoreName": "data-store-name",
      "datastoreStorage": {
          "iotSiteWiseMultiLayerStorage": {
              "customerManagedS3Storage": {
                  "bucket": "s3-bucket-name"
              }
          }
      },
      "retentionPeriod": {
          "numberOfDays": 90
      }
  }
```

Example response

```
{
      "datastoreName": "datastore_IoTSiteWise_demo",
```

```
      "datastoreArn": "arn:aws:iotanalytics:us-west-2:123456789012:datastore/
datastore_IoTSiteWise_demo",
      "retentionPeriod": {
          "numberOfDays": 90,
          "unlimited": false
      }
  }
```

Fehlerbehebung bei den Speichereinstellungen

Verwenden Sie die folgenden Informationen, um Probleme mit der Speicherkonfiguration zu beheben und zu lösen.

Problembereiche

- Fehler: Bucket ist nicht vorhanden
- Fehler: Zugriff auf den Amazon S3-Pfad verweigert
- Fehler: Rollen-ARN kann nicht übernommen werden
- Fehler: Auf den regionsübergreifenden Amazon S3 S3-Bucket konnte nicht zugegriffen werden

Fehler: Bucket ist nicht vorhanden

Lösung: Ihr Amazon S3 S3-Bucket AWS IoT SiteWise konnte nicht gefunden werden. Stellen Sie sicher, dass Sie den Namen eines vorhandenen Amazon S3 S3-Buckets in der aktuellen Region eingeben.

Fehler: Zugriff auf den Amazon S3-Pfad verweigert

Lösung: AWS IoT SiteWise Ich konnte nicht auf Ihren Amazon S3 S3-Bucket zugreifen. Gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie denselben Amazon S3 S3-Bucket verwenden, den Sie in der IAM-Richtlinie angegeben haben.
- Stellen Sie sicher, dass Ihre Rolle über die im folgenden Beispiel gezeigten Berechtigungen verfügt.

  Example Berechtigungsrichtlinie

  ```
  {
  ```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Ersetzen Sie *bucket-name* durch den Namen Ihres Amazon S3 S3-Buckets.

Fehler: Rollen-ARN kann nicht übernommen werden

Lösung: Die IAM-Rolle AWS IoT SiteWise konnte nicht in Ihrem Namen übernommen werden. Stellen Sie sicher, dass Ihre Rolle dem folgenden Dienst vertraut:. `iotsitewise.amazonaws.com` Weitere Informationen finden Sie unter Ich kann keine Rolle annehmen im IAM-Benutzerhandbuch.

Fehler: Auf den regionsübergreifenden Amazon S3 S3-Bucket konnte nicht zugegriffen werden

Lösung: Der Amazon S3 S3-Bucket, den Sie angegeben haben, befindet sich in einer anderen AWS Region. Stellen Sie sicher, dass sich Ihr Amazon S3 S3-Bucket und Ihre AWS IoT SiteWise Assets in derselben Region befinden.

Dateipfade und Schemas von Daten, die auf der kalten Ebene gespeichert wurden

AWS IoT SiteWise speichert Ihre Daten auf der kalten Ebene, indem Zeitreihen repliziert werden, einschließlich Messungen, Metriken, Transformationen und Aggregaten sowie Definitionen von

Anlagen und Anlagenmodellen. Im Folgenden werden die Dateipfade und Schemas der Daten beschrieben, die an die Cold-Tier gesendet werden.

Themen

Gerätedaten (Messungen)

AWS IoT SiteWise exportiert alle sechs Stunden Gerätedaten (Messungen) in die Kühlzelle. Rohdaten werden im Cold-Tier im Apache AVRO (`.avro`) -Format gespeichert.

Dateipfad

AWS IoT SiteWise speichert Gerätedaten (Messungen) im Cold-Tier unter Verwendung der folgenden Vorlage.

```
{keyPrefix}/raw/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
seriesBucket={seriesBucket}/raw_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Jeder Dateipfad zu Rohdaten in Amazon S3 enthält die folgenden Komponenten.

Pfadkomponente	Beschreibung
`keyPrefix`	Das Amazon S3 S3-Präfix, das Sie in der AWS IoT SiteWise Speicherkonfiguration angegeben haben. Amazon S3 verwendet das Präfix als Ordnernamen im Bucket.
`raw`	Der Ordner, in dem Zeitreihendaten von Geräten (Messungen) gespeichert werden. Der `raw` Ordner wird im Präfixordner gespeichert.
`seriesBucket`	Eine Hexadezimalzahl zwischen 00 und ff. Diese Zahl ist abgeleitet von. `timeSerie`

Pfadkomponente	Beschreibung
	`sId` Diese Partition wird verwendet, um den Durchsatz bei AWS IoT SiteWise Schreibvorgängen auf das Cold-Tier zu erhöhen. Wenn Sie Amazon Athena zum Ausführen von Abfragen verwenden, können Sie die Partition für eine detaillierte Partitionierung verwenden, um die Abfrageleistung zu verbessern. `seriesBucket` und `timeSeriesBucket` in den Asset-Metadaten steht dieselbe Zahl.
`startYear`	Das Jahr der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist.
`startMonth`	Der Monat der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist.
`startDay`	Der Tag des Monats, an dem die exklusive Startzeit den Zeitreihendaten zugeordnet ist.

Pfadkomponente	Beschreibung
`fileName`	Der Dateiname verwendet den Unterstrich (_) als Trennzeichen, um Folgendes zu trennen: • Das Präfix. `raw` • Der `timeSeriesId` Wert. • Der Epochenzeitstempel der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist. • Die Qualität der Daten. Gültige Werte: `GOODBAD`, und`UNCERTAIN` . Weitere Informationen finden Sie unter AssetPropertyValue in der AWS IoT SiteWise API-Referenz. Die Datei wird mithilfe der Snappy-Komprimierung in dem `.avro` Format gespeichert.

Example Dateipfad zu den Rohdaten in der kalten Ebene

```
keyPrefix/raw/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
raw_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Felder

Das Schema der Rohdaten, die in die Cold-Tier exportiert werden, enthält die folgenden Felder.

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
`seriesId`	`string`	N/A	Die ID, die die Zeitreihendaten von Geräten (Messungen) identifiziert. Sie können dieses

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
			Feld verwenden, um Rohdaten und Asset-Metadaten in Abfragen zu verknüpfen.
`timeInSeconds`	`long`	N/A	Das Zeitstempeldatum in Sekunden im Unix-Epochenformat. Daten in Bruchteilen von Nanosekunden werden bereitgestellt von. `offsetInNanos`
`offsetInNanos`	`long`	N/A	Der Nanosekunden-Offset von. `timeInSeconds`
`quality`	`string`	N/A	Die Qualität des Zeitreihenwerts.
`doubleValue`	`double` oder `null`	`null`	Zeitreihendaten vom Typ Double (Fließkommazahl).
`stringValue`	`string` oder `null`	`null`	Zeitreihendaten vom Typ Zeichenfolge (Zeichenfolge).
`integerValue`	`int` oder `null`	`null`	Zeitreihendaten vom Typ Integer (ganze Zahl).

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
`booleanValue`	`boolean` oder `null`	`null`	Zeitreihendaten vom Typ Boolean (wahr oder falsch).
`jsonValue`	`string` oder `null`	`null`	Zeitreihendaten des Typs JSON (komplexe Datentypen, die als Zeichenfolge gespeichert werden).
`recordVersion`	`long` oder `null`	`null`	Die Versionsnummer für den Datensatz. Sie können die Versionsnummer verwenden, um den neuesten Datensatz auszuwählen. Neuere Datensätze haben größere Versionsnummern.

Example Rohdaten in der kalten Stufe

```
{"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675887,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.75},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675889,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.69},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675890,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.66},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675891,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.92},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
```

```
  {"seriesId":"e9687d2a-0dbe-4f65-9ed6-6f443cba41f7_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeInSeconds":1625675892,"offsetInNanos":0,"quality":"GOOD","doubleValue":
{"double":0.73},"stringValue":null,"integerValue":null,"booleanValue":null,"jsonValue":null,"re
```

Metriken, Transformationen und Aggregationen

AWS IoT SiteWise exportiert alle sechs Stunden Metriken, Transformationen und Aggregationen in das Cold-Tier. Metriken, Transformationen und Aggregate werden im Cold-Tier im Apache AVRO () - Format gespeichert. `.avro`

Dateipfad

AWS IoT SiteWise speichert Metriken, Transformationen und Aggregate im Cold-Tier mithilfe der folgenden Vorlage.

```
{keyPrefix}/agg/startYear={startYear}/startMonth={startMonth}/startDay={startDay}/
seriesBucket={seriesBucket}/agg_{timeseriesId}_{startTimestamp}_{quality}.avro
```

Jeder Dateipfad zu Metriken, Transformationen und Aggregationen in Amazon S3 enthält die folgenden Komponenten.

Pfadkomponente	Beschreibung
`keyPrefix`	Das Amazon S3 S3-Präfix, das Sie in der AWS IoT SiteWise Speicherkonfiguration angegeben haben. Amazon S3 verwendet das Präfix als Ordnernamen im Bucket.
`agg`	Der Ordner, in dem Zeitreihendaten aus Metriken gespeichert werden. Der `agg` Ordner wird im Präfixordner gespeichert.
`seriesBucket`	Eine Hexadezimalzahl zwischen 00 und ff. Diese Zahl ist abgeleitet von. `timeSerie sId` Diese Partition wird verwendet, um den Durchsatz bei AWS IoT SiteWise Schreibvo rgängen auf das Cold-Tier zu erhöhen. Wenn Sie Amazon Athena zum Ausführen von Abfragen verwenden, können Sie die Partition

Pfadkomponente	Beschreibung
	für eine detaillierte Partitionierung verwenden, um die Abfrageleistung zu verbessern. `seriesBucket` und `timeSeriesBucket` in den Asset-Metadaten steht dieselbe Zahl.
`startYear`	Das Jahr der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist.
`startMonth`	Der Monat der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist.
`startDay`	Der Tag des Monats, an dem die exklusive Startzeit den Zeitreihendaten zugeordnet ist.
`fileName`	Der Dateiname verwendet den Unterstrich (_) als Trennzeichen, um Folgendes zu trennen: • Das Präfix. `raw` • Der `timeSeriesId` Wert. • Der Epochenzeitstempel der exklusiven Startzeit, die den Zeitreihendaten zugeordnet ist. • Die Qualität der Daten. Gültige Werte: `GOOD`, `BAD`, und `UNCERTAIN`. Weitere Informationen finden Sie unter AssetPropertyValue in der AWS IoT SiteWise API-Referenz. Die Datei wird mithilfe der Snappy-Komprimierung in dem `.avro` Format gespeichert.

Example Dateipfad zu den Messwerten in der kalten Stufe

```
keyPrefix/agg/startYear=2021/startMonth=1/startDay=2/seriesBucket=a2/
agg_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1609577700_GOOD.avro
```

Felder

Das Schema der Metriken, Transformationen und Aggregate, die in das Cold-Tier exportiert werden, enthält die folgenden Felder.

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
`seriesId`	`string`	N/A	Die ID, die die Zeitreihendaten von Geräten, Metriken oder Transform ationen identifiziert. Sie können dieses Feld verwenden, um Rohdaten und Asset-Metadaten in Abfragen zu verknüpfen.
`timeInSeconds`	`long`	N/A	Das Zeitstemp eldatum in Sekunden im Unix-Epoc henformat. Daten in Bruchteilen von Nanosekunden werden bereitges tellt von. `offsetInN anos`
`offsetInNanos`	`long`	N/A	Der Nanosekun den-Offset von. `timeInSeconds`

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
`quality`	`string`	N/A	Die Qualität, nach der Anlagendaten gefiltert werden sollen.
`resolution`	`string`	N/A	Das Zeitintervall, über das Daten aggregiert werden sollen.
`count`	`double` oder `null`	`null`	Die Gesamtzahl der Datenpunkte für die angegebenen Variablen im aktuellen Zeitintervall.
`average`	`double` oder `null`	`null`	Der Mittelwert der Werte der angegeben en Variablen im aktuellen Zeitintervall.
`min`	`double` oder `null`	`null`	Das Minimum der Werte der angegeben en Variablen im aktuellen Zeitintervall.
`max`	`boolean` oder `null`	`null`	Das Maximum der Werte der angegeben en Variablen im aktuellen Zeitintervall.
`sum`	`string` oder `null`	`null`	Die Summe der Werte der angegebenen Variablen im aktuellen Zeitintervall.

Feldname	Unterstützte -Typen	-Standardtyp	Beschreibung
`recordVersion`	`long` oder `null`	`null`	Die Versionsnummer für den Datensatz. Sie können die Versionsnummer verwenden, um den neuesten Datensatz auszuwählen. Neuere Datensätze haben größere Versionsnummern.

Example Metrische Daten in der kalten Stufe

```
{"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334060,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334120,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334540,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637334600,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":46.0},"min":{"double":32.0},"max":{"double":60.0},"sum":
{"double":1334.0},"recordVersion":null}
  {"seriesId":"f74c2828-5317-4df3-
ba16-6d41b5bcb531","timeInSeconds":1637335020,"offsetInNanos":0,"quality":"GOOD","resolution":"
{"double":16.0},"min":{"double":1.0},"max":{"double":31.0},"sum":
{"double":496.0},"recordVersion":null}
```

Asset-Metadaten

Wenn Sie AWS IoT SiteWise zum ersten Mal den Export von Daten in die kalte Ebene aktivieren, werden Asset-Metadaten in die kalte Ebene exportiert. AWS IoT SiteWise Exportiert nach der

Erstkonfiguration Asset-Metadaten nur dann in die Ebene, wenn Sie Asset-Modelldefinitionen oder Asset-Definitionen ändern. Asset-Metadaten werden in der kalten Ebene im durch Zeilenumbrüche getrennten JSON () `.ndjson` -Format gespeichert.

Dateipfad

AWS IoT SiteWise speichert Asset-Metadaten unter Verwendung der folgenden Vorlage in der kalten Ebene.

```
{keyPrefix}/asset_metadata/asset_{assetId}.ndjson
```

Jeder Dateipfad zu Asset-Metadaten in der kalten Ebene enthält die folgenden Komponenten.

Pfadkomponente	Beschreibung
`keyPrefix`	Das Amazon S3 S3-Präfix, das Sie in der Speicherkonfiguration AWS IoT SiteWise s angegeben haben. Amazon S3 verwendet das Präfix als Ordnernamen im Bucket.
`asset_metadata`	Der Ordner, der Asset-Metadaten speichert . Der `asset_metadata` Ordner wird im Präfixordner gespeichert.
`fileName`	Der Dateiname verwendet den Unterstrich (_) als Trennzeichen, um Folgendes zu trennen: • Das Präfix. `asset` • Der `assetId` Wert. Die Datei wird im `.ndjson` Format gespeichert.

Example Dateipfad zu den Asset-Metadaten in der kälteren Ebene

`keyPrefix/asset_metadata/asset_35901915-d476-4dca-8637-d9ed4df939ed.ndjson`

Felder

Das Schema der Asset-Metadaten, das in die kalte Ebene exportiert wird, enthält die folgenden Felder.

Feldname	Beschreibung
`assetId`	Die ID der -Komponente.
`assetName`	Der Name des Assets.
`assetExternalId`	Die externe ID des Assets.
`assetModelId`	Die ID des Asset-Modells, das zur Erstellung dieses Assets verwendet wurde.
`assetModelName`	Der Name des Asset-Modells.
`assetModelExternalId`	Die externe ID des Asset-Modells.
`assetPropertyId`	Die ID der Asset-Eigenschaft.
`assetPropertyName`	Der Name der Anlageeigenschaft.
`assetPropertyExternalId`	Die externe ID der Anlageeigenschaft.
`assetPropertyDataType`	Der Datentyp der Anlageneigenschaft.
`assetPropertyUnit`	Die Einheit der Anlageeigenschaft (z. B. `Newtons` und`RPM`).
`assetPropertyAlias`	Der Alias, der die Asset-Eigenschaft identifiziert, z. B. ein OPC-UA-Serverdatenstream-Pfad (zum Beispiel`/company/windfarm/3/turbine/7/temperature`).
`timeSeriesId`	Die ID, die die Zeitreihendaten von Geräten, Metriken oder Transformationen identifiziert. Sie können dieses Feld verwenden, um

Feldname	Beschreibung
	Rohdaten und Asset-Metadaten in Abfragen zu verknüpfen.
`timeSeriesBucket`	Eine Hexadezimalzahl zwischen 00 und ff. Diese Zahl ist abgeleitet von. `timeSeriesId` Diese Partition wird verwendet, um den Durchsatz bei AWS IoT SiteWise Schreibvorgängen auf das Cold-Tier zu erhöhen. Wenn Sie Amazon Athena zum Ausführen von Abfragen verwenden, können Sie die Partition für eine detaillierte Partitionierung verwenden, um die Abfrageleistung zu verbessern. `timeSeriesBucket` und `seriesBucket` im Dateipfad zu den Rohdaten stehen dieselben Zahlen.
`assetCompositeModelId`	Die ID des zusammengesetzten Modells.
`assetCompositeModelExternalId`	Die externe ID des zusammengesetzten Modells.
`assetCompositeModelDescription`	Die Beschreibung des zusammengesetzten Modells.
`assetCompositeModelName`	Der Name des zusammengesetzten Modells.
`assetCompositeModelType`	Der Typ des zusammengesetzten Modells. Bei zusammengesetzten Alarmmodellen ist dieser Typ `AWS/ALARM` .
`assetCreationDate`	Das Datum, an dem das Asset erstellt wurde, in Unix-Epochenzeit.
`assetLastUpdateDate`	Das Datum, an dem das Asset zuletzt aktualisiert wurde, in Unix-Epochenzeit.

Feldname	Beschreibung
`assetStatusErrorCode`	Der Fehlercode.
`assetStatusErrorMessage`	Die Fehlermeldung.
`assetStatusState`	Der aktuelle Status des Assets.

Example Asset-Metadaten auf der kalten Ebene


```
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"95e63da7-d34e-43e1-
bc6f-1b490154b07a","assetPropertyExternalId":null,"assetPropertyName":"Temperature","assetPrope
Washington/Seattle/WT2/temp","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a","timeSeriesBucket":"f6","assetArn":null,"assetCompositeModelDescription":nul
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind Turbine Asset
 Model","assetPropertyId":"c706d54d-4c11-42dc-9a01-63662fc697b4","assetPropertyExternalId":null
Washington/Seattle/WT2/pressure","timeSeriesId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d_c706d54d-4c11-42dc-9a01-63662fc697b4","timeSeriesBucket":"1e","assetArn":null,"ass
  {"assetId":"7020c8e2-e6db-40fa-9845-
ed0dddd4c77d","assetExternalId":null,"assetName":"Wind Turbine Asset
 2","assetModelId":"ec1d924f-f07d-444f-b072-
e2994c165d35","assetModelExternalId":null,"assetModelName":"Wind
 Turbine Asset Model","assetPropertyId":"8cf1162f-dead-4fbe-b468-
c8e24cde9f50","assetPropertyExternalId":null,"assetPropertyName":"Max
 Temperature","assetPropertyDataType":"DOUBLE","assetPropertyUnit":null,"assetPropertyAlias":nu
e6db-40fa-9845-ed0dddd4c77d_8cf1162f-dead-4fbe-b468-
c8e24cde9f50","timeSeriesBucket":"d7","assetArn":null,"assetCompositeModelDescription":null,"as

 {"assetId":"3a5f2a22-3b37-4332-9c1c-404ea1d73fab","assetExternalId":null,"assetName":"BatchAss
ebc75e75e827","assetModelExternalId":null,"assetModelName":"FlashTestAssetModelDouble","assetPr
b410-
ab401a9176ed","assetPropertyExternalId":null,"assetPropertyName":"measurementProperty","assetPr
ae89-
```

ff316f5ff8aa","timeSeriesBucket":"af","assetArn":null,"assetCompositeModelDescription":null,"as

Metadaten der Asset-Hierarchie

Wenn Sie das Speichern von Daten AWS IoT SiteWise auf der kalten Ebene zum ersten Mal aktivieren, werden Metadaten der Asset-Hierarchie in die kalte Ebene exportiert. AWS IoT SiteWise Exportiert nach der Erstkonfiguration Metadaten der Asset-Hierarchie nur dann in die Cold-Tier, wenn Sie Änderungen am Asset-Modell oder an den Asset-Definitionen vornehmen. Metadaten der Asset-Hierarchie werden in der kalten Ebene im durch Zeilenumbrüche getrennten JSON () `.ndjson` - Format gespeichert.

Eine externe Kennung für die Hierarchie, das Ziel-Asset oder das Quell-Asset wird durch Aufrufen der API abgerufen. DescribeAsset

Dateipfad

AWS IoT SiteWise speichert Metadaten der Asset-Hierarchie auf der kalten Ebene mithilfe der folgenden Vorlage.

```
{keyPrefix}/asset_hierarchy_metadata/{parentAssetId}_{hierarchyId}.ndjson
```

Jeder Dateipfad zu den Metadaten der Asset-Hierarchie in der kalten Ebene enthält die folgenden Komponenten.

Pfadkomponente	Beschreibung
`keyPrefix`	Das Amazon S3 S3-Präfix, das Sie in der AWS IoT SiteWise Speicherkonfiguration angegeben haben. Amazon S3 verwendet das Präfix als Ordnernamen im Bucket.
`asset_hierarchy_metadata`	Der Ordner, in dem Metadaten der Asset-Hierarchie gespeichert werden. Der `asset_hierarchy_metadata` Ordner wird im Präfixordner gespeichert.

Pfadkomponente	Beschreibung
`fileName`	Der Dateiname verwendet den Unterstrich (_) als Trennzeichen, um Folgendes zu trennen: • Der Wert. `parentAssetId` • Der `hierarchyId` Wert. Die Datei wird im `.ndjson` Format gespeichert.

Example Dateipfad zu den Metadaten der Asset-Hierarchie in der kalten Ebene

```
keyPrefix/asset_hierarchy_metadata/35901915-d476-4dca-8637-
d9ed4df939ed_c5b3ced8-589a-48c7-9998-cdccfc9747a0.ndjson
```

Felder

Das Schema der Metadaten der Asset-Hierarchie, das in die kalte Ebene exportiert wird, enthält die folgenden Felder.

Feldname	Beschreibung
`sourceAssetId`	Die ID des Quell-Assets in dieser Asset-Bez iehung.
`targetAssetId`	Die ID der Zielanlage in dieser Vermögens beziehung.
`hierarchyId`	Die ID der Hierarchie.
`associationType`	Der Zuordnungstyp dieser Vermögens beziehung. Der Wert muss sein`CHILD`. Die Zielanlage ist eine untergeordnete Anlage der Quellanlage.

Example Metadaten der Asset-Hierarchie auf der kalten Ebene

```
{"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"2b866c25-0c74-4750-bdf5-
b73683c8a2a2","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
  {"sourceAssetId":"80388e72-2284-44fb-9c89-
bfbaf0dfedd2","targetAssetId":"6b51246e-984d-460d-
bc0b-470ea47d1e31","hierarchyId":"bbed9f59-0412-4585-
a61d-6044db526aee","associationType":"CHILD"}
```

Um Ihre Daten auf der kalten Ebene anzuzeigen

1. Navigieren Sie zur Amazon S3 S3-Konsole.
2. Wählen Sie im Navigationsbereich Buckets und dann Ihren Amazon S3 S3-Bucket aus.
3. Navigieren Sie zu dem Ordner, der die Rohdaten, Asset-Metadaten oder Asset-Hierarchie-Metadaten enthält.
4. Wählen Sie die Dateien aus, und klicken Sie dann unter Aktionen auf Herunterladen.

Speicherdaten, Indexdateien

AWS IoT SiteWise verwendet diese Dateien, um die Leistung von Datenabfragen zu optimieren. Sie werden in Ihrem Amazon S3 S3-Bucket angezeigt, aber Sie müssen sie nicht verwenden.

Dateipfad

AWS IoT SiteWise speichert Datenindexdateien mithilfe der folgenden Vorlage im Cold-Tier.

```
keyPrefix/index/series=timeseriesId/startYear=startYear/startMonth=startMonth/
startDay=startDay/index_timeseriesId_startTimestamp_quality
```

Example Dateipfad zur Datenspeicher-Indexdatei

```
keyPrefix/index/series=7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-
d34e-43e1-bc6f-1b490154b07a/startYear=2022/startMonth=02/startDay=03/
index_7020c8e2-e6db-40fa-9845-ed0dddd4c77d_95e63da7-d34e-43e1-
bc6f-1b490154b07a_1643846400_GOOD
```

Sicherheit in AWS IoT SiteWise

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

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

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

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

Themen

- Bewährte Sicherheitsmethoden für AWS IoT SiteWise

Datenschutz in AWS IoT SiteWise

Das AWS Modell der gilt für den Datenschutz in AWS IoT SiteWise. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

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

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS IoT SiteWise oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben,

die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen

Richtlinie für den Datenverkehr zwischen Netzwerken

Verbindungen zwischen AWS IoT SiteWise und lokalen Anwendungen, wie SiteWise Edge-Gateways, werden über TLS-Verbindungen (Transport Layer Security) gesichert. Weitere Informationen finden Sie unter Verschlüsselung während der Übertragung.

AWS IoT SiteWise unterstützt keine Verbindungen zwischen Availability Zones innerhalb einer AWS Region oder Verbindungen zwischen AWS Konten.

Sie können IAM Identity Center jeweils nur in einer Region konfigurieren. SiteWise Monitor stellt eine Verbindung zu der Region her, die Sie für IAM Identity Center konfiguriert haben. Das bedeutet, dass Sie eine Region für den Zugriff auf das IAM Identity Center verwenden, aber Sie können Portale in jeder Region erstellen.

Datenverschlüsselung

Datenverschlüsselung bezieht sich auf den Schutz von Daten während der Übertragung (bei der Übertragung zu und von AWS IoT SiteWise und zwischen SiteWise Edge-Gateways und -Servern) und im Ruhezustand (während sie auf lokalen Geräten oder in AWS Diensten gespeichert werden). Sie können Daten während der Übertragung mit TLS (Transport Layer Security) oder im Ruhezustand mit clientseitiger Verschlüsselung schützen.

> **Note**
>
> AWS IoT SiteWise Die Edge-Verarbeitung macht APIs verfügbar, die auf SiteWise Edge-Gateways gehostet werden und auf die über das lokale Netzwerk zugegriffen werden kann. Diese APIs werden über eine TLS-Verbindung verfügbar gemacht, die durch ein Serverzertifikat gestützt wird, das dem AWS IoT SiteWise Edge-Connector gehört. Für die Client-Authentifizierung verwenden diese APIs ein Passwort für die Zugriffskontrolle. Der

private Schlüssel des Serverzertifikats und das Passwort für die Zugriffskontrolle werden beide auf der Festplatte gespeichert. AWS IoT SiteWise Die Edge-Verarbeitung stützt sich auf die Dateisystemverschlüsselung, um die Sicherheit dieser Anmeldeinformationen im Ruhezustand zu gewährleisten.

Weitere Informationen zur serverseitigen Verschlüsselung und zur clientseitigen Verschlüsselung finden Sie in den unten aufgeführten Themen.

Themen

Verschlüsselung im Ruhezustand

AWS IoT SiteWise speichert Ihre Daten in der AWS Cloud und auf AWS IoT SiteWise Edge-Gateways.

Daten im Ruhezustand in der Cloud AWS

AWS IoT SiteWise speichert Daten in anderen AWS Diensten, die Daten im Ruhezustand standardmäßig verschlüsseln. Encryption at Rest ist in AWS Key Management Service (AWS KMS) integriert, um den Verschlüsselungsschlüssel zu verwalten, der zum Verschlüsseln Ihrer Objektwerte und Aggregatwerte in verwendet wird. AWS IoT SiteWise Sie können sich dafür entscheiden, einen vom Kunden verwalteten Schlüssel zur Verschlüsselung von Vermögenswerten und Aggregatwerten in zu verwenden. AWS IoT SiteWise Sie können Ihren Verschlüsselungsschlüssel über AWS KMS erstellen, verwalten und einsehen.

Sie können einen auswählen, AWS-eigener Schlüssel um Ihre Daten zu verschlüsseln, oder einen vom Kunden verwalteten Schlüssel wählen, um Ihre Immobilienwerte und aggregierten Werte zu verschlüsseln:

Funktionsweise

Encryption at Rest ist in die Verwaltung des Verschlüsselungsschlüssels integriert, der zur Verschlüsselung Ihrer Daten verwendet wird. AWS KMS

- AWS-eigener Schlüssel — Standard-Verschlüsselungsschlüssel. AWS IoT SiteWise besitzt diesen Schlüssel. Sie können diesen Schlüssel nicht in Ihrem AWS Konto einsehen. Sie können auch keine Operationen mit dem Schlüssel in den AWS CloudTrail Protokollen sehen. Sie können diesen Schlüssel ohne zusätzliche Kosten verwenden.
- Vom Kunden verwalteter Schlüssel — Der Schlüssel wird in Ihrem Konto gespeichert, das Sie erstellen, besitzen und verwalten. Sie haben die volle Kontrolle über den KMS-Schlüssel. Es AWS KMS fallen zusätzliche Gebühren an.

AWS-eigene Schlüssel

AWS-eigene Schlüssel sind nicht in Ihrem Konto gespeichert. Sie sind Teil einer Sammlung von KMS-Schlüsseln, die AWS Eigentümer sind und für die Verwendung in mehreren AWS Konten verwaltet werden. AWS Dienste, die Sie AWS-eigene Schlüssel zum Schutz Ihrer Daten verwenden können.

Sie können ihre Verwendung nicht einsehen, verwalten AWS-eigene Schlüssel, verwenden oder überprüfen. Sie müssen jedoch keine Arbeit verrichten oder Programme ändern, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden.

Für die Nutzung wird Ihnen keine monatliche Gebühr oder Nutzungsgebühr berechnet AWS-eigene Schlüssel, und sie werden auch nicht auf die AWS KMS Kontingente für Ihr Konto angerechnet.

Kundenverwaltete Schlüssel

Kundenverwaltete Schlüssel sind KMS-Schlüssel in Ihrem , die Sie erstellen, besitzen und verwalten. Sie haben die volle Kontrolle über diese KMS-Schlüssel, z. B. über die folgenden:

- Festlegung und Pflege ihrer wichtigsten Richtlinien, IAM-Richtlinien und Zuschüsse
- Sie aktivieren und deaktivieren
- Rotation ihres kryptografischen Materials
- Hinzufügen von Tags
- Aliase erstellen, die auf sie verweisen
- Sie für das Löschen planen

Sie können auch Amazon CloudTrail CloudWatch Logs verwenden, um die Anfragen zu verfolgen, die in Ihrem Namen AWS IoT SiteWise AWS KMS an gesendet werden.

Wenn Sie vom Kunden verwaltete Schlüssel verwenden, müssen Sie AWS IoT SiteWise Zugriff auf den in Ihrem Konto gespeicherten KMS-Schlüssel gewähren. AWS IoT SiteWise verwendet Umschlagverschlüsselung und Schlüsselhierarchie, um Daten zu verschlüsseln. Ihr AWS KMS Verschlüsselungsschlüssel wird verwendet, um den Stammschlüssel dieser Schlüsselhierarchie zu verschlüsseln. Weitere Informationen zur Envelope-Verschlüsselung finden Sie im AWS Key Management Service -Entwicklerhandbuch.

Die folgende Beispielrichtlinie gewährt einem Benutzer die AWS IoT SiteWise Erlaubnis, in Ihrem Namen einen vom Kunden verwalteten Schlüssel zu erstellen. Wenn Sie Ihren Schlüssel erstellen, müssen Sie die `kms:DescribeKey` Aktionen `kms:CreateGrant` und zulassen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1603902045292",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Der Verschlüsselungskontext für Ihren erstellten Zuschuss verwendet Ihre Konto-ID `aws:iotsitewise:subscriberId` und Ihre Konto-ID.

Daten im Ruhezustand auf SiteWise Edge-Gateways

AWS IoT SiteWise Gateways speichern die folgenden Daten im lokalen Dateisystem:

- Konfigurationsinformationen zu OPC-UA-Quellen
- Der Satz von OPC-UA-Datenstrompfaden von verbundenen OPC-UA-Quellen
- Industriedaten werden zwischengespeichert, wenn das SiteWise Edge-Gateway die Verbindung zum Internet verliert

SiteWise Edge-Gateways laufen auf. AWS IoT Greengrass AWS IoT Greengrass stützt sich auf Unix-Dateiberechtigungen und vollständige Festplattenverschlüsselung (falls aktiviert), um Daten zu

schützen, die sich auf dem Kern befinden. Es liegt in Ihrer Verantwortung, das Dateisystem und das Gerät zu sichern.

Verschlüsselt AWS IoT Greengrass jedoch lokale Kopien Ihrer OPC-UA-Servergeheimnisse, die Sie aus Secrets Manager abgerufen haben. Weitere Informationen finden Sie unter Secrets-Verschlüsselung im Developer Guide.AWS IoT Greengrass Version 1

Weitere Informationen zur Verschlüsselung ruhender AWS IoT Greengrass Kerne finden Sie unter Verschlüsselung im Ruhezustand im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

Verschlüsselung während der Übertragung

AWS IoT SiteWise hat drei Kommunikationsmodi, bei denen Daten übertragen werden:

- Über das Internet — Die Kommunikation zwischen lokalen Geräten (einschließlich SiteWise Edge-Gateways) AWS IoT SiteWise erfolgt verschlüsselt.
- Über das lokale Netzwerk — Die Kommunikation zwischen unseren OpsHub SiteWise Anwendungen und SiteWise Edge-Gateways ist immer verschlüsselt. Die Kommunikation zwischen der SiteWise Monitor-Anwendung, die in Ihrem Browser ausgeführt wird, und den SiteWise Edge-Gateways ist immer verschlüsselt. Die Kommunikation zwischen SiteWise Edge-Gateways und OPC-UA-Quellen kann verschlüsselt werden.
- Zwischen Komponenten auf SiteWise Edge-Gateways — Die Kommunikation zwischen AWS IoT Greengrass Komponenten auf SiteWise Edge-Gateways ist nicht verschlüsselt.

Themen

- Daten in Übertragung über das Internet
- Daten in Übertragung über das lokale Netzwerk
- Daten werden zwischen lokalen Komponenten auf SiteWise Edge-Gateways übertragen

Daten in Übertragung über das Internet

AWS IoT SiteWise verwendet Transport Layer Security (TLS), um die gesamte Kommunikation über das Internet zu verschlüsseln. Alle an die AWS Cloud gesendeten Daten werden über eine TLS-Verbindung unter Verwendung der Protokolle MQTT oder HTTPS gesendet, sodass sie standardmäßig sicher sind. SiteWise Edge-Gateways, die laufen AWS IoT Greengrass, und Benachrichtigungen über Eigenschaftswerte verwenden das AWS IoT Transportsicherheitsmodell. Weitere Informationen finden Sie unter Transportsicherheit im AWS IoT -Entwicklerhandbuch.

Daten in Übertragung über das lokale Netzwerk

SiteWise Edge-Gateways folgen den OPC-UA-Spezifikationen für die Kommunikation mit lokalen OPC-UA-Quellen. Sie sind dafür verantwortlich, Ihre Quellen für die Verwendung eines Nachrichtensicherheitsmodus zu konfigurieren, der Daten während der Übertragung verschlüsselt.

Wenn Sie einen Sicherheitsmodus für Signnachrichten wählen, werden Daten, die zwischen SiteWise Edge-Gateways und Quellen übertragen werden, signiert, aber nicht verschlüsselt. Wenn Sie einen Sicherheitsmodus zum Signieren und Verschlüsseln von Nachrichten wählen, werden die Daten, die zwischen SiteWise Edge-Gateways und Quellen übertragen werden, signiert und verschlüsselt. Weitere Informationen zur Konfiguration von Quellen finden Sie unter Konfigurieren von Datenquellen.

Die Kommunikation zwischen der Edge-Konsolenanwendung und den SiteWise Edge-Gateways wird immer mit TLS verschlüsselt. Der SiteWise Edge-Connector auf dem SiteWise Edge-Gateway generiert und speichert ein selbstsigniertes Zertifikat, um eine TLS-Verbindung mit der Edge-Konsole für AWS IoT SiteWise die Anwendung herstellen zu können. Sie müssen dieses Zertifikat für die AWS IoT SiteWise Anwendung von Ihrem SiteWise Edge-Gateway auf die Edge-Konsole kopieren, bevor Sie die Anwendung mit dem SiteWise Edge-Gateway verbinden. Dadurch wird sichergestellt, dass die Edge-Konsole für die AWS IoT SiteWise Anwendung überprüfen kann, ob sie eine Verbindung zu Ihrem vertrauenswürdigen SiteWise Edge-Gateway hergestellt hat.

Zusätzlich zu TLS für Geheimhaltung und Serverauthentizität verwendet SiteWise Edge das SigV4-Protokoll, um die Authentizität der Edge-Konsolenanwendung festzustellen. Der SiteWise Edge-Connector auf dem SiteWise Edge-Gateway akzeptiert und speichert ein Passwort, um eingehende Verbindungen von der Edge-Konsolenanwendung, der SiteWise Monitor-Anwendung, die in Browsern ausgeführt wird, und anderen Clients, die auf dem SDK basieren, verifizieren zu können. AWS IoT SiteWise

Weitere Informationen zum Generieren des Kennworts und des Serverzertifikats finden Sie unterthe section called “Verwalten von SiteWise Edge-Gateways”.

Daten werden zwischen lokalen Komponenten auf SiteWise Edge-Gateways übertragen

SiteWise Edge-Gateways laufen auf AWS IoT Greengrass, wodurch Daten, die lokal auf dem AWS IoT Greengrass Core ausgetauscht werden, nicht verschlüsselt werden, da die Daten das Gerät nicht verlassen. Dazu gehört auch die Kommunikation zwischen AWS IoT Greengrass Komponenten wie

dem AWS IoT SiteWise Connector. Weitere Informationen finden Sie unter Daten auf dem Kerngerät im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

Schlüsselverwaltung

AWS IoT SiteWise Verwaltung von Cloud-Schlüsseln

Wird standardmäßig Von AWS verwaltete Schlüssel zum Schutz Ihrer Daten in der AWS Cloud AWS IoT SiteWise verwendet. Sie können Ihre Einstellungen aktualisieren, um einige Daten mit einem vom Kunden verwalteten Schlüssel zu verschlüsseln. AWS IoT SiteWise Sie können Ihren Verschlüsselungsschlüssel über AWS Key Management Service (AWS KMS) erstellen, verwalten und einsehen.

AWS IoT SiteWise unterstützt serverseitige Verschlüsselung mit vom Kunden verwalteten Schlüsseln AWS KMS , um die folgenden Daten zu verschlüsseln:

- Eigenschaftswerte von Vermögenswerten
- Werte aggregieren

> **Note**
>
> Andere Daten und Ressourcen werden mit der Standardverschlüsselung mit Schlüsseln verschlüsselt, die von verwaltet werden AWS IoT SiteWise. Dieser Schlüssel wird im AWS IoT SiteWise Konto gespeichert.

Weitere Informationen finden Sie unter Was ist AWS Key Management Service? im AWS Key Management Service Entwicklerhandbuch.

Aktivieren Sie die Verschlüsselung mit vom Kunden verwalteten Schlüsseln

Um vom Kunden verwaltete Schlüssel mit verwenden zu können AWS IoT SiteWise, müssen Sie Ihre AWS IoT SiteWise Einstellungen aktualisieren.

Um die Verschlüsselung mit KMS-Schlüsseln zu aktivieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie Kontoeinstellungen und dann Bearbeiten, um die Seite Kontoeinstellungen bearbeiten zu öffnen.

3. Wählen Sie als Typ des Verschlüsselungsschlüssels die Option Anderen AWS KMS Schlüssel auswählen aus. Dies ermöglicht die Verschlüsselung mit vom Kunden verwalteten Schlüsseln, die in gespeichert sind AWS KMS.

   > **Note**
   >
   > Derzeit können Sie die vom Kunden verwaltete Schlüsselverschlüsselung nur für Immobilienwerte und aggregierte Werte verwenden.

4. Wählen Sie Ihren KMS-Schlüssel mit einer der folgenden Optionen:

   - Um einen vorhandenen KMS-Schlüssel zu verwenden — Wählen Sie Ihren KMS-Schlüsselalias aus der Liste aus.
   - Um einen neuen KMS-Schlüssel zu erstellen — Wählen Sie Create an AWS KMS key.

   > **Note**
   >
   > Dadurch wird das AWS KMS -Dashboard geöffnet. Weitere Informationen zum Erstellen eines KMS-Schlüssels finden Sie unter Creating Keys im AWS Key Management Service Developer Guide.

5. Wählen Sie Speichern, um Ihre Einstellungen zu aktualisieren.

SiteWise Schlüsselverwaltung für das Edge-Gateway

SiteWise Edge-Gateways laufen auf und AWS IoT Greengrass Kerngeräte verwenden öffentliche und private Schlüssel AWS IoT Greengrass, um sich bei der AWS Cloud zu authentifizieren und lokale Geheimnisse wie OPC-UA-Authentifizierungsgeheimnisse zu verschlüsseln. Weitere Informationen finden Sie unter Schlüsselverwaltung im Entwicklerhandbuch.AWS IoT Greengrass Version 1

Identitäts- und Zugriffsmanagement für AWS IoT SiteWise

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

Themen

Zielgruppe

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

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

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

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

Authentifizierung mit Identitäten

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

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

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

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

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

AWS-Konto Root-Benutzer

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

Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

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

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

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

IAM-Rollen

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

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM

erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

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

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

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

Wie AWS IoT SiteWise funktioniert mit IAM

Bevor Sie AWS Identity and Access Management (IAM) zur Verwaltung des Zugriffs auf verwenden AWS IoT SiteWise, sollten Sie wissen, mit welchen IAM-Funktionen Sie arbeiten können. AWS IoT SiteWise

IAM-Feature	Unterstzt von? AWS IoT SiteWis
Identitätsbasierte Richtlinien mit Berechtigungen auf Ressourcenebene	Ja

IAM-Feature	Unterstzt von? AWS IoT SiteWis
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
Ressourcenbasierte Richtlinien	Nein
Zugriffssteuerungslisten (ACLs)	Nein
Tag-basierte Autorisierung (ABAC)	Ja
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten (FAS)	Ja
Service-verknüpfte Rollen	Ja
Servicerollen	Ja

Einen allgemeinen Überblick darüber, wie AWS IoT SiteWise und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Inhalt

- Autorisierung auf der Basis von AWS IoT SiteWise -Tags
- AWS IoT SiteWise identitätsbasierte Richtlinien
  - Richtlinienaktionen
    - BatchPutAssetPropertyValue Autorisierung
  - Richtlinienressourcen
  - Bedingungsschlüssel für die Richtlinie
  - Beispiele
- AWS IoT SiteWise Beispiele für identitätsbasierte Richtlinien
  - Bewährte Methoden für Richtlinien
  - Verwenden der AWS IoT SiteWise -Konsole
  - Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen
  - Ermöglicht Benutzern, Daten in Komponenten in einer Hierarchie zu erfassen
  - Anzeigen von AWS IoT SiteWise -Komponenten basierend auf Tags
- Verwalten des Zugriffs mit Richtlinien
  - Identitätsbasierte Richtlinien
  - Ressourcenbasierte Richtlinien
  - Zugriffssteuerungslisten (ACLs)
  - Weitere Richtlinientypen
  - Mehrere Richtlinientypen

AWS IoT SiteWise IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

Verwenden temporärer Anmeldeinformationen mit AWS IoT SiteWise

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

AWS IoT SiteWise unterstützt die Verwendung temporärer Anmeldeinformationen.

SiteWise Monitor unterstützt Verbundbenutzer beim Zugriff auf Portale. Portalbenutzer authentifizieren sich mit ihren IAM Identity Center- oder IAM-Anmeldeinformationen.

> **Important**
>
> Benutzer oder Rollen müssen über die `iotsitewise:DescribePortal` Berechtigung verfügen, sich beim Portal anzumelden.

Wenn sich ein Benutzer bei einem Portal anmeldet, generiert SiteWise Monitor eine Sitzungsrichtlinie, die die folgenden Berechtigungen bietet:

- Schreibgeschützter Zugriff auf die Assets und Asset-Daten AWS IoT SiteWise in Ihrem Konto, auf die die Rolle dieses Portals Zugriff gewährt.
- Zugriff auf Projekte in diesem Portal, auf die der Benutzer Administratorzugriff (Projektbesitzer) oder schreibgeschützten Zugriff (Projektanzeiger) hat.

Weitere Informationen zu föderierten Portalbenutzerberechtigungen finden Sie unter Verwenden von Servicerollen für AWS IoT SiteWise Monitor.

Zugriffssitzungen (FAS) weiterleiten für AWS IoT SiteWise

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Service-verknüpfte Rollen

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

AWS IoT SiteWise unterstützt dienstbezogene Rollen. Details zum Erstellen oder Verwalten von serviceverknüpften AWS IoT SiteWise -Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS IoT SiteWise.

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 erscheinen in Ihrem Konto AWS-Konto und gehören dem Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

AWS IoT SiteWise verwendet eine Servicerolle, um SiteWise Monitor-Portalbenutzern den Zugriff auf einige Ihrer AWS IoT SiteWise Ressourcen in Ihrem Namen zu ermöglichen. Weitere Informationen finden Sie unter Verwenden von Servicerollen für AWS IoT SiteWise Monitor.

Sie müssen über die erforderlichen Berechtigungen verfügen, bevor Sie AWS IoT Events Alarmmodelle in erstellen können AWS IoT SiteWise. Weitere Informationen finden Sie unter Berechtigungen für AWS IoT Events Alarme einrichten.

Auswählen einer IAM-Rolle in AWS IoT SiteWise

Wenn Sie eine `portal` Ressource in erstellen AWS IoT SiteWise, müssen Sie eine Rolle auswählen, auf die die Verbundbenutzer Ihres SiteWise Monitor-Portals in AWS IoT SiteWise Ihrem Namen zugreifen können. Wenn Sie zuvor eine Servicerolle erstellt haben, AWS IoT SiteWise erhalten Sie eine Liste mit Rollen, aus denen Sie wählen können. Andernfalls können Sie beim Erstellen eines Portals eine Rolle mit den erforderlichen Berechtigungen erstellen. Es ist wichtig, eine Rolle auszuwählen, die den Zugriff auf Ihre Komponenten und Komponentendaten ermöglicht. Weitere Informationen finden Sie unter Verwenden von Servicerollen für AWS IoT SiteWise Monitor.

Autorisierung auf der Basis von AWS IoT SiteWise -Tags

Sie können Tags an AWS IoT SiteWise Ressourcen anhängen oder Tags in einer Anfrage an diese weitergeben AWS IoT SiteWise. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen über das Markieren von AWS IoT SiteWise -Ressourcen mit Tags finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Anzeigen von AWS IoT SiteWise -Komponenten basierend auf Tags.

AWS IoT SiteWise identitätsbasierte Richtlinien

Mit IAM-Richtlinien können Sie steuern, wer was in tun kann. AWS IoT SiteWise Sie können entscheiden, welche Aktionen zulässig sind oder nicht, und spezifische Bedingungen für diese Aktionen festlegen. Sie können beispielsweise Regeln dafür festlegen, wer Informationen sehen oder ändern kann AWS IoT SiteWise. AWS IoT SiteWise 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.

Richtlinienaktionen

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

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

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

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS IoT SiteWise verwendet:`iotsitewise:`. Um beispielsweise jemandem die Erlaubnis zu erteilen, Objektdaten im Rahmen des `BatchPutAssetPropertyValue` API-Vorgangs hochzuladen, nehmen Sie die `iotsitewise:BatchPutAssetPropertyValue` Aktion in seine Richtlinie auf. AWS IoT SiteWise Richtlinienerklärungen müssen `Action` entweder ein `NotAction` Oder-Element enthalten. AWS IoT SiteWise definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

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

```
"Action": [
  "iotsitewise:action1",
  "iotsitewise: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": "iotsitewise:Describe*"
```

Eine Liste der AWS IoT SiteWise Aktionen finden Sie AWS IoT SiteWise im IAM-Benutzerhandbuch unter Definierte Aktionen von.

BatchPutAssetPropertyValue Autorisierung

AWS IoT SiteWise autorisiert den Zugriff auf die BatchPutAssetPropertyValue-Aktion auf ungewöhnliche Weise. Wenn Sie bei den meisten Aktionen den Zugriff zulassen oder verweigern, gibt diese Aktion einen Fehler zurück, wenn keine Berechtigungen erteilt wurden. Mit `BatchPutAssetPropertyValue` können Sie in einer einzigen API-Anfrage mehrere Dateneinträge an verschiedene Assets und Asset-Eigenschaften senden. AWS IoT SiteWise autorisiert jede Dateneingabe unabhängig. Fügt für jeden einzelnen Eintrag, bei dem die Autorisierung in der Anfrage fehlschlägt AWS IoT SiteWise , eine Fehlerliste `AccessDeniedException` in die zurückgegebene Liste ein. AWS IoT SiteWise empfängt die Daten für jeden Eintrag, der autorisiert wurde und erfolgreich ist, auch wenn ein anderer Eintrag in derselben Anfrage fehlschlägt.

> **Important**
>
> Gehen Sie wie folgt vor, bevor Sie Daten in einen Datenstream aufnehmen:
>
> - Autorisieren Sie die `time-series` Ressource, wenn Sie einen Eigenschaftsalias verwenden, um den Datenstrom zu identifizieren.
> - Autorisieren Sie die `asset` Ressource, wenn Sie eine Asset-ID verwenden, um das Asset zu identifizieren, das die zugehörige Asset-Eigenschaft enthält.

Richtlinienressourcen

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

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

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

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

Jede IAM-Richtlinienanweisung gilt für die Ressourcen, die Sie mithilfe ihrer ARNs angegeben haben. Ein ARN weist die folgende allgemeine Syntax auf:

```
arn:${Partition}:${Service}:${Region}:${Account}:${ResourceType}/${ResourcePath}
```

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

Um beispielsweise die Komponente mit der ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE"
```

Um alle Datenströme anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:iotsitewise:region:123456789012:time-series/*"
```

Um alle Komponenten anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:iotsitewise:region:123456789012:asset/*"
```

Einige AWS IoT SiteWise Aktionen, z. B. die zum Erstellen von Ressourcen, können für eine bestimmte Ressource nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

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

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

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

Bedingungsschlüssel für die Richtlinie

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

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann

gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

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

> **Important**
>
> Einige API-Aktionen verwenden mehrere Ressourcen. Viele Bedingungsschlüssel sind jedoch ressourcenspezifisch. Wenn Sie eine Richtlinienanweisung mit einem Bedingungsschlüssel schreiben, legen Sie über das `Resource`-Element der Anweisung fest, für welche Ressource der Bedingungsschlüssel gültig ist. Andernfalls verhindert die Richtlinie möglicherweise, dass Benutzer die Aktion überhaupt ausführen können, da die Bedingungsprüfung für die Ressourcen fehlschlägt, für die der Bedingungsschlüssel nicht gilt. Wenn Sie keine Ressource angeben möchten oder über das `Action`-Element Ihrer Richtlinie mehrere API-Aktionen hinzugefügt haben, müssen Sie mit dem `...IfExists`-Bedingungstyp sicherstellen, dass der Bedingungsschlüssel für die Ressourcen, die ihn nicht verwenden, ignoriert wird. Weitere Informationen finden Sie unter... IfExists Bedingungen im IAM-Benutzerhandbuch.

AWS IoT SiteWise definiert seinen eigenen Satz von Bedingungsschlüsseln und unterstützt auch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

AWS IoT SiteWise Bedingungsschlüssel

Bedingungsschlüssel	Beschreibung	Typen
`iotsitewise:isAssociatedWithAssetProperty`	Ob Datenströme mit einer Anlageneigenschaft verknüpft sind. Verwenden Sie diesen Bedingungsschlüssel, um Berechtigungen zu definieren, die auf dem Vorhandensein einer zugehörigen Asset-Eig	String

Bedingungsschlüssel	Beschreibung	Typen
	enschaft für Datenstreams basieren. Beispielwert: `true`	
`iotsitewise:assetHierarchyPath`	Der Hierarchiepfad der Komponente, bei dem es sich um eine Zeichenfolge von Komponenten-IDs handelt, die jeweils durch einen Schrägstrich getrennt sind. Verwenden Sie diesen Bedingungsschlüssel, um Berechtigungen basierend auf einer Teilmenge Ihrer Hierarchie aller Komponenten in Ihrem Konto zu definieren. Beispielwert: `/a1b2c3d4-5678-90ab-cdef-222222EXAMPLE/a1b2c3d4-5678-90ab-cdef-666666EXAMPLE`	String

Bedingungsschlüssel	Beschreibung	Typen
`iotsitewise:propertyId`	Die ID einer Komponenteneigenschaft. Verwenden Sie diesen Bedingungsschlüssel, um Berechtigungen basierend auf der angegebenen Eigenschaft eines Komponentenmodells zu definieren. Dieser Bedingungsschlüssel gilt für alle Komponenten dieses Modells. Beispielwert: `a1b2c3d4-5678-90ab-cdef-33333EXAMPLE`	String
`iotsitewise:childAssetId`	ID einer Komponente, die als untergeordnetes Element mit einer anderen Komponente verknüpft ist. Verwenden Sie diesen Bedingungsschlüssel, um Berechtigungen basierend auf untergeordneten Komponenten zu definieren. Um Berechtigungen basierend auf übergeordneten Komponenten zu definieren, verwenden Sie den Ressourcenabschnitt einer Richtlinienanweisung. Beispielwert: `a1b2c3d4-5678-90ab-cdef-66666EXAMPLE`	String

Bedingungsschlüssel	Beschreibung	Typen
`iotsitewise:iam`	Der ARN einer IAM-Identität beim Auflisten von Zugriffsrichtlinien. Verwenden Sie diesen Bedingungsschlüssel, um Zugriffsrichtlinienberechtigungen für eine IAM-Identität zu definieren. Beispielwert: `arn:aws:iam::123456789012:user/JohnDoe`	Zeichenfolge, Null
`iotsitewise:propertyAlias`	Der Alias, der eine Asset-Eigenschaft oder einen Datenstrom identifiziert. Verwenden Sie diesen Bedingungsschlüssel, um Berechtigungen auf der Grundlage des Alias zu definieren.	String
`iotsitewise:user`	Die ID eines IAM Identity Center-Benutzers beim Auflisten von Zugriffsrichtlinien. Verwenden Sie diesen Bedingungsschlüssel, um Zugriffsrichtlinienberechtigungen für einen IAM Identity Center-Benutzer zu definieren. Beispielwert: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE`	Zeichenfolge, Null

Bedingungsschlüssel	Beschreibung	Typen
`iotsitewise:group`	Die ID einer IAM Identity Center-Gruppe bei der Auflistung der Zugriffsrichtlinien. Verwenden Sie diesen Bedingungsschlüssel, um Zugriffsrichtlinienberechtigungen für eine IAM Identity Center-Gruppe zu definieren. Beispielwert: `a1b2c3d4e5-a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE`	Zeichenfolge, Null
`iotsitewise:portal`	Die ID eines Portals in einer Zugriffsrichtlinie. Verwenden Sie diesen Bedingungsschlüssel, um Zugriffsrichtlinienberechtigungen basierend auf einem Portal zu definieren. Beispielwert: `a1b2c3d4-5678-90ab-cdef-77777EXAMPLE`	Zeichenfolge, Null

Bedingungsschlüssel	Beschreibung	Typen
`iotsitewise:project`	Die ID eines Projekts in einer Zugriffsrichtlinie oder die ID eines Projekts für ein Dashboard. Verwenden Sie diesen Bedingungsschlüssel, um Dashboard- oder Zugriffsrichtlinienberechtigungen basierend auf einem Projekt zu definieren. Beispielwert: `a1b2c3d4-5678-90ab-cdef-888888EXAMPLE`	Zeichenfolge, Null

Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS IoT SiteWise.

Beispiele

Beispiele für AWS IoT SiteWise identitätsbasierte Richtlinien finden Sie unter. AWS IoT SiteWise Beispiele für identitätsbasierte Richtlinien

AWS IoT SiteWise Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind Entitäten (Benutzer und Rollen) nicht berechtigt, AWS IoT SiteWise Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Um Berechtigungen anzupassen, muss ein AWS Identity and Access Management (IAM-) Administrator wie folgt vorgehen:

1. Erstellen Sie IAM-Richtlinien, die Benutzern und Rollen die Berechtigung gewähren, bestimmte API-Operationen für Ressourcen auszuführen, die sie benötigen.
2. Ordnen Sie diese Richtlinien den Benutzern oder Gruppen zu, die diese Berechtigungen benötigen.

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

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS IoT SiteWise -Konsole
- Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen
- Ermöglicht Benutzern, Daten in Komponenten in einer Hierarchie zu erfassen
- Anzeigen von AWS IoT SiteWise -Komponenten basierend auf Tags

Bewährte Methoden für Richtlinien

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

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

um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

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

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

Verwenden der AWS IoT SiteWise -Konsole

Für den Zugriff auf die AWS IoT SiteWise Konsole benötigen Sie grundlegende Berechtigungen. Mit diesen Berechtigungen können Sie Details zu den AWS IoT SiteWise Ressourcen in Ihrem anzeigen und verwalten AWS-Konto.

Wenn Sie eine zu restriktive Richtlinie festlegen, funktioniert die Konsole für Benutzer oder Rollen (Entitäten), für die diese Richtlinie gilt, möglicherweise nicht wie erwartet. Um sicherzustellen, dass diese Entitäten die AWS IoT SiteWise Konsole weiterhin verwenden können, fügen Sie ihnen die AWSIoTSiteWiseConsoleFullAccessverwaltete Richtlinie bei oder definieren Sie entsprechende Berechtigungen für diese Entitäten. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Wenn Entitäten nur die AWS Command Line Interface (CLI) oder die AWS IoT SiteWise API und nicht die Konsole verwenden, benötigen sie diese Mindestberechtigungen nicht. Geben Sie ihnen in diesem Fall einfach Zugriff auf die spezifischen Aktionen, die sie für ihre API-Aufgaben benötigen.

Benutzern die Berechtigung zur Anzeige eigener Berechtigungen erteilen

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Ermöglicht Benutzern, Daten in Komponenten in einer Hierarchie zu erfassen

In diesem Beispiel möchten Sie einem Benutzer AWS-Konto Zugriff auf das Schreiben von Daten für alle Asset-Eigenschaften in einer bestimmten Asset-Hierarchie gewähren, beginnend mit dem Stammobjekt. `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` Die Richtlinie erteilt dem Benutzer die `iotsitewise:BatchPutAssetPropertyValue`-Berechtigung. Diese Richtlinie verwendet den `iotsitewise:assetHierarchyPath`-Bedingungsschlüssel, um den Zugriff auf Komponenten einzuschränken, deren Hierarchiepfad mit der Komponenten oder ihren abhängigen Elementen übereinstimmt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PutAssetPropertyValuesForHierarchy",
      "Effect": "Allow",
      "Action": "iotsitewise:BatchPutAssetPropertyValue",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
      "Condition": {
        "StringLike": {
          "iotsitewise:assetHierarchyPath": [
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
            "/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE/*"
          ]
        }
      }
    }
  ]
}
```

Anzeigen von AWS IoT SiteWise -Komponenten basierend auf Tags

Verwenden Sie Bedingungen in Ihrer identitätsbasierten Richtlinie, um den Zugriff auf AWS IoT SiteWise Ressourcen anhand von Tags zu steuern. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen, die das Anzeigen von Assets ermöglicht. Die Berechtigung wird jedoch nur erteilt, wenn das Tag der Komponente `Owner` den Wert des Benutzernamens dieses Benutzers hat. Diese Richtlinie gewährt auch die Erlaubnis, diese Aktion auf der Konsole abzuschließen.

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

```
    {
      "Sid": "ListAllAssets",
      "Effect": "Allow",
      "Action": [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeAssetIfOwner",
      "Effect": "Allow",
      "Action": "iotsitewise:DescribeAsset",
      "Resource": "arn:aws:iotsitewise:*:*:asset/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Owner": "${aws:username}"
        }
      }
    }
  ]
}
```

Hängen Sie diese Richtlinie den Benutzern in Ihrem Konto an. Wenn ein benannter Benutzer `richard-roe` versucht, ein AWS IoT SiteWise Asset aufzurufen, muss das Asset mit `0wner=richard-roe` oder markiert werden`owner=richard-roe`. Andernfalls wird Richard der Zugriff verweigert. Bei den Schlüsselnamen der Bedingungstags wird nicht zwischen Groß- und Kleinschreibung unterschieden. `0wner`Entspricht also sowohl als `0wner` auch`owner`. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

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

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

Identitätsbasierte Richtlinien

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

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

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen

in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

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

Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

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

Mehrere Richtlinientypen

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

AWS verwaltete Richtlinien für AWS IoT SiteWise

Vereinfachen Sie das Hinzufügen von Berechtigungen für Benutzer, Gruppen und Rollen mithilfe AWS verwalteter Richtlinien, anstatt Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um vom Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team präzise Berechtigungen gewähren. Für eine schnellere Einrichtung sollten Sie in Erwägung ziehen, unsere AWS verwalteten Richtlinien für allgemeine Anwendungsfälle zu verwenden. AWS Verwaltete Richtlinien finden Sie in Ihrem AWS-Konto. Weitere Informationen zu verwalteten AWS -Richtlinien finden Sie unter Verwaltete AWS -Richtlinien im IAM-Leitfaden.

AWS Dienste kümmern sich um die Aktualisierung und Wartung der AWS verwalteten Richtlinien, sodass Sie die Berechtigungen dieser Richtlinien nicht ändern können. Gelegentlich AWS IoT SiteWise können Berechtigungen hinzugefügt werden, um neuen Funktionen gerecht zu werden, was sich auf alle Identitäten auswirkt, an die die Richtlinie angehängt ist. Solche Aktualisierungen treten häufig bei der Einführung neuer Dienste oder Funktionen auf. Berechtigungen werden jedoch niemals entfernt, um sicherzustellen, dass Ihre Einstellungen intakt bleiben.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die AWS verwaltete ReadOnlyAccess-Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst ein neues Feature startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste mit

Beschreibungen der Richtlinien für Jobfunktionen finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien für Jobfunktionen.

AWS verwaltete Richtlinie: AWSIoTSiteWiseReadOnlyAccess

Verwenden Sie die `AWSIoTSiteWiseReadOnlyAccess` AWS verwaltete Richtlinie, um schreibgeschützten Zugriff auf zu gewähren. AWS IoT SiteWise

Sie können die `AWSIoTSiteWiseReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Berechtigungen auf Dienstebene

Diese Richtlinie bietet nur Lesezugriff auf. AWS IoT SiteWise In dieser Richtlinie sind keine anderen Dienstberechtigungen enthalten.

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

AWS verwaltete Richtlinie: AWSServiceRoleForIoTSiteWise

Die `AWSServiceRoleForIoTSiteWise` Rolle verwendet die `AWSServiceRoleForIoTSiteWise` Richtlinie mit den folgenden Berechtigungen. Diese Richtlinie:

- Ermöglicht AWS IoT SiteWise die Bereitstellung von SiteWise Edge-Gateways (die auf ausgeführt werden`AWS IoT Greengrass`).
- Ermöglicht AWS IoT SiteWise die Protokollierung.
- Ermöglicht AWS IoT SiteWise die Ausführung einer Metadaten-Suchabfrage in der AWS IoT TwinMaker Datenbank.

Wenn Sie ein einzelnes Benutzerkonto verwenden AWS IoT SiteWise , erstellt die `AWSServiceRoleForIoTSiteWise` Rolle die `AWSServiceRoleForIoTSiteWise` Richtlinie in Ihrem IAM-Konto und fügt sie den `AWSServiceRoleForIoTSiteWise` dienstverknüpften Rollen für hinzu. AWS IoT SiteWise

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AllowSiteWiseReadGreenGrass",
   "Effect": "Allow",
   "Action": [
    "greengrass:GetAssociatedRole",
    "greengrass:GetCoreDefinition",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowSiteWiseAccessLogGroup",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup",
    "logs:DescribeLogGroups"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
  },
  {
   "Sid": "AllowSiteWiseAccessLog",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:PutLogEvents"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
  },
  {
   "Sid": "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
   "Effect": "Allow",
```

```
    "Action": [
     "iottwinmaker:GetWorkspace",
     "iottwinmaker:ExecuteQuery"
    ],
    "Resource": "arn:aws:iottwinmaker:*:*:workspace/*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "iottwinmaker:linkedServices": [
       "IOTSITEWISE"
      ]
     }
    }
   }
  ]
}
```

AWS IoT SiteWise Aktualisierungen der verwalteten Richtlinien AWS

Sie können sich Details zu Aktualisierungen AWS verwalteter Richtlinien anzeigen lassen, und zwar ab dem Zeitpunkt AWS IoT SiteWise, zu dem dieser Dienst mit der Nachverfolgung der Änderungen begann. Abonnieren Sie den RSS-Feed auf der Seite AWS IoT SiteWise Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSServiceRoleForIoTSiteWise – Aktualisierung auf eine bestehende Richtlinie	AWS IoT SiteWise kann jetzt eine Metadaten-Suchabfrage für die AWS IoT TwinMaker Datenbank ausführen.	6. November 2023
AWSIoTSiteWiseReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	AWS IoT SiteWise hat ein neues Richtlinienpräfix hinzugefügt`BatchGet*` , das es Ihnen ermöglicht, Batch-Lesevorgänge durchzuführen.	16. September 2022
AWSIoTSiteWiseReadOnlyAccess – Neue Richtlinie.	AWS IoT SiteWise hat eine neue Richtlinie hinzugefügt, auf die nur Lesezugriff	24. November 2021

Änderung	Beschreibung	Datum
	gewährt werden kann. AWS IoT SiteWise	
AWS IoT SiteWise hat begonnen, Änderungen zu verfolgen	AWS IoT SiteWise hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	24. November 2021

Verwenden von serviceverknüpften Rollen für AWS IoT SiteWise

AWS IoT SiteWise verwendet dienstverknüpfte Rollen AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS IoT SiteWise Mit Diensten verknüpfte Rollen sind vordefiniert AWS IoT SiteWise und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Dienstbezogene Rollen vereinfachen die Konfiguration von, AWS IoT SiteWise indem sie automatisch alle erforderlichen Berechtigungen einbeziehen. AWS IoT SiteWise definiert die Berechtigungen seiner dienstbezogenen Rollen und AWS IoT SiteWise kann, sofern nicht anders definiert, nur seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Und diese Berechtigungsrichtlinie kann keiner anderen IAM-Entität zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre AWS IoT SiteWise Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-Linked Role (Serviceverknüpfte Rolle) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

- Berechtigungen von serviceverknüpften Rollen für AWS IoT SiteWise
- Erstellen einer serviceverknüpften Rolle für AWS IoT SiteWise
- Bearbeiten einer serviceverknüpften Rolle für AWS IoT SiteWise

- Löschen einer serviceverknüpften Rolle für AWS IoT SiteWise
- Unterstützte Regionen für serviceverknüpfte Rollen AWS IoT SiteWise
- Verwenden von Servicerollen für AWS IoT SiteWise Monitor

Berechtigungen von serviceverknüpften Rollen für AWS IoT SiteWise

AWS IoT SiteWise verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen. AWSServiceRoleForIoTSiteWise AWS IoT SiteWise verwendet diese dienstgebundene Rolle, um SiteWise Edge-Gateways (die auf laufen AWS IoT Greengrass) bereitzustellen und die Protokollierung durchzuführen.

Die `AWSServiceRoleForIoTSiteWise` dienstverknüpfte Rolle verwendet die `AWSServiceRoleForIoTSiteWise` Richtlinie mit den folgenden Berechtigungen. Diese Richtlinie:

- Ermöglicht AWS IoT SiteWise die Bereitstellung von SiteWise Edge-Gateways (die auf ausgeführt werden`AWS IoT Greengrass`).
- Ermöglicht AWS IoT SiteWise die Protokollierung.
- Ermöglicht AWS IoT SiteWise die Ausführung einer Metadaten-Suchabfrage in der AWS IoT TwinMaker Datenbank.

Weitere Informationen zu den zulässigen Aktionen in finden Sie `AWSServiceRoleForIoTSiteWise` unter AWS Verwaltete Richtlinien für AWS IoT SiteWise.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AllowSiteWiseReadGreenGrass",
   "Effect": "Allow",
   "Action": [
    "greengrass:GetAssociatedRole",
    "greengrass:GetCoreDefinition",
    "greengrass:GetCoreDefinitionVersion",
    "greengrass:GetGroup",
    "greengrass:GetGroupVersion"
   ],
   "Resource": "*"
  },
  {
```

```
    "Sid": "AllowSiteWiseAccessLogGroup",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup",
     "logs:DescribeLogGroups"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
   },
   {
    "Sid": "AllowSiteWiseAccessLog",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogStream",
     "logs:DescribeLogStreams",
     "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
   },
   {
    "Sid": "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
    "Effect": "Allow",
    "Action": [
     "iottwinmaker:GetWorkspace",
     "iottwinmaker:ExecuteQuery"
    ],
    "Resource": "arn:aws:iottwinmaker:*:*:workspace/*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "iottwinmaker:linkedServices": [
       "IOTSITEWISE"
      ]
     }
    }
   }
  ]
}
```

Sie können die Protokolle verwenden, um Ihre SiteWise Edge-Gateways zu überwachen und Fehler zu beheben. Weitere Informationen finden Sie unter Überwachung von SiteWise Edge-Gateway-Protokollen.

Damit eine IAM-Entität (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann, müssen Sie zunächst die Berechtigungen

konfigurieren. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für AWS IoT SiteWise

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie die folgenden Operationen in der AWS IoT SiteWise Konsole ausführen, AWS IoT SiteWise erstellt die dienstverknüpfte Rolle für Sie.

- Erstellen Sie ein Greengrass V1-Gateway.
- Konfigurieren Sie die Protokollierungsoption.
- Wählen Sie die Opt-in-Schaltfläche im Banner „Abfrage ausführen“.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Vorgang in der AWS IoT SiteWise Konsole ausführen, AWS IoT SiteWise wird die mit dem Dienst verknüpfte Rolle erneut für Sie erstellt.

Sie können auch die IAM-Konsole oder API verwenden, um eine serviceverknüpfte Rolle für zu erstellen. AWS IoT SiteWise

- Erstellen Sie dazu in der IAM-Konsole eine Rolle mit der AWSServiceRoleForIoTSiteWiseRichtlinie und einer Vertrauensbeziehung mit. `iotsitewise.amazonaws.com`
- Erstellen Sie dazu mithilfe der AWS CLI oder der IAM-API eine Rolle mit der `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise` Richtlinie und eine Vertrauensbeziehung mit. `iotsitewise.amazonaws.com`

Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für AWS IoT SiteWise

AWS IoT SiteWise erlaubt es Ihnen nicht, die mit dem AWSServiceRoleForIoTSiteWise Service verknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden.

Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS IoT SiteWise

Wenn eine Funktion oder ein Dienst, für den eine serviceverknüpfte Rolle erforderlich ist, nicht mehr verwendet wird, empfiehlt es sich, die zugehörige Rolle zu löschen. Auf diese Weise soll vermieden werden, dass eine inaktive Entität nicht überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der AWS IoT SiteWise Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies der Fall ist, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS IoT SiteWise Ressourcen zu löschen, die verwendet werden von AWSServiceRoleForIoTSiteWise

1. Deaktivieren Sie die Protokollierung für AWS IoT SiteWise. Weitere Informationen finden Sie unter Ändern Sie Ihre Protokollierungsebene.
2. Löschen Sie alle aktiven SiteWise Edge-Gateways.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForIoTSiteWise dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Rollen AWS IoT SiteWise

AWS IoT SiteWise unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS IoT SiteWise -Endpunkte und -Kontingente.

Verwenden von Servicerollen für AWS IoT SiteWise Monitor

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, 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.

Um Benutzern des SiteWise Verbundmonitor-Portals den Zugriff auf Ihre AWS IAM Identity Center Ressourcen AWS IoT SiteWiseund Ihre Ressourcen zu ermöglichen, müssen Sie jedem Portal, das Sie erstellen, eine Servicerolle zuordnen. In der Servicerolle muss SiteWise Monitor als vertrauenswürdige Entität angegeben und die AWSIoTSiteWiseMonitorPortalAccessverwaltete Richtlinie enthalten oder entsprechende Berechtigungen definiert werden. Diese Richtlinie wird von den Berechtigungen verwaltet AWS und definiert die Berechtigungen, die SiteWise Monitor für den Zugriff auf Ihre AWS IoT SiteWise und IAM Identity Center-Ressourcen verwendet.

Wenn Sie ein SiteWise Monitor-Portal erstellen, müssen Sie eine Rolle auswählen, die Benutzern dieses Portals den Zugriff auf Ihre Ressourcen AWS IoT SiteWiseund die Ressourcen von IAM Identity Center ermöglicht. Die AWS IoT SiteWise Konsole kann die Rolle für Sie erstellen und konfigurieren. Sie können die Rolle später in IAM bearbeiten. Ihre Portalbenutzer werden Probleme bei der Verwendung ihrer SiteWise Monitor-Portale haben, wenn Sie die erforderlichen Berechtigungen aus der Rolle entfernen oder die Rolle löschen.

> **Note**
>
> Portale, die vor dem 29. April 2020 erstellt wurden, haben keine Servicerollen benötigt. Wenn Sie vor diesem Datum Portale erstellt haben, müssen Sie diesen Servicerollen anfügen, um sie weiter verwenden zu können. Navigieren Sie dazu in der AWS IoT SiteWise Konsole zur Seite Portale und wählen Sie dann Alle Portale migrieren, um IAM-Rollen zu verwenden.

In den folgenden Abschnitten wird beschrieben, wie Sie die SiteWise Monitor-Servicerolle in der AWS Management Console oder der AWS Command Line Interface erstellen und verwalten.

Inhalt

- Erstellen einer SiteWise Monitor-Servicerolle (IAM-Konsole)
- Änderung der Servicerolle eines Portals (Konsole)
- Verwaltung der SiteWise Monitor-Servicerolle (CLI)
  - Suche der Servicerolle eines Portals (CLI)
  - Die SiteWise Monitor-Servicerolle (CLI) erstellen
- SiteWise Überwachen Sie Aktualisierungen für AWSIoTSiteWiseMonitorServiceRole

Berechtigungen für die Servicerolle für SiteWise Monitor

Wenn Sie ein Portal erstellen, AWS IoT SiteWise können Sie damit eine Rolle erstellen, deren Name mit beginnt AWSIoTSiteWiseMonitorServiceRole. Diese Rolle ermöglicht Benutzern von Federated SiteWise Monitor den Zugriff auf Ihre Portalkonfiguration, Ihre Assets, Asset-Daten sowie die IAM Identity Center-Konfiguration .

Die Rolle vertraut darauf, dass der folgende Service diese Rolle annimmt:

- `monitor.iotsitewise.amazonaws.com`

Die Rolle verwendet die folgende Berechtigungsrichtlinie, deren Name mit beginnt AWSIoTSiteWiseMonitorServicePortalPolicy, damit SiteWise Monitor-Benutzer Aktionen an Ressourcen in Ihrem Konto ausführen können. Die AWSIoTSiteWiseMonitorPortalAccessverwaltete Richtlinie definiert äquivalente Berechtigungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal",
                "iotsitewise:CreateProject",
                "iotsitewise:DescribeProject",
                "iotsitewise:UpdateProject",
                "iotsitewise:DeleteProject",
                "iotsitewise:ListProjects",
                "iotsitewise:BatchAssociateProjectAssets",
                "iotsitewise:BatchDisassociateProjectAssets",
                "iotsitewise:ListProjectAssets",
                "iotsitewise:CreateDashboard",
```

```
                "iotsitewise:DescribeDashboard",
                "iotsitewise:UpdateDashboard",
                "iotsitewise:DeleteDashboard",
                "iotsitewise:ListDashboards",
                "iotsitewise:CreateAccessPolicy",
                "iotsitewise:DescribeAccessPolicy",
                "iotsitewise:UpdateAccessPolicy",
                "iotsitewise:DeleteAccessPolicy",
                "iotsitewise:ListAccessPolicies",
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssets",
                "iotsitewise:ListAssociatedAssets",
                "iotsitewise:DescribeAssetProperty",
                "iotsitewise:GetAssetPropertyValue",
                "iotsitewise:GetAssetPropertyValueHistory",
                "iotsitewise:GetAssetPropertyAggregates",
                "iotsitewise:BatchPutAssetPropertyValue",
                "iotsitewise:ListAssetRelationships",
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:ListAssetModels",
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting",
                "sso-directory:DescribeUsers",
                "sso-directory:DescribeUser",
                "iotevents:DescribeAlarmModel",
                "iotevents:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:BatchAcknowledgeAlarm",
                "iotevents:BatchSnoozeAlarm",
                "iotevents:BatchEnableAlarm",
                "iotevents:BatchDisableAlarm"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "iotevents:keyValue": "false"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:UpdateAlarmModel",
                "iotevents:DeleteAlarmModel"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "iotevents.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Weitere Informationen zu den erforderlichen Berechtigungen für Alarme finden Sie unterBerechtigungen für AWS IoT Events Alarme einrichten.

Wenn sich ein Portalbenutzer anmeldet, erstellt SiteWise Monitor eine Sitzungsrichtlinie, die auf der Schnittmenge zwischen der Servicerolle und den Zugriffsrichtlinien dieses Benutzers basiert. Zugriffsrichtlinien definieren die Zugriffsstufe von -Identitäten auf Ihre Portale und Projekte. Weitere Informationen zu Portalberechtigungen und Zugriffsrichtlinien finden Sie unter Verwaltung Ihrer SiteWise Monitor-Portale und CreateAccessRichtlinie.

Verwaltung der SiteWise Monitor-Dienstrolle (Konsole)

Das AWS-IoT-SiteWise-Konsole erleichtert die Verwaltung der SiteWise Monitor-Dienstrolle für Portale. Beim Erstellen eines Portals sucht die Konsole nach vorhandenen Rollen, die für eine Zuordnung geeignet sind. Wenn keine verfügbar sind, kann die Konsole eine Servicerolle für Sie erstellen und konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Portals.

Themen

- Suchen der Servicerolle eines Portals (Konsole)
- Erstellen einer SiteWise Monitor-Dienstrolle (AWS IoT SiteWise Konsole)
- Erstellen einer SiteWise Monitor-Servicerolle (IAM-Konsole)
- Änderung der Servicerolle eines Portals (Konsole)

Suchen der Servicerolle eines Portals (Konsole)

Gehen Sie wie folgt vor, um die einem SiteWise Monitor-Portal zugeordnete Servicerolle zu finden.

So finden Sie die Servicerolle eines Portals

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Portale aus.
3. Wählen Sie das Portal aus, dessen Servicerolle Sie finden möchten.

   Die dem Portal angefügte Rolle wird unter Permissions (Berechtigungen), Service role (Servicerolle) angezeigt.

Erstellen einer SiteWise Monitor-Dienstrolle (AWS IoT SiteWise Konsole)

Wenn Sie ein SiteWise Monitor-Portal erstellen, können Sie eine Servicerolle für Ihr Portal erstellen. Weitere Informationen finden Sie unter Erstellen eines Portals.

Sie können auch eine Servicerolle für ein vorhandenes Portal in der AWS IoT SiteWise Konsole erstellen. Dies ersetzt die bestehende Servicerolle des Portals.

So erstellen Sie eine Servicerolle für ein vorhandenes Portal

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Portale aus.
3. Wählen Sie das Portal aus, für das Sie eine neue Servicerolle erstellen möchten.
4. Wählen Sie unter Portal details (Portaldetails) die Option Edit (Bearbeiten).
5. Wählen Sie unter Permissions (Berechtigungen) die Option Create and use a new service role (Eine neue Servicerolle erstellen und verwenden) aus der Liste aus.
6. Geben Sie einen Namen für die neue Rolle ein.
7. Wählen Sie Speichern.

Erstellen einer SiteWise Monitor-Servicerolle (IAM-Konsole)

Sie können eine Servicerolle anhand der Servicerollenvorlage in der IAM-Konsole erstellen. Diese Rollenvorlage enthält die AWSIoTSiteWiseMonitorPortalAccessverwaltete Richtlinie und gibt SiteWise Monitor als vertrauenswürdige Entität an.

Um eine Servicerolle aus der Servicerollenvorlage des Portals zu erstellen

1. Navigieren Sie zur IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie unter Wählen Sie einen Anwendungsfall die Option IoT aus SiteWise.
5. Wählen Sie unter Wählen Sie Ihren Anwendungsfall aus die Option IoT SiteWise Monitor - Portal.
6. Wählen Sie Next: Permissions aus.
7. Wählen Sie Next: Tags (Weiter: Tags) aus.
8. Klicken Sie auf Weiter: Prüfen.
9. Geben Sie einen Rollennamen für die neue Servicerolle ein.

10. Wählen Sie Rolle erstellen aus.

Änderung der Servicerolle eines Portals (Konsole)

Gehen Sie wie folgt vor, um eine andere SiteWise Monitor-Servicerolle für ein Portal auszuwählen.

So ändern Sie die Servicerolle eines Portals

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Portale aus.
3. Wählen Sie das Portal aus, dessen Servicerolle Sie ändern möchten.
4. Wählen Sie unter Portal details (Portaldetails) die Option Edit (Bearbeiten).
5. Wählen Sie unter Permissions (Berechtigungen) die Option Use an existing role (Vorhandene Rolle verwenden) aus.
6. Wählen Sie eine vorhandene Rolle aus, die diesem Portal angefügt werden soll.
7. Wählen Sie Speichern.

Verwaltung der SiteWise Monitor-Servicerolle (CLI)

Sie können den AWS CLI für die folgenden Aufgaben zur Verwaltung der Portaldienstrollen verwenden:

Themen

- Suche der Servicerolle eines Portals (CLI)
- Die SiteWise Monitor-Servicerolle (CLI) erstellen

Suche der Servicerolle eines Portals (CLI)

Um die einem SiteWise Monitor-Portal zugeordnete Servicerolle zu finden, führen Sie den folgenden Befehl aus, um alle Ihre Portale in der aktuellen Region aufzulisten.

```
aws iotsitewise list-portals
```

Die Operation gibt eine Antwort mit einer Portalzusammenfassung im folgenden Format zurück.

```
{
```

```
  "portalSummaries": [
    {
      "id": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
      "name": "WindFarmPortal",
      "description": "A portal that contains wind farm projects for Example Corp.",
      "roleArn": "arn:aws:iam::123456789012:role/service-role/role-name",
      "startUrl": "https://a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE.app.iotsitewise.aws",
      "creationDate": "2020-02-04T23:01:52.90248068Z",
      "lastUpdateDate": "2020-02-04T23:01:52.90248078Z"
    }
  ]
}
```

Sie können den DescribePortalVorgang auch verwenden, um die Rolle Ihres Portals zu ermitteln, wenn Sie die ID Ihres Portals kennen.

Die SiteWise Monitor-Servicerolle (CLI) erstellen

Gehen Sie wie folgt vor, um eine neue SiteWise Monitor-Dienstrolle zu erstellen.

Um eine SiteWise Monitor-Dienstrolle zu erstellen

1. Erstellen Sie eine Rolle mit einer Vertrauensrichtlinie, die es SiteWise Monitor ermöglicht, die Rolle zu übernehmen. In diesem Beispiel wird eine Rolle Mit dem Namen **`MySiteWiseMonitorPortalRole`** aus einer Vertrauensrichtlinie erstellt, die in einer JSON-Zeichenfolge gespeichert ist.

   Linux, macOS, or Unix

   ```
   aws iam create-role --role-name MySiteWiseMonitorPortalRole --assume-role-
   policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Service": "monitor.iotsitewise.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }'
   ```

Windows command prompt

```
aws iam create-role --role-name MySiteWiseMonitorPortalRole --assume-role-
policy-document "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"Service\":\"monitor.iotsitewise.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}"
```

2. Kopieren Sie den Rollen-ARN aus den Rollenmetadaten in der Ausgabe. Wenn Sie ein Portal erstellen, verwenden Sie diesen ARN, um die Rolle Ihrem Portal zuzuordnen. Weitere Informationen zum Erstellen eines Portals finden Sie CreatePortalin der AWS IoT SiteWise API-Referenz.
3. Weisen Sie die `AWSIoTSiteWiseMonitorPortalAccess`-Richtlinie an die Rolle zu, oder fügen Sie eine Richtlinie hinzu, die entsprechende Berechtigungen definiert.

```
aws iam attach-role-policy --role-name MySiteWiseMonitorPortalRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess
```

So fügen Sie einem vorhandenen Portal eine Servicerolle an

1. Führen Sie den folgenden Befehl aus, um die vorhandenen Details des Portals abzurufen. Ersetzen Sie *`portal-id`* durch die ID des Portals.

```
aws iotsitewise describe-portal --portal-id portal-id
```

Die Operation gibt eine Antwort zurück, die die Details des Portals im folgenden Format enthält.

```
{
    "portalId": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
    "portalArn": "arn:aws:iotsitewise:region:account-id:portal/a1b2c3d4-5678-90ab-
cdef-aaaaaEXAMPLE",
    "portalName": "WindFarmPortal",
    "portalDescription": "A portal that contains wind farm projects for Example
 Corp.",
    "portalClientId": "E-1a2b3c4d5e6f_sn6tbqHVzLWVEXAMPLE",
    "portalStartUrl": "https://a1b2c3d4-5678-90ab-cdef-
aaaaaEXAMPLE.app.iotsitewise.aws",
    "portalContactEmail": "support@example.com",
    "portalStatus": {
        "state": "ACTIVE"
```

```
    },
    "portalCreationDate": "2020-04-29T23:01:52.90248068Z",
    "portalLastUpdateDate": "2020-04-29T00:28:26.103548287Z",
    "roleArn": "arn:aws:iam::123456789012:role/service-role/
AWSIoTSiteWiseMonitorServiceRole_1aEXAMPLE"
}
```

2. Führen Sie den folgenden Befehl aus, um einem Portal eine Servicerolle anzufügen. Ersetzen Sie *role-arn* durch den Servicerollen-ARN. Ersetzen Sie die übrigen Parameter durch die vorhandenen Werte des Portals.

```
aws iotsitewise update-portal \
  --portal-id portal-id \
  --role-arn role-arn \
  --portal-name portal-name \
  --portal-description portal-description \
  --portal-contact-email portal-contact-email
```

SiteWise Überwachen Sie Aktualisierungen für AWSIoTSiteWiseMonitorServiceRole

Sie können sich Details zu Updates AWSIoTSiteWiseMonitorServiceRolefür SiteWise Monitor anzeigen lassen, und zwar ab dem Zeitpunkt, zu dem dieser Dienst mit der Nachverfolgung der Änderungen begann. Abonnieren Sie den RSS-Feed auf der Seite AWS IoT SiteWise Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSIoTSiteWiseMonitorPortalAccess— Aktualisierte Richtlinie	AWS IoT SiteWise AWSIoTSiteWiseMonitorPortalAccesshat die verwaltete Richtlinie für die Alarmfunktion aktualisiert.	27. Mai 2021
AWS IoT SiteWise hat begonnen, Änderungen zu verfolgen	AWS IoT SiteWise hat begonnen, Änderungen für seine Servicerolle zu verfolgen .	15. Dezember 2020

Berechtigungen für AWS IoT Events Alarme einrichten

Wenn Sie ein AWS IoT Events Alarmmodell zur Überwachung einer AWS IoT SiteWise Anlageneigenschaft verwenden, benötigen Sie die folgenden IAM-Berechtigungen:

- Eine AWS IoT Events Servicerolle, AWS IoT Events an die Daten gesendet werden können. AWS IoT SiteWise Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS IoT Events im AWS IoT Events Entwicklerhandbuch.
- Sie benötigen die folgenden AWS IoT SiteWise Aktionsberechtigungen: `iotsitewise:DescribeAssetModel` und`iotsitewise:UpdateAssetModelPropertyRouting`. Diese Berechtigungen ermöglichen AWS IoT SiteWise das Senden von Objekteigenschaftswerten an AWS IoT Events Alarmmodelle.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Ressourcenbasierte Richtlinien.

Erforderliche Aktionsberechtigungen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen. Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können.

Bevor Sie ein AWS IoT Events Alarmmodell definieren, müssen Sie die folgenden Berechtigungen erteilen, die es ermöglichen, Asset-Eigenschaftswerte AWS IoT SiteWise an das Alarmmodell zu senden.

- `iotsitewise:DescribeAssetModel`— Ermöglicht AWS IoT Events die Überprüfung, ob eine Anlageneigenschaft existiert.
- `iotsitewise:UpdateAssetModelPropertyRouting`— Ermöglicht AWS IoT SiteWise das automatische Erstellen von Abonnements, AWS IoT SiteWise an die Daten gesendet werden können AWS IoT Events.

Weitere Informationen zu AWS IoT SiteWise unterstützten Aktionen finden Sie unter Aktionen definiert von AWS IoT SiteWise in der Service Authorization Reference.

Example Beispiel für eine Berechtigungsrichtlinie 1

Die folgende Richtlinie ermöglicht AWS IoT SiteWise das Senden von Objekteigenschaftswerten an beliebige AWS IoT Events Alarmmodelle.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        }
    ]
}
```

Example Beispiel für eine Berechtigungsrichtlinie 2

Die folgende Richtlinie ermöglicht AWS IoT SiteWise das Senden von Werten einer bestimmten Anlageneigenschaft an ein bestimmtes AWS IoT Events Alarmmodell.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:UpdateAlarmModel"
            ],
            "Resource": "arn:aws:iotevents:us-east-1:123456789012:alarmModel/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribeAssetModel"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:UpdateAssetModelPropertyRouting"
            ],
            "Resource": [
                "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/12345678-90ab-
cdef-1234-567890abcdef"
            ],
            "Condition": {
                "StringLike": {
                    "iotsitewise:propertyId": "abcdef12-3456-7890-abcd-ef1234567890",
                    "iotevents:alarmModelArn": "arn:aws:iotevents:us-
east-1:123456789012:alarmModel/MyAlarmModel"
                }
            }
        }
    ]
}
```

(Optionale) ListInputRoutings Erlaubnis

Wenn Sie ein Asset-Modell aktualisieren oder löschen, AWS IoT SiteWise kann überprüft werden, ob ein Alarmmodell eine mit diesem Asset-Modell verknüpfte Anlageneigenschaft überwacht. AWS IoT Events Dadurch wird verhindert, dass Sie eine Anlageneigenschaft löschen, die derzeit von einem AWS IoT Events Alarm verwendet wird. Um diese Funktion in zu aktivieren AWS IoT SiteWise, benötigen Sie die `iotevents:ListInputRoutings` entsprechende Genehmigung. Diese Berechtigung ermöglicht das Ausführen AWS IoT SiteWise von Aufrufen des ListInputRoutings-API-Vorgangs, der von AWS IoT Events unterstützt wird.

> **Note**
>
> Wir empfehlen dringend, dass Sie die `ListInputRoutings` Berechtigung hinzufügen.

Example Beispiel für eine Berechtigungsrichtlinie

Die folgende Richtlinie ermöglicht es Ihnen, Asset-Modelle zu aktualisieren und zu löschen und die `ListInputRoutings` API in zu verwenden AWS IoT SiteWise.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:DeleteAssetModel",
                "iotevents:ListInputRoutings"
            ],
            "Resource": "arn:aws:iotsitewise:us-east-1:123456789012:asset-model/*"
        }
    ]
}
```

Erforderliche Berechtigungen für SiteWise Monitor

Wenn Sie die Alarmfunktion in SiteWise Monitor-Portalen verwenden möchten, müssen Sie die SiteWise Monitor-Servicerolle mit der folgenden Richtlinie aktualisieren:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal",
                "iotsitewise:CreateProject",
                "iotsitewise:DescribeProject",
                "iotsitewise:UpdateProject",
                "iotsitewise:DeleteProject",
                "iotsitewise:ListProjects",
                "iotsitewise:BatchAssociateProjectAssets",
                "iotsitewise:BatchDisassociateProjectAssets",
                "iotsitewise:ListProjectAssets",
                "iotsitewise:CreateDashboard",
                "iotsitewise:DescribeDashboard",
                "iotsitewise:UpdateDashboard",
```

```
                "iotsitewise:DeleteDashboard",
                "iotsitewise:ListDashboards",
                "iotsitewise:CreateAccessPolicy",
                "iotsitewise:DescribeAccessPolicy",
                "iotsitewise:UpdateAccessPolicy",
                "iotsitewise:DeleteAccessPolicy",
                "iotsitewise:ListAccessPolicies",
                "iotsitewise:DescribeAsset",
                "iotsitewise:ListAssets",
                "iotsitewise:ListAssociatedAssets",
                "iotsitewise:DescribeAssetProperty",
                "iotsitewise:GetAssetPropertyValue",
                "iotsitewise:GetAssetPropertyValueHistory",
                "iotsitewise:GetAssetPropertyAggregates",
                "iotsitewise:BatchPutAssetPropertyValue",
                "iotsitewise:ListAssetRelationships",
                "iotsitewise:DescribeAssetModel",
                "iotsitewise:ListAssetModels",
                "iotsitewise:UpdateAssetModel",
                "iotsitewise:UpdateAssetModelPropertyRouting",
                "sso-directory:DescribeUsers",
                "sso-directory:DescribeUser",
                "iotevents:DescribeAlarmModel",
                "iotevents:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:BatchAcknowledgeAlarm",
                "iotevents:BatchSnoozeAlarm",
                "iotevents:BatchEnableAlarm",
                "iotevents:BatchDisableAlarm"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "iotevents:keyValue": "false"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iotevents:CreateAlarmModel",
                "iotevents:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iotevents:UpdateAlarmModel",
                "iotevents:DeleteAlarmModel"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/iotsitewisemonitor": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "iotevents.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In kann AWS ein dienstübergreifender Identitätswechsel zum Problem des verwirrten Stellvertreters führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der Anruf-Service) einen anderen Service anruft (den aufgerufenen Service). Der Anruf-Service 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, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS IoT SiteWise Ressource einen anderen Dienst gewähren. Wenn der `aws:SourceArn`-Wert nicht die Konto-ID enthält, z. B. den Amazon-Ressourcennamen (ARN) eines Amazon-S3-Buckets, müssen Sie beide globale Bedingungskontext-Schlüssel verwenden, um Berechtigungen einzuschränken. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird.

- Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten.
- Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der Wert von `aws:SourceArn` muss die AWS IoT SiteWise Kundenressource sein, die der `sts:AssumeRole` Anfrage zugeordnet ist.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen 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. z. B. `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Example — Verwirrter Stellvertreter, Prävention

Das folgende Beispiel zeigt, wie Sie die Kontexttasten `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, AWS IoT SiteWise um das Problem des verwirrten Stellvertreters zu verhindern.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "iotsitewise.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Resource": [
      "arn:aws:iotsitewise:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:iotsitewise:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Problembehebung bei AWS IoT SiteWise Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS IoT SiteWise und AWS Identity and Access Management (IAM) auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS IoT SiteWise
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert.
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS IoT SiteWise Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS IoT SiteWise

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

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu einem Asset anzuzeigen, aber nicht über die `iotsitewise:DescribeAsset` entsprechenden Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotsitewise:DescribeAsset on resource: a1b2c3d4-5678-90ab-cdef-22222EXAMPLE
```

In diesem Fall bittet Mateo den Administrator, die Richtlinien zu aktualisieren, um ihm den Zugriff auf die Ressource mit der ID `a1b2c3d4-5678-90ab-cdef-22222EXAMPLE` über die Aktion `iotsitewise:DescribeAsset` zu ermöglichen.

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 SiteWiseübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

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

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

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

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

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS IoT SiteWise Ressourcen ermöglichen

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

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS IoT SiteWise unterstützt werden, finden Sie unterWie AWS IoT SiteWise funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Konformitätsprüfung für AWS IoT SiteWise

AWS IoT SiteWise fällt nicht in den Geltungsbereich AWS irgendwelcher Compliance-Programme.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

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

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS IoT SiteWise hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden

Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.
- Zehn goldene Sicherheitsregeln für industrielle IoT-Lösungen — In diesem Blogbeitrag werden zehn goldene Regeln vorgestellt, mit denen Sie Ihre industriellen Steuerungssysteme (ICS), das industrielle Internet der Dinge (IIoT) und Cloud-Umgebungen schützen können.
- Bewährte Sicherheitspraktiken für OT-Systeme in der Fertigung — In diesem Whitepaper werden bewährte Sicherheitsmethoden für die Entwicklung, Bereitstellung und Architektur dieser hybriden Fertigungs-Workloads vor Ort für die Cloud beschrieben. AWS

Resilienz in AWS IoT SiteWise

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

AWS IoT SiteWise wird vollständig verwaltet und nutzt hochverfügbare und langlebige AWS Dienste wie Amazon S3 und Amazon EC2. Um die Verfügbarkeit im Falle einer Unterbrechung der Availability Zone sicherzustellen, AWS IoT SiteWise arbeitet in mehreren Verfügbarkeitszonen.

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

Zusätzlich zur AWS globalen Infrastruktur AWS IoT SiteWise bietet es mehrere Funktionen, die Sie bei Ihren Anforderungen an Datenstabilität und Datensicherung unterstützen:

- Sie können Aktualisierungen von Eigenschaftswerten AWS IoT Core über MQTT-Nachrichten veröffentlichen und dann Regeln konfigurieren, um auf diese Daten zu reagieren. Mit dieser Funktion können Sie Daten in anderen AWS Diensten wie Amazon S3 und Amazon DynamoDB sichern. Weitere Informationen finden Sie unter Interaktion mit anderen AWS Diensten und Exportieren Sie Daten mit Benachrichtigungen über Vermögenseigenschaften nach Amazon S3.
- Sie können die AWS IoT SiteWise `Get*` APIs verwenden, um historische Vermögensdaten abzurufen und zu sichern. Weitere Informationen finden Sie unter Abfragen von historischen Komponenteneigenschaftswerten.
- Sie können die AWS IoT SiteWise `Describe*` APIs verwenden, um die Definitionen für Ihre Ressourcen, wie z. B. Vermögenswerte und Modelle, abzurufen. Sie können diese Definitionen sichern und später verwenden, um Ihre Ressourcen neu zu erstellen. Weitere Informationen finden Sie in der AWS IoT SiteWise -API-Referenz.

Sicherheit der Infrastruktur in AWS IoT SiteWise

Als verwalteter Dienst AWS IoT SiteWise ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS IoT SiteWise über das Netzwerk. 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.

SiteWise Edge-Gateways, die auf ausgeführt werden AWS IoT Greengrass, verwenden X.509-Zertifikate und kryptografische Schlüssel, um sich mit der Cloud zu verbinden und zu authentifizieren. AWS Weitere Informationen finden Sie unter Geräteauthentifizierung und Autorisierung für AWS IoT Greengrass im Entwicklerhandbuch.AWS IoT Greengrass Version 1

Konfigurations- und Schwachstellenanalyse

IoT-Flotten können aus einer großen Anzahl von Geräten mit unterschiedlichsten Funktionen bestehen, sind langlebig und geografisch verteilt. Aufgrund dieser Merkmale ist die Flotteneinrichtung komplex und fehleranfällig. Da Geräte in der Regel nur über begrenzte Rechenleistung, Arbeitsspeicher und Speicherplatz verfügen, können sie Verschlüsselung und andere Sicherheitsmaßnahmen nicht immer unterstützen. Außerdem verwenden Geräte häufig Software mit bekannten Schwachstellen. Diese Faktoren machen IoT-Flotten zu einem attraktiven Ziel für Hacker und erschweren die kontinuierliche Sicherung Ihrer Geräteflotte.

AWS IoT Device Defender begegnet diesen Herausforderungen durch die Bereitstellung von Tools zur Identifizierung von Sicherheitsproblemen und Abweichungen von bewährten Verfahren. Wird AWS IoT Device Defender zur Analyse, Prüfung und Überwachung verbundener Geräte verwendet, um ungewöhnliches Verhalten zu erkennen und Sicherheitsrisiken zu minimieren. AWS IoT Device Defender kann Geräteflotten überprüfen, um sicherzustellen, dass sie sich an bewährte Sicherheitsmethoden halten, und um abnormales Verhalten auf Geräten zu erkennen. Auf diese Weise können Sie einheitliche Sicherheitsrichtlinien für Ihre gesamte AWS IoT Geräteflotte durchsetzen und schnell reagieren, wenn Geräte kompromittiert werden. Weitere Informationen finden Sie unter AWS IoT Device Defender im AWS IoT -Entwicklerhandbuch.

Wenn Sie SiteWise Edge-Gateways verwenden, um Daten in den Dienst aufzunehmen, liegt es in Ihrer Verantwortung, die Umgebung Ihres SiteWise Edge-Gateways zu konfigurieren und zu warten. Diese Verantwortung umfasst die Aktualisierung auf die neuesten Versionen der Systemsoftware, AWS IoT Greengrass Software und des Connectors des SiteWise AWS IoT SiteWise Edge-Gateways. Weitere Informationen finden Sie unter Konfiguration des AWS IoT Greengrass Kerns im AWS IoT Greengrass Version 1 Entwicklerhandbuch undAktualisieren eines Connectors.

VPC-Endpunkte

Ein Schnittstellen-VPC-Endpunkt stellt eine private Verbindung zwischen Ihrer Virtual Private Cloud (VPC) und her. AWS IoT SiteWiseAWS PrivateLinkversorgt Schnittstellenendpunkte und ermöglicht so den privaten Zugriff auf AWS IoT SiteWise API-Operationen. Sie können die Notwendigkeit eines Internet-Gateways, eines NAT-Geräts, einer VPN-Verbindung oder AWS Direct Connect umgehen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit AWS IoT SiteWise API-Vorgängen zu kommunizieren. Datenverkehr zwischen Ihrer VPC und verlässt das AWS Netzwerk AWS IoT SiteWise nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt.

Bevor Sie einen Schnittstellen-VPC-Endpunkt für einrichten AWS IoT SiteWise, lesen Sie die Eigenschaften und Einschränkungen des Schnittstellen-Endpunkts im Amazon VPC-Benutzerhandbuch.

Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Unterstützte API-Operationen für VPC-Endpunkte

AWS IoT SiteWise unterstützt Aufrufe der folgenden AWS IoT SiteWise API-Operationen von Ihrer VPC aus:

- Verwenden Sie für alle API-Operationen auf der Datenebene den folgenden Endpunkt: *region*Ersetzen Sie durch AWS-Region

  ```
  data.iotsitewise.region.amazonaws.com
  ```

  Die API-Operationen auf der Datenebene umfassen Folgendes:

  - BatchGetAssetPropertyWert
  - BatchGetAssetPropertyValueHistory
  - BatchPutAssetPropertyWert
  - GetAssetPropertyAggregates
  - GetAssetPropertyValue
  - GetAssetPropertyValueGeschichte

- GetInterpolatedAssetPropertyWerte

- Verwenden Sie für die API-Operationen der Steuerungsebene, mit denen Sie Asset-Modelle, Assets, SiteWise Edge-Gateways, Tags und Kontokonfigurationen verwalten, den folgenden Endpunkt. Ersetze *region* durch deine AWS-Region.

  ```
  api.iotsitewise.region.amazonaws.com
  ```

  Zu den unterstützten API-Vorgängen auf der Kontrollebene gehören:

  - AssociateAssets
  - CreateAsset
  - CreateAssetModell
  - DeleteAsset
  - DeleteAssetModell
  - DeleteDashboard
  - DescribeAsset
  - DescribeAssetModell
  - DescribeAssetEigentum
  - DescribeDashboard
  - DescribeLoggingOptionen
  - DisassociateAssets
  - ListAssetModelle
  - ListAssetBeziehungen
  - ListAssets
  - ListAssociatedVermögenswerte
  - PutLoggingOptionen
  - UpdateAsset
  - UpdateAssetModell
  - UpdateAssetEigentum
  - CreateGateway
  - DeleteGateway
  - DescribeDefaultEncryptionConfiguration

- DescribeGateway
- DescribeGatewayCapabilityConfiguration
- DescribeStorageKonfiguration
- ListGateways
- ListTagsForResource
- UpdateGateway
- UpdateGatewayCapabilityConfiguration
- PutDefaultEncryptionConfiguration
- PutStorageKonfiguration
- TagResource
- UntagResource

> **Note**
>
> Der VPC-Schnittstellen-Endpunkt für die API-Operationen der Kontrollebene unterstützt derzeit keine Aufrufe der folgenden SiteWise Monitor-API-Operationen:
>
> - BatchAssociateProjectAssets
> - BatchDisassociateProjectAssets
> - CreateAccessRichtlinie
> - CreateDashboard
> - CreatePortal
> - CreateProject
> - DeleteAccessPolitik
> - DeletePortal
> - DeleteProject
> - DescribeAccessPolitik
> - DescribePortal
> - DescribeProject
> - ListAccessRichtlinien
> - ListDashboards
> - ListPortals

- ListProjects
- ListProjectVermögenswerte
- UpdateAccessPolitik
- UpdateDashboard
- UpdatePortal
- UpdateProject

Erstellen eines Schnittstellen-VPC-Endpunkts für AWS IoT SiteWise

Um einen VPC-Endpunkt für den AWS IoT SiteWise Service zu erstellen, verwenden Sie entweder die Amazon VPC-Konsole oder die AWS Command Line Interface ()AWS CLI. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für, AWS IoT SiteWise indem Sie einen der folgenden Dienstnamen verwenden:

- Verwenden Sie für die API-Operationen auf Datenebene den folgenden Dienstnamen:

```
com.amazonaws.region.iotsitewise.data
```

- Verwenden Sie für die API-Operationen auf der Steuerungsebene den folgenden Dienstnamen:

```
com.amazonaws.region.iotsitewise.api
```

Zugriff AWS IoT SiteWise über eine Schnittstelle (VPC-Endpunkt)

Wenn Sie einen Schnittstellenendpunkt erstellen, generieren wir endpunktspezifische DNS-Hostnamen, mit denen Sie kommunizieren können. AWS IoT SiteWise Die private DNS-Option ist standardmäßig aktiviert. Weitere Informationen finden Sie unter Verwenden von privat gehosteten Zonen im Amazon VPC-Benutzerhandbuch.

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an einen AWS IoT SiteWise der folgenden VPC-Endpunkte stellen.

- Verwenden Sie für die API-Operationen auf der Datenebene den folgenden Endpunkt: Ersetzen Sie *Region durch Ihren*. AWS-Region

```
data.iotsitewise.region.amazonaws.com
```

- Verwenden Sie für die API-Operationen auf der Kontrollebene den folgenden Endpunkt: Ersetzen Sie *Region* durch Ihre AWS-Region.

```
api.iotsitewise.region.amazonaws.com
```

Wenn Sie privates DNS für den Endpunkt deaktivieren, müssen Sie für den Zugriff AWS IoT SiteWise über den Endpunkt wie folgt vorgehen:

1. Geben Sie die VPC-Endpunkt-URL in API-Anfragen an.
   - Verwenden Sie für die API-Operationen auf der Datenebene die folgende Endpunkt-URL. Ersetzen Sie *vpc-endpoint-id* und *region* durch Ihre VPC-Endpunkt-ID und Region.

     ```
     vpc-endpoint-id.data.iotsitewise.region.vpce.amazonaws.com
     ```

   - Verwenden Sie für die API-Operationen auf der Kontrollebene die folgende Endpunkt-URL. Ersetzen Sie *vpc-endpoint-id* und *region* durch Ihre VPC-Endpunkt-ID und Region.

     ```
     vpc-endpoint-id.api.iotsitewise.region.vpce.amazonaws.com
     ```

2. Deaktivieren Sie die Host-Präfix-Injektion. Die AWS SDKs AWS CLI und stellen dem Service-Endpunkt verschiedene Host-Präfixe voran, wenn Sie die einzelnen API-Operationen aufrufen. Diese Funktion veranlasst die AWS SDKs AWS CLI und, URLs zu erzeugen, die nicht gültig sind, AWS IoT SiteWise wenn Sie einen VPC-Endpunkt angeben.

   > **Important**
   >
   > Sie können die Hostpräfixinjektion in der AWS CLI oder der nicht deaktivieren. AWS Tools for PowerShell Das heißt, wenn Sie privates DNS deaktivieren, können Sie diese Tools nicht für den Zugriff AWS IoT SiteWise über den VPC-Endpunkt verwenden. Aktivieren Sie privates DNS, um das AWS CLI oder das für den AWS Tools for PowerShell Zugriff AWS IoT SiteWise über den Endpunkt zu verwenden.

   Weitere Informationen zur Deaktivierung der Hostpräfixinjektion in den AWS SDKs finden Sie in den folgenden Dokumentationsabschnitten für jedes SDK:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Go v2
- AWS SDK for Java
- AWS SDK for Java 2.x
- AWS SDK for JavaScript
- AWS SDK for .NET
- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für AWS IoT SiteWise

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf AWS IoT SiteWise steuert. Die Richtlinie gibt die folgenden Informationen an:

- Der Principal, der Operationen ausführen kann.
- Die Operationen, die ausgeführt werden können.
- Die Ressourcen, auf denen Operationen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS IoT SiteWise

Das Folgende ist ein Beispiel für eine Endpunktrichtlinie für AWS IoT SiteWise. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie dem Benutzer Zugriff auf die *iotsitewiseadmin*in AWS-Konto *123456789012* aufgelisteten AWS IoT SiteWise Aktionen für das angegebene Asset.

```
{
    "Statement": [
        {
```

```
            "Action": [
                "iotsitewise:CreateAsset",
                "iotsitewise:ListGateways",
                "iotsitewise:ListTagsForResource"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iotsitewise:us-west-2:123456789012:asset/
a1b2c3d4-5678-90ab-cdef-33333EXAMPLE",
            "Principal": {
                "AWS": [
                    "123456789012:user/iotsitewiseadmin"
                ]
            }
        }
    ]
}
```

Bewährte Sicherheitsmethoden für AWS IoT SiteWise

Dieses Thema enthält bewährte Sicherheitsmethoden für AWS IoT SiteWise.

Verwenden Sie Anmeldeinformationen für die Authentifizierung auf Ihren OPC-UA-Servern

Verlangen Sie Anmeldeinformationen für die Authentifizierung zum Herstellen einer Verbindung mit Ihren OPC-UA-Servern. Weitere Informationen hierzu finden Sie in der Dokumentation für Ihren Server. Damit Ihr SiteWise Edge-Gateway dann eine Verbindung zu Ihren OPC-UA-Servern herstellen kann, fügen Sie Ihrem SiteWise Edge-Gateway Serverauthentifizierungsgeheimnisse hinzu. Weitere Informationen finden Sie unter Konfigurieren der Quellauthentifizierung.

Verwenden Sie verschlüsselter Kommunikationsmodi für Ihre OPC-UA-Server

Wählen Sie einen nicht veralteten Sicherheitsmodus für verschlüsselte Nachrichten, wenn Sie Ihre OPC-UA-Quellen für Ihr Edge-Gateway konfigurieren. SiteWise Dies trägt zum Schutz Ihrer Industriedaten bei der Übertragung von Ihren OPC-UA-Servern zum Edge-Gateway bei. SiteWise Weitere Informationen finden Sie unter Daten in Übertragung über das lokale Netzwerk und Konfigurieren von Datenquellen.

Halten Sie Ihre Komponenten auf dem neuesten Stand

Wenn Sie SiteWise Edge-Gateways verwenden, um Daten in den Dienst aufzunehmen, liegt es in Ihrer Verantwortung, die Umgebung Ihres Edge-Gateways zu konfigurieren und zu warten. SiteWise Diese Verantwortung umfasst die Aktualisierung auf die neuesten Versionen der Systemsoftware, AWS IoT Greengrass Software und Konnektoren des Gateways.

> **Note**
>
> Der AWS IoT SiteWise Edge-Connector speichert Geheimnisse in Ihrem Dateisystem. Diese Geheimnisse steuern, wer die in Ihrem SiteWise Edge-Gateway zwischengespeicherten Daten einsehen kann. Es wird dringend empfohlen, die Festplatten- oder Dateisystemverschlüsselung für das System zu aktivieren, auf dem Ihr SiteWise Edge-Gateway ausgeführt wird.

Verschlüsseln Sie das Dateisystem Ihres SiteWise Edge-Gateways

Verschlüsseln und sichern Sie Ihr SiteWise Edge-Gateway, sodass Ihre Industriedaten sicher sind, wenn sie das SiteWise Edge-Gateway passieren. Wenn Ihr SiteWise Edge-Gateway über ein Hardware-Sicherheitsmodul verfügt, können Sie es so konfigurieren, AWS IoT Greengrass dass Ihr SiteWise Edge-Gateway gesichert wird. Weitere Informationen finden Sie unter Hardwaresicherheitsintegration im AWS IoT Greengrass Version 1 Entwicklerhandbuch. Andernfalls finden Sie in der Dokumentation Ihres Betriebssystems Informationen zum Verschlüsseln und Sichern des Dateisystems.

Sicherer Zugriff auf Ihre Edge-Konfiguration

Geben Sie weder Ihr Passwort für die Edge-Console-Anwendung noch das Passwort Ihrer SiteWise Monitor-Anwendung weiter. Geben Sie dieses Passwort nicht an Orten ab, an denen es für jedermann sichtbar ist. Implementieren Sie eine Richtlinie zur korrekten Passwortrotation, indem Sie ein geeignetes Ablaufdatum für Ihr Passwort konfigurieren.

Gewähren SiteWise Sie Monitor-Benutzern die geringstmöglichen Berechtigungen

Folgen Sie dem Prinzip der geringsten Rechte, indem Sie die Mindestanzahl an Zugriffsrichtlinienberechtigungen für Ihre Portalbenutzer verwenden.

- Definieren Sie bei der Erstellung eines Portals eine Rolle, die die Mindestanzahl der für dieses Portal erforderlichen Komponenten zulässt. Weitere Informationen finden Sie unter Verwenden von Servicerollen für AWS IoT SiteWise Monitor.
- Wenn Sie und Ihre Portaladministratoren Projekte erstellen und freigeben, verwenden Sie die Mindestanzahl an Komponenten, die für dieses Projekt erforderlich sind.
- Wenn eine Identität keinen Zugriff mehr auf ein Portal oder Projekt benötigt, entfernen Sie sie aus dieser Ressource. Wenn diese Identität für Ihre Organisation nicht mehr gilt, löschen Sie diese Identität aus Ihrem Identitätsspeicher.

Die bewährte Methode nach dem Prinzip „Least Principes“ gilt auch für IAM-Rollen. Weitere Informationen finden Sie unter Bewährte Methoden für Richtlinien.

Legen Sie vertrauliche Informationen nicht offen

Sie sollten verhindern, dass Anmeldeinformationen und andere vertrauliche Informationen wie beispielsweise personenbezogene Daten protokolliert werden. Es wird empfohlen, die folgenden Sicherheitsvorkehrungen zu implementieren, auch wenn für den Zugriff auf lokale Protokolle auf einem SiteWise Edge-Gateway Root-Rechte und für den Zugriff auf CloudWatch Protokolle IAM-Berechtigungen erforderlich sind.

- Verwenden Sie keine vertraulichen Informationen in Namen, Beschreibungen oder Eigenschaften Ihrer Komponenten oder Modelle.
- Verwenden Sie keine vertraulichen Informationen in SiteWise Edge-Gateways oder Quellnamen.
- Verwenden Sie keine vertraulichen Informationen in Namen oder Beschreibungen Ihrer Portale, Projekte oder Dashboards.

Befolgen Sie AWS IoT Greengrass die bewährten Sicherheitsmethoden

Befolgen Sie die bewährten AWS IoT Greengrass Sicherheitsmethoden für Ihr SiteWise Edge-Gateway. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden im AWS IoT Greengrass Version 1 Entwicklerhandbuch.

Weitere Informationen finden Sie auch unter

- Bewährte Sicherheitsmethoden im AWS IoT Entwicklerhandbuch
- Zehn goldene Sicherheitsregeln für industrielle IoT-Lösungen

Einloggen und Überwachen AWS IoT SiteWise

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS IoT SiteWise anderen AWS Lösungen. AWS IoT SiteWise unterstützt die folgenden Überwachungstools, um den Service zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Erfassen und verfolgen Sie Kennzahlen, erstellen Sie maßgeschneiderte Dashboards und richten Sie Alarme ein, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen bestimmten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon CloudWatch Logs überwacht, speichert und greift auf Ihre Protokolldateien von SiteWise Edge-Gateways und anderen CloudTrail Quellen zu. CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden. Anschließend CloudTrail werden die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket übermittelt. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.

Themen

Überwachung mit Amazon CloudWatch Logs

Stellen Sie AWS IoT SiteWise die Konfiguration so ein, dass Informationen in CloudWatch Logs protokolliert werden, um den Dienst zu überwachen und Fehler zu beheben.

Wenn Sie die AWS IoT SiteWise Konsole verwenden, AWS IoT SiteWise wird eine dienstbezogene Rolle erstellt, die es dem Dienst ermöglicht, Informationen in Ihrem Namen zu protokollieren. Wenn Sie die AWS IoT SiteWise Konsole nicht verwenden, müssen Sie manuell eine dienstbezogene Rolle erstellen, um Protokolle zu empfangen. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle für AWS IoT SiteWise.

Sie benötigen eine Ressourcenrichtlinie, die es ermöglicht, Protokollereignisse in CloudWatch Streams AWS IoT SiteWise zu speichern. Führen Sie den folgenden Befehl aus, um eine Ressourcenrichtlinie für CloudWatch Logs zu erstellen und zu aktualisieren. *logging-policy-name*Ersetzen Sie ihn durch den Namen der zu erstellenden Richtlinie.

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

CloudWatch Logs unterstützt auch die Kontextschlüssel aws: SourceArn und aws: SourceAccount condition. Diese Bedingungskontextschlüssel sind optional.

Um eine Ressourcenrichtlinie zu erstellen oder AWS IoT SiteWise zu aktualisieren, die es erlaubt, nur Protokolle, die mit der angegebenen AWS IoT SiteWise Ressource verknüpft sind, in CloudWatch Streams zu speichern, führen Sie den Befehl aus und gehen Sie wie folgt vor:

- *logging-policy-name*Ersetzen Sie ihn durch den Namen der zu erstellenden Richtlinie.
- Ersetzen Sie *Source-ARN* durch den ARN Ihrer AWS IoT SiteWise Ressource, z. B. eines Asset-Modells oder eines Assets. Den ARN für jeden AWS IoT SiteWise Ressourcentyp finden Sie unter Ressourcentypen definiert von AWS IoT SiteWise in der Service Authorization Reference.
- Ersetzen Sie *Account-ID* durch die AWS Konto-ID, die der angegebenen AWS IoT SiteWise Ressource zugeordnet ist.

```
aws logs put-resource-policy --policy-name logging-policy-name --policy-
document "{ \"Version\": \"2012-10-17\", \"Statement\": [ { \"Sid\":
```

```
 \"IoTSiteWiseToCloudWatchLogs\", \"Effect\": \"Allow\", \"Principal\": { \"Service
\": [ \"iotsitewise.amazonaws.com\" ] }, \"Action\":\"logs:PutLogEvents\", \"Resource
\": \"*\", \"Condition\":{\"StringLike\":{\"aws:SourceArn\":[\"source-ARN\"],
\"aws:SourceAccount\":[\"account-ID\"]}}}]}"
```

Standardmäßig werden AWS IoT SiteWise keine Informationen in Logs protokolliert. CloudWatch Um die Protokollierung zu aktivieren, wählen Sie eine andere Protokollierungsebene als Deaktiviert (`OFF`). AWS IoT SiteWise unterstützt die folgenden Protokollierungsebenen:

- `OFF`— Die Protokollierung ist ausgeschaltet.
- `ERROR`— Fehler werden protokolliert.
- `INFO`— Fehler und Informationsmeldungen werden protokolliert.

Sie können SiteWise Edge-Gateways so konfigurieren, dass sie Informationen in CloudWatch Logs protokollieren. AWS IoT Greengrass Weitere Informationen finden Sie unter Überwachung von SiteWise Edge-Gateway-Protokollen.

Sie können auch so konfigurieren AWS IoT Core , dass Informationen in CloudWatch Protokollen protokolliert werden, wenn Sie eine AWS IoT SiteWise Regelaktion beheben. Weitere Informationen finden Sie unter Problembehandlung und AWS IoT SiteWise Regelaktion.

Inhalt

Verwaltung der Anmeldung AWS IoT SiteWise

Verwenden Sie die AWS IoT SiteWise Konsole oder AWS CLI für die folgenden Aufgaben zur Konfiguration der Protokollierung.

Finden Sie Ihre Protokollierungsebene

Console

Gehen Sie wie folgt vor, um die aktuelle Protokollierungsstufe in der AWS IoT SiteWise -Konsole zu finden.

Um Ihre aktuelle AWS IoT SiteWise Protokollierungsstufe zu ermitteln

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Logging options (Protokollierungsoptionen) aus.

   Der aktuelle Protokollierungsstatus wird unter Logging status (Protokollierungsstatus) angezeigt. Wenn die Protokollierung aktiviert ist, wird die aktuelle Protokollierungsstufe unter Ausführlichkeitsstufe angezeigt.

AWS CLI

Führen Sie den folgenden Befehl aus, um Ihre aktuelle AWS IoT SiteWise Protokollierungsstufe mit dem zu ermitteln. AWS CLI

```
aws iotsitewise describe-logging-options
```

Die Operation gibt eine Antwort mit Ihrer Protokollierungsstufe im folgenden Format zurück.

```
{
  "loggingOptions": {
    "level": "String"
  }
}
```

Ändern Sie Ihre Protokollierungsebene

Gehen Sie wie folgt vor, um Ihre Protokollierungsstufe in der AWS IoT SiteWise Konsole oder mithilfe von zu ändern AWS CLI.

Console

Um Ihre AWS IoT SiteWise Protokollierungsstufe zu ändern

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im linken Navigationsbereich Logging options (Protokollierungsoptionen) aus.
3. Wählen Sie Bearbeiten aus.
4. Wählen Sie den Grad der Ausführlichkeit, den Sie aktivieren möchten.

5. Wählen Sie Speichern.

AWS CLI

Führen Sie den folgenden AWS CLI Befehl aus, um Ihre AWS IoT SiteWise Protokollierungsstufe zu ändern. Ersetzen Sie *logging-level* durch die gewünschte Protokollierungsstufe.

```
aws iotsitewise put-logging-options --logging-options level=logging-level
```

Beispiel: Einträge in AWS IoT SiteWise Protokolldateien

Jeder AWS IoT SiteWise Protokolleintrag enthält Ereignisinformationen und relevante Ressourcen für dieses Ereignis, sodass Sie die Protokolldaten verstehen und analysieren können.

Das folgende Beispiel zeigt einen CloudWatch Logs-Eintrag, der AWS IoT SiteWise protokolliert, wann Sie ein Asset-Modell erfolgreich erstellt haben.

```
{
  "eventTime": "2020-05-05T00:10:22.902Z",
  "logLevel": "INFO",
  "eventType": "AssetModelCreationSuccess",
  "message": "Successfully created asset model.",
  "resources": {
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE"
  }
}
```

Überwachung von SiteWise Edge-Gateway-Protokollen

Sie können Ihr AWS IoT SiteWise Edge-Gateway so konfigurieren, dass Informationen in Amazon CloudWatch Logs oder im lokalen Dateisystem protokolliert werden.

Themen

- Amazon CloudWatch Logs verwenden
- Verwenden von Serviceprotokollen
- Verwenden von Ereignisprotokollen

Amazon CloudWatch Logs verwenden

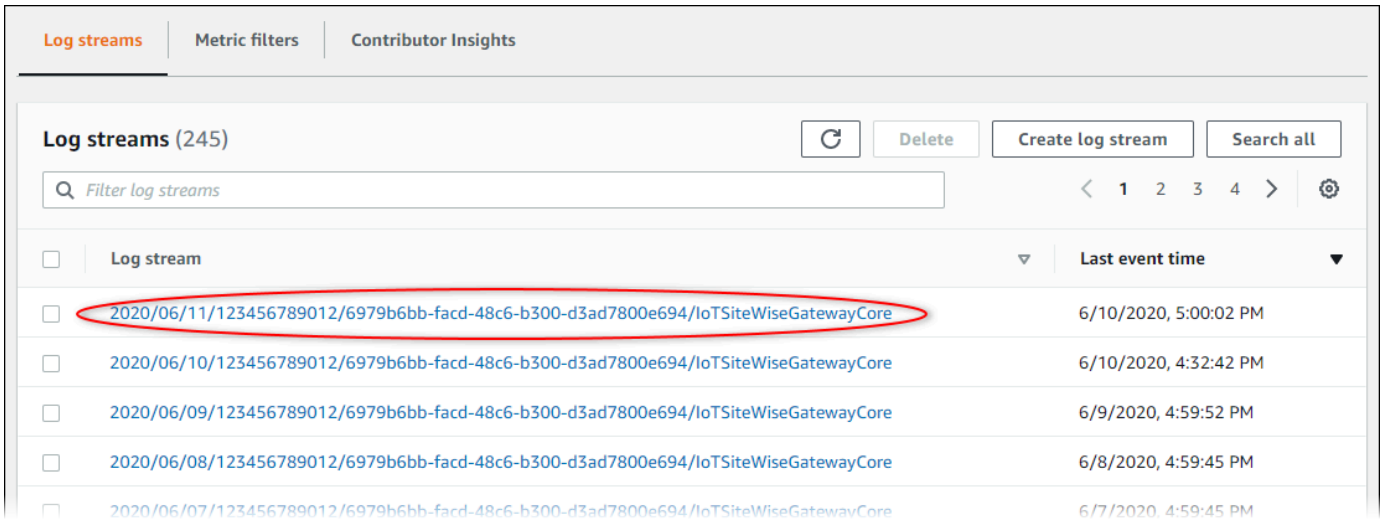
Sie können Ihr SiteWise Edge-Gateway so konfigurieren, dass CloudWatch Protokolle an Logs gesendet werden. Weitere Informationen finden Sie unter Aktivieren der Protokollierung für CloudWatch Protokolle im AWS IoT Greengrass Version 2 Entwicklerhandbuch.

So konfigurieren Sie CloudWatch Protokolle und greifen auf sie zu (Konsole)

1. Navigieren Sie zur CloudWatch-Konsole.
2. Wählen Sie im Navigationsbereich Protokollgruppen aus.
3. Sie finden die AWS IoT SiteWise Komponentenprotokolle in den folgenden Protokollgruppen:

   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgeCollectorOpcua`— Die Protokolle für die Komponente des SiteWise Edge-Gateways, die Daten aus den OPC-UA-Quellen des SiteWise Edge-Gateways sammelt.
   - `/aws/greengrass/UserComponent/region/aws.iot.SiteWiseEdgePublisher`— Die Protokolle für die Komponente des SiteWise Edge-Gateways, für die OPC-UA-Datenströme veröffentlicht werden. AWS IoT SiteWise

   Wählen Sie die Protokollgruppe für die Funktion aus, die debuggt werden soll.
4. Wählen Sie einen Protokollstream aus, dessen Name mit dem Namen Ihrer AWS IoT Greengrass Gruppe endet. CloudWatch Zeigt standardmäßig den neuesten Log-Stream zuerst an.



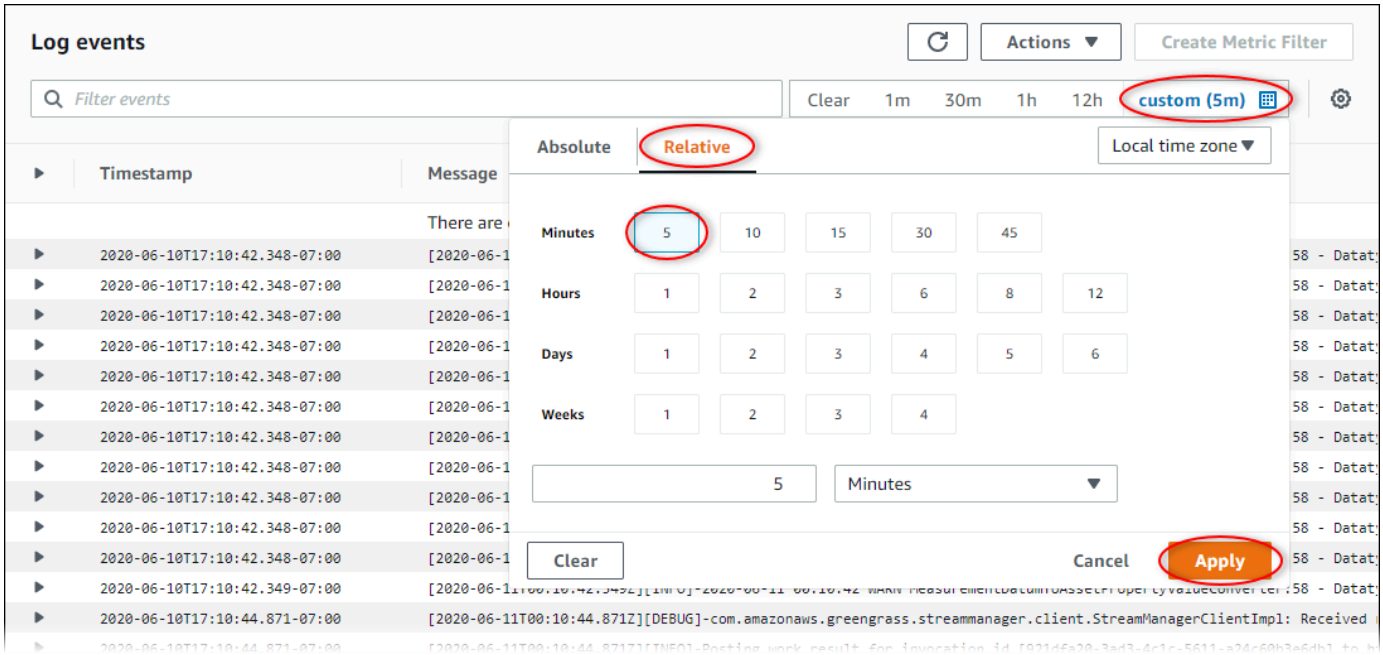
5. Führen Sie die folgenden Schritte aus, um Protokolle der letzten 5 Minuten anzuzeigen:

a. Wählen Sie in der oberen rechten Ecke Custom (Benutzerdefiniert).

b. Wählen Sie Relative (Relativ).

c. Wählen Sie 5 Minuten.

d. Wählen Sie Apply (Anwenden) aus.



6. (Optional) Um weniger Protokolle anzuzeigen, können Sie rechts oben 1m auswählen.

7. Scrollen Sie zum Ende der Protokolleinträge, um die neuesten Protokolle anzuzeigen.

Verwenden von Serviceprotokollen

SiteWise Edge-Gateway-Geräte enthalten Dienstprotokolldateien, die beim Debuggen von Problemen helfen. Die folgenden Abschnitte helfen Ihnen dabei, die Dienstprotokolldateien für die Komponenten AWS IoT SiteWise OPC-UA Collector und Publisher zu finden und AWS IoT SiteWise zu verwenden.

AWS IoT SiteWise OPC-UA Collector-Serviceprotokolldatei

Die AWS IoT SiteWise OPC-UA Collector-Komponente verwendet die folgende Protokolldatei.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log
```

Um die Logs dieser Komponente einzusehen

- Führen Sie den folgenden Befehl auf dem Kerngerät aus, um die Protokolldatei dieser Komponente in Echtzeit anzuzeigen. Ersetzen Sie */greengrass/v2*oder *C:\greengrass\v2* durch den Pfad zum AWS IoT Greengrass Stammordner.

  Linux

  ```
  sudo tail -f /greengrass/v2/logs/aws.iot.SiteWiseEdgeCollectorOpcua.log
  ```

  Windows (PowerShell)

  ```
  Get-Content C:\greengrass\v2\logs\aws.iot.SiteWiseEdgeCollectorOpcua.log -Tail
   10 -Wait
  ```

AWS IoT SiteWise Protokolldatei des Publisher-Dienstes

Die AWS IoT SiteWise Publisher-Komponente verwendet die folgende Protokolldatei.

Linux

```
/greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows

```
C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log
```

Um die Protokolle dieser Komponente anzuzeigen

- Führen Sie den folgenden Befehl auf dem Kerngerät aus, um die Protokolldatei dieser Komponente in Echtzeit anzuzeigen. Ersetzen Sie */greengrass/v2*oder *C:\greengrass\v2* durch den Pfad zum AWS IoT Greengrass Stammordner.

Linux

```
sudo tail -f /greengrass/v2/logs/aws.iot.SiteWiseEdgePublisher.log
```

Windows (PowerShell)

```
Get-Content C:\greengrass\v2\logs\aws.iot.SiteWiseEdgePublisher.log -Tail 10 -
Wait
```

Verwenden von Ereignisprotokollen

SiteWise Edge-Gateway-Geräte enthalten Ereignisprotokolldateien, die beim Debuggen von Problemen helfen. Die folgenden Abschnitte helfen Ihnen dabei, die Ereignisprotokolldateien für die Komponenten AWS IoT SiteWise OPC-UA Collector und Publisher zu finden und AWS IoT SiteWise zu verwenden.

AWS IoT SiteWise OPC-UA Collector-Ereignisprotokolle

Die AWS IoT SiteWise OPC-UA Collector-Komponente umfasst ein Ereignisprotokoll, mit dem Kunden Probleme identifizieren und beheben können. Die Protokolldatei ist von der lokalen Protokolldatei getrennt und befindet sich im folgenden Verzeichnis. Ersetzen Sie */greengrass/v2*oder *C:\greengrass\v2* durch den Pfad zum AWS IoT Greengrass Stammordner.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgeCollectorOpcua/logs/
IotSiteWiseOpcUaCollectorEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgeCollectorOpcua\logs
\IotSiteWiseOpcUaCollectorEvents.log
```

Dieses Protokoll enthält detaillierte Informationen und Anweisungen zur Fehlerbehebung. Informationen zur Fehlerbehebung werden zusammen mit der Diagnose bereitgestellt. Sie enthalten eine Beschreibung, wie das Problem behoben werden kann, und manchmal auch Links zu weiteren Informationen. Die Diagnoseinformationen umfassen Folgendes:

- Schweregrad
- Zeitstempel
- Zusätzliche ereignisspezifische Informationen

Example Beispielprotokoll

```
dataSourceConnectionSuccess:
  Summary: Successfully connected to OpcUa server
  Level: INFO
  Timestamp: '2023-06-15T21:04:16.303Z'
  Description: Successfully connected to the data source.
  AssociatedMetrics:
  - Name: FetchedDataStreams
    Description: The number of fetched data streams for this data source
    Value: 1.0
    Namespace: IoTSiteWise
    Dimensions:
    - Name: SourceName
      Value: SourceName{value=OPC-UA Server}
    - Name: ThingName
      Value: test-core
  AssociatedData:
  - Name: DataSourceTrace
    Description: Name of the data source
    Data:
    - OPC-UA Server
  - Name: EndpointUri
    Description: The endpoint to which the connection was attempted.
    Data:
    - '"opc.tcp://10.0.0.1:1234"'
```

AWS IoT SiteWise Ereignisprotokolle des Herausgebers

Die AWS IoT SiteWise Publisher-Komponente umfasst ein Ereignisprotokoll, mit dem Kunden Probleme identifizieren und beheben können. Die Protokolldatei ist von der lokalen Protokolldatei getrennt und befindet sich am folgenden Speicherort. Ersetzen Sie */greengrass/v2*oder *C:\greengrass\v2* durch den Pfad zum AWS IoT Greengrass Stammordner.

Linux

```
/greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/logs/
IotSiteWisePublisherEvents.log
```

Windows

```
C:\greengrass\v2\work\aws.iot.SiteWiseEdgePublisher\logs
\IotSiteWisePublisherEvents.log
```

Dieses Protokoll enthält detaillierte Informationen und Anweisungen zur Fehlerbehebung. Informationen zur Fehlerbehebung werden zusammen mit der Diagnose bereitgestellt. Sie enthalten eine Beschreibung, wie das Problem behoben werden kann, und manchmal auch Links zu weiteren Informationen. Die Diagnoseinformationen umfassen Folgendes:

- Schweregrad
- Zeitstempel
- Zusätzliche ereignisspezifische Informationen

Example Beispielprotokoll

```
accountBeingThrottled:
  Summary: Data upload speed slowed due to quota limits
  Level: WARN
  Timestamp: '2023-06-09T21:30:24.654Z'
  Description: The IoT SiteWise Publisher is limited to the "Rate of data points
 ingested"
    quota for a customers account. See the associated documentation and associated
    metric for the number of requests that were limited for more information. Note
    that this may be temporary and not require any change, although if the issue
 continues
    you may need to request an increase for the mentioned quota.
  FurtherInformation:
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/quotas.html
  - https://docs.aws.amazon.com/iot-sitewise/latest/userguide/troubleshooting-
gateway.html#gateway-issue-data-streams
  AssociatedMetrics:
  - Name: TotalErrorCount
    Description: The total number of errors of this type that occurred.
```

```
    Value: 327724.0
  AssociatedData:
  - Name: AggregatePropertyAliases
    Description: The aggregated property aliases of the throttled data.
    FileLocation: /greengrass/v2/work/aws.iot.SiteWiseEdgePublisher/./logs/data/
AggregatePropertyAliases_1686346224654.log
```

Überwachung AWS IoT SiteWise mit CloudWatch Amazon-Metriken

Sie können die AWS IoT SiteWise Nutzung überwachen CloudWatch, wobei Rohdaten gesammelt und zu lesbaren Metriken verarbeitet werden, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

AWS IoT SiteWise veröffentlicht die in den folgenden Abschnitten aufgeführten Metriken und Dimensionen im `AWS/IoTSiteWise` Namespace.

> **Tip**
>
> AWS IoT SiteWise veröffentlicht Metriken in einem Intervall von einer Minute. Wenn Sie diese Metriken in der CloudWatch Konsole grafisch anzeigen, empfehlen wir Ihnen, einen Zeitraum von 1 Minute zu wählen. So können Sie die Metrikdaten in der höchsten verfügbaren Auflösung anzeigen.

Themen

AWS IoT Greengrass Version 2 Gateway-Metriken

AWS IoT SiteWise veröffentlicht die folgenden SiteWise Edge-Gateway-Metriken. Alle SiteWise Edge-Gateway-Metriken werden in einem Intervall von einer Minute veröffentlicht.

SiteWise Edge-Gateway-Metriken

Metrik	Beschreibung
`Gateway.CpuUsage`	Die CPU-Auslastung eines SiteWise Edge-Gateways. Einheit: Prozentsatz Dimension: Keine
`Gateway.TotalDiskSpace`	Der gesamte Festplattenspeicher eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.UsedDiskSpace`	Der verwendete Festplattenspeicher eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.AvailableDiskSpace`	Der verfügbare Festplattenspeicher eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.UsedPercentageDiskSpace`	Der verwendete Prozentsatz des Festplattenspeichers eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.TotalMemory`	Der gesamte Speicher eines SiteWise Edge-Gateways.

Metrik	Beschreibung
	Einheit: Byte Dimension: Keine
`Gateway.UsedMemory`	Der verwendete Speicher eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.AvailableMemory`	Der verfügbare Speicher eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.UsedPercentageMemory`	Der prozentuale Anteil des verwendeten Speichers eines SiteWise Edge-Gateways. Einheit: Byte Dimension: Keine
`Gateway.CloudConnectivity`	Der Cloud-Konnektivitätsstatus eines SiteWise Edge-Gateways. Einheit: keine Abmessung: GatewayId
`Gateway.SWE.Component.RunningStatus`	Der Betriebsstatus von Komponenten auf einem SiteWise Edge-Gateway. Einheit: keine Abmessung: GatewayId

OPC-UA-Collector-Metriken

Metrik	Beschreibung
`OpcUaCollector.Heartbeat`	Wird jede Minute für jede OPC-UA-Quelle (`sourceName`) generiert, die mit einem SiteWise Edge-Gateway () verbunden ist. `gatewayId` Einheit: Anzahl (1 steht für die Verbindung der Quelle und 0 für die Unterbrechung der Quelle.) Abmessungen: GatewayId, SourceName
`OpcUaCollector.ActiveDataStreamCount`	Die Anzahl der Datenströme, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle () abonniert hat. `sourceName` Einheit: Anzahl Abmessungen:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Die Anzahl der pro Minute generierten Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle (`sourceName`) empfangen hat. Einheit: Anzahl Abmessungen: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) von einer OPC-UA-Quelle (`sourceName`) empfängt und bei denen es sich nicht um gültige Werte handelt. Diese Datenpunkte werden nicht vom OpcUa Collector aufgenommen, sondern jede Minute generiert.

Metrik	Beschreibung
	Einheit: Anzahl Abmessungen: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.ConversionErrors`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle (`sourceName`) empfangen hat, was zu Konvertierungsfehlern beim Senden der Daten führte. AWS IoT SiteWise Diese Datenpunkte werden nicht von Collector aufgenommen. OpcUa Einheit: Anzahl Abmessungen: GatewayId, SourceName

AWS IoT SiteWise Prozessor-Metriken

Metrik	Beschreibung
`Gateway.DataProcessor.IngestionSuccess`	Die Anzahl der Datenpunkte, die erfolgreich aufgenommen wurden und pro Minute generiert wurden. Einheit: Anzahl Dimensionen: Keine
`Gateway.DataProcessor.IngestionThrottled`	Die Anzahl der pro Minute generierten Datenpunkte, die gedrosselt wurden. Einheit: Anzahl Abmessungen: ThrottledAt
`Gateway.DataProcessor.MeasurementRejected`	Die Anzahl der verworfenen Messungen, die pro Minute generiert wurden.

Metrik	Beschreibung
	Einheit: Anzahl Abmessungen: Grund
`Gateway.DataProcessor.MeasurementUnmodeled`	Die Anzahl der Messungen, die nicht modelliert wurden und pro Minute generiert wurden. Einheit: Anzahl Abmessungen: Grund
`Gateway.DataProcessor.MessagesRemaining`	Die Anzahl der in einem Stream verbleibenden Nachrichten, die jede Minute generiert werden. Einheit: Anzahl Abmessungen: StreamName
`Gateway.DataProcessor.ProcessingError`	Die Anzahl der Verarbeitungsfehler, die jede Minute generiert werden. Einheit: Anzahl Dimensionen: Grund
`IoTSiteWiseProcessor.IsConnectedToMqttBroker`	Wird jede Minute vom Prozessor im SiteWise Edge-Gateway generiert. Einheit: 1 (1 steht für den Prozessor, der mit einem MQTT-Broker verbunden ist.) Abmessungen: GatewayId

Metrik	Beschreibung
`IoTSiteWiseProcessor.NumberOfSubscriptionsToMqttBroker`	Die Anzahl der Themen, die der Prozessor pro Minute für den MQTT-Broker abonniert hat. Ein mehrstufiges Wildcard-Thema wird als 1 gezählt. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWiseProcessor.NumberOfUniqueMqttTopicsReceived`	Die Anzahl der eindeutigen Themen, die der Prozessor vom MQTT-Broker erhält und pro Minute generiert wird. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWiseProcessor.MqttMessageReceivedSuccessCount`	Die Anzahl der Nachrichten, die der Prozessor erfolgreich vom MQTT-Broker empfangen hat und jede Minute generiert wird. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWiseProcessor.MqttReceivedSuccessBytes`	Die Anzahl der Byte an Nachrichtendaten, die der Prozessor erfolgreich vom MQTT-Broker empfangen hat und die jede Minute generiert werden. Einheit: Anzahl Abmessungen: GatewayId

AWS IoT SiteWise Metriken für Herausgeber

Metrik	Beschreibung
`IoTSiteWisePublisher.Heartbeat`	Wird jede Minute vom Publisher im SiteWise Edge-Gateway generiert. Einheit: 1 (1 steht dafür, dass der Publisher läuft und der Datenpunkt fehlt, was bedeutet, dass der Publisher nicht läuft.) Abmessungen: GatewayId
`IoTSiteWisePublisher.PublishSuccessCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`GatewayId `) erfolgreich in der Cloud veröffentlicht hat und die jede Minute generiert wurden. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.PublishFailureCount`	Die Anzahl der pro Minute generierten Datenpunkte, die ein SiteWise Edge-Gateway (`GatewayId `) nicht veröffentlichen konnte. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.PublishRejectedCount`	Die Anzahl der pro Minute generierten Datenpunkte, die ein SiteWise Edge-Gateway (`GatewayId `) von der Cloud-Seite zurückgewiesen hat. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.DroppedCount`	Die Anzahl der Datenpunkte, die von einem SiteWise Edge-Gateway (`GatewayId `)

Metrik	Beschreibung
	gelöscht und nicht in der Cloud veröffentlicht werden, wird jede Minute generiert. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.IsConnectedToMqttBroker`	Wird jede Minute vom Publisher im SiteWise Edge-Gateway generiert. Einheit: 1 (1 steht für den Herausgeber, der mit einem MQTT-Broker verbunden ist.) Abmessungen: GatewayId
`IoTSiteWisePublisher.NumberOfSubscriptionsToMqttBroker`	Die Anzahl der Themen, die der Publisher für den MQTT-Broker abonniert hat, wird jede Minute generiert. Ein mehrstufiges Wildcard-Thema wird als 1 gezählt. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.NumberOfUniqueMqttTopicsReceived`	Die Anzahl der eindeutigen Themen, die der Publisher vom MQTT-Broker erhält und pro Minute generiert wird. Einheit: Anzahl Abmessungen: GatewayId
`IoTSiteWisePublisher.MqttMessageReceivedSuccessCount`	Die Anzahl der Nachrichten, die der Publisher erfolgreich vom MQTT-Broker empfangen hat und die jede Minute generiert wurden. Einheit: Anzahl Abmessungen: GatewayId

Metrik	Beschreibung
`IoTSiteWisePublisher.MqttReceivedSuccessBytes`	Die Anzahl der Byte an Nachrichtendaten, die der Publisher erfolgreich vom MQTT-Broker empfangen hat und die jede Minute generiert wurden. Einheit: Anzahl Abmessungen: GatewayId

AWS IoT Greengrass Version 1 Gateway-Metriken

AWS IoT SiteWise veröffentlicht die folgenden SiteWise Edge-Gateway-Metriken. Alle SiteWise Edge-Gateway-Metriken werden in einem Intervall von einer Minute veröffentlicht.

> **Important**
>
> Um SiteWise Edge-Gateway-Metriken zu erhalten, müssen Sie mindestens Version 6 des AWS IoT SiteWise Connectors auf Ihrem SiteWise Edge-Gateway verwenden. Weitere Informationen finden Sie unter AWS IoT SiteWise OPC-UA Collector im AWS IoT Greengrass Version 1 Developer Guide.

SiteWise Edge-Gateway-Metriken

Metrik	Beschreibung
`Gateway.Heartbeat`	Wird jede Minute für jedes verbundene SiteWise Edge-Gateway (`gatewayId`) generiert. Einheit: 1 (1 steht dafür, dass das SiteWise Edge-Gateway aktiv ist und der Datenpunkt fehlt, der repräsentiert, dass das SiteWise Edge-Gateway von der Cloud getrennt ist.) Abmessung: GatewayId

Metrik	Beschreibung
`Gateway.PublishSuccessCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) erfolgreich veröffentlicht hat. Einheit: Anzahl Dimension: GatewayId
`Gateway.PublishFailureCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) nicht veröffent lichen konnte. Diese Metrik zählt Fehler, die sich aus den Aufrufen des SiteWise Edge-Gateways für den BatchPutAssetPropertyValueVorgang ergeben. Weitere Informationen zur Fehlerbeh ebung bei SiteWise Edge-Gateways finden Sie unterFehlerbehebung bei einem SiteWise Edge-Gateway. Einheit: Anzahl Abmessung: GatewayId

Metrik	Beschreibung
`Gateway.ProcessFailureCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) nicht verarbeiten konnte. Diese Metrik zählt Fehler, die zwischen dem SiteWise Edge-Gateway und den Quellen des SiteWise Edge-Gateways auftreten, einschließlich der Fehler, die von Quellen gemeldet wurden. Weitere Informationen zur Fehlerbehebung bei SiteWise Edge-Gateways finden Sie unterFehlerbehebung bei einem SiteWise Edge-Gateway. Einheit: Anzahl Abmessung: GatewayId
`Gateway.PublishRejectedCount`	Die Anzahl der Datenpunkte von einem SiteWise Edge-Gateway (`gatewayId`), die zurückgewiesen wurden. Einheit: Anzahl Dimension: GatewayId

OPC-UA-bezogene Metriken

Metrik	Beschreibung
`OPCUACollector.Heartbeat`	Wird jede Minute für jede OPC-UA-Quelle (`sourceName`) generiert, die mit einem SiteWise Edge-Gateway () verbunden ist. `gatewayId` Einheit: Anzahl (1 steht für die Verbindung der Quelle und 0 für die Unterbrechung der Quelle.)

Metrik	Beschreibung
	Abmessungen: GatewayId, SourceName
`OPCUACollector.ActiveDataStreamCount`	Die Anzahl der Datenströme, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle () abonniert hat. `sourceName` Einheit: Anzahl Abmessungen:,, GatewayId SourceName PropertyGroup
`OpcUaCollector.IncomingValuesCount`	Die Anzahl der pro Minute generierten Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle (`sourceName`) empfangen hat. Einheit: Anzahl Abmessungen: GatewayId,, SourceName PropertyGroup
`OpcUaCollector.IncomingValuesError`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) von einer OPC-UA-Quelle (`sourceName`) empfangen hat und die keine gültigen Werte sind. Diese Datenpunkte werden nicht vom OpcUa Collector aufgenommen und jede Minute generiert. Einheit: Anzahl Abmessungen: GatewayId,, SourceName PropertyGroup

Metrik	Beschreibung
`OpcUaCollector.ConversionErrors`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine OPC-UA-Quelle (`sourceName`) empfangen hat, was zu Konvertierungsfehlern beim Senden der Daten führte. AWS IoT SiteWise Diese Datenpunkte werden nicht von Collector aufgenommen. OpcUa Einheit: Anzahl Abmessungen: GatewayId, SourceName

EIP-bezogene Metriken

Metrik	Beschreibung
`EIPCollector.Heartbeat`	Wird jede Minute für jede EIP-Quelle (`sourceName`) generiert, die mit einem SiteWise Edge-Gateway (`gatewayId`) verbunden ist. Einheit: 1 (1 steht für die Quelle ist verbunden und fehlt der Datenpunkt, der die Quelle darstellt, ist getrennt.) Abmessungen:, GatewayId SourceName
`EIPCollector.IncomingValuesCount`	Die Anzahl der Datenströme, die ein SiteWise Edge-Gateway (`gatewayId`) für eine EIP-Quelle (`sourceName`) abonniert hat. Einheit: Anzahl Abmessungen:, GatewayId SourceName

Metrik	Beschreibung
`EIPCollector.ActiveDataStreamCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine EIP-Quelle (`sourceName`) empfangen hat. Einheit: Anzahl Abmessungen: GatewayId, SourceName

Modbus-bezogene Metriken

Metrik	Beschreibung
`ModbusTCPCollector.Heartbeat`	Wird jede Minute für jede Modbus-Quelle (`sourceName`) generiert, die mit einem SiteWise Edge-Gateway (`gatewayId`) verbunden ist. Einheit: 1 (1 steht dafür, dass die Modbus-Quelle angeschlossen ist und der Datenpunkt, der die Quelle repräsentiert, fehlt, ist getrennt.) GatewayIdAbmessungen:, SourceName
`ModbusTCPCollector.IncomingValuesCount`	Die Anzahl der Datenströme, die ein SiteWise Edge-Gateway (`gatewayId`) für eine Modbus-Quelle (`sourceName`) abonniert hat. Einheit: Anzahl Abmessungen:, GatewayId SourceName
`ModbusTCPCollector.ActiveDataStreamCount`	Die Anzahl der Datenpunkte, die ein SiteWise Edge-Gateway (`gatewayId`) für eine Modbus-Quelle (`sourceName`) empfangen hat. Einheit: Anzahl

Metrik	Beschreibung
	Abmessungen: GatewayId, SourceName

Protokollieren von AWS IoT SiteWise API-Aufrufen mit AWS CloudTrail

AWS IoT SiteWise ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines - AWS Services in AWS IoT SiteWise. CloudTrail captures API-Aufrufe für AWS IoT SiteWise als Ereignisse aufzeichnet. Zu den erfassten Aufrufen gehören Aufrufe von der AWS IoT SiteWise Konsole und Codeaufrufe der AWS IoT SiteWise API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für AWS IoT SiteWise. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an gestellte Anfrage AWS IoT SiteWise, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

AWS IoT SiteWise -Informationen in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn die unterstützte Ereignisaktivität in auftritt AWS IoT SiteWise, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für AWS IoT SiteWise, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit. Darüber hinaus können Sie andere - AWS Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen CloudTrail von Protokolldateien aus mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung von einem anderen AWS Service gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

AWS IoT SiteWise -Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. Lesen oder Schreiben in ein Amazon-S3-Objekt). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Standardmäßig protokolliert CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zu CloudTrail Preisen finden Sie unter -AWS CloudTrail Preise.

Sie können Datenereignisse für die AWS IoT SiteWise Ressourcentypen mithilfe der CloudTrail Konsole AWS CLIoder API CloudTrail -Operationen protokollieren. Die Tabelle in diesem Abschnitt zeigt die Ressourcentypen, die für verfügbar sind AWS IoT SiteWise.

- Um Datenereignisse mit der CloudTrail Konsole zu protokollieren, erstellen Sie einen Trail oder Ereignisdatenspeicher, um Datenereignisse zu protokollieren, oder aktualisieren Sie einen vorhandenen Trail oder Ereignisdatenspeicher, um Datenereignisse zu protokollieren.

  1. Wählen Sie Datenereignisse aus, um Datenereignisse zu protokollieren.

2. Wählen Sie in der Liste Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten.
3. Wählen Sie die Protokollauswahlvorlage aus, die Sie verwenden möchten. Sie können alle Datenereignisse für den Ressourcentyp protokollieren, alle `readOnly` Ereignisse protokollieren, alle `writeOnly` Ereignisse protokollieren oder eine benutzerdefinierte Protokollselektorvorlage erstellen, um nach den `resources.ARN` Feldern `readOnly`, `eventName`und zu filtern.

- Um Datenereignisse mit der zu protokollieren AWS CLI, konfigurieren Sie den `---advanced-event-selectors`Parameter so, dass das `-eventCategory`Feld auf `Data` und das `-resources.type`Feld auf den Ressourcentypwert gesetzt wird (siehe Tabelle). Sie können Bedingungen hinzufügen, um nach den Werten der `resources.ARN` Felder `readOnlyeventName`, und zu filtern.
  - Um einen Trail für die Protokollierung von Datenereignissen zu konfigurieren, führen Sie den AWS CloudTrail put-event-selectors Befehl aus. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen für Trails mit der AWS CLI.
  - Um einen Ereignisdatenspeicher für die Protokollierung von Datenereignissen zu konfigurieren, führen Sie den AWS CloudTrail create-event-data-store Befehl aus, um einen neuen Ereignisdatenspeicher für die Protokollierung von Datenereignissen zu erstellen, oder führen Sie den AWS CloudTrail update-event-data-store Befehl aus, um einen vorhandenen Ereignisdatenspeicher zu aktualisieren. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen für Ereignisdatenspeicher mit der AWS CLI.

In der folgenden Tabelle sind die AWS IoT SiteWise Ressourcentypen aufgeführt. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, den Sie aus der Liste Datenereignistyp in der CloudTrail Konsole auswählen können. Die Spalte resources.type value zeigt den `resources.type` Wert an, den Sie bei der Konfiguration erweiterter Ereignisselektoren mit der AWS CLI oder CloudTrail APIs angeben würden. Die Spalte Daten-APIs, die in protokolliert CloudTrail wurden, zeigt die API-Aufrufe an, die CloudTrail für den -Ressourcentyp protokolliert wurden.

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten-APIs, die bei CloudTrail* protokolliert wurden
AWS IoT SiteWise Komponente	`AWS::IoTSiteWise::Asset`	• BatchPutAssetPropertyValue • GetAssetPropertyValue

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten-APIs, die bei CloudTrail* protokolliert wurden
		• GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates
AWS IoT SiteWise Zeitreihen	`AWS::IoTSiteWise::TimeSeries`	• BatchPutAssetPropertyValue • GetAssetPropertyValue • GetAssetPropertyValueHistory • GetAssetPropertyAggregates • GetInterpolatedAssetPropertyValues • BatchGetAssetPropertyValue • BatchGetAssetPropertyValueHistory • BatchGetAssetPropertyAggregates

> **Note**
>
> Der im Cloudtrail-Ereignis protokollierte resources.type hängt von der ID ab, die in der API-Anforderung verwendet wird. Wenn eine Komponenten-ID in der Anforderung angegeben ist, wird der Asset resources.type protokolliert, andernfalls wird der TimeSeries resources.type protokolliert.

* Sie können erweiterte Ereignisselektoren konfigurieren`eventName`, um nach den `resources.ARN` Feldern `readOnly`, und zu filtern und nur die Ereignisse zu protokollieren, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector.

AWS IoT SiteWise -Verwaltungsereignisse in CloudTrail

Verwaltungsereignisse liefern Informationen zu Verwaltungsvorgängen, die für Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. Standardmäßig CloudTrail protokolliert Verwaltungsereignisse.

AWS IoT SiteWise protokolliert alle Operationen auf AWS IoT SiteWise Steuerebene als Verwaltungsereignisse. Eine Liste der Operationen auf AWS IoT SiteWise Steuerebene, die in AWS IoT SiteWise protokolliert CloudTrail, finden Sie in der APIAWS IoT SiteWise -Referenz zu .

Beispiel: AWS IoT SiteWise Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Operation, das Datum und die Uhrzeit der Operation, die Anforderungsparameter usw. CloudTrail Protokolldateien 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 -`CreateAsset`Operation demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
    "arn": "arn:aws:iam::123456789012:user/Administrator",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Administrator",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-03-11T17:26:40Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2020-03-11T18:01:22Z",
  "eventSource": "iotsitewise.amazonaws.com",
  "eventName": "CreateAsset",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "assetName": "Wind Turbine 1",
    "assetModelId": "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE",
    "clientToken": "a1b2c3d4-5678-90ab-cdef-00000EXAMPLE"
  },
  "responseElements": {
    "assetId": "a1b2c3d4-5678-90ab-cdef-22222EXAMPLE",
    "assetArn": "arn:aws:iotsitewise:us-east-1:123456789012:asset/a1b2c3d4-5678-90ab-
cdef-22222EXAMPLE",
    "assetStatus": {
      "state": "CREATING"
    }
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-aaaaaEXAMPLE",
  "eventID": "a1b2c3d4-5678-90ab-cdef-bbbbbEXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Verschlagworten Sie Ihre Ressourcen AWS IoT SiteWise

Das Taggen Ihrer AWS IoT SiteWise Ressourcen bietet eine leistungsstarke Möglichkeit, Unternehmensressourcen effizient zu kategorisieren, zu verwalten und abzurufen. Durch die Zuweisung von Tags, die aus Schlüssel-Wert-Paaren bestehen, können Sie Ihren Ressourcen beschreibende Metadaten hinzufügen. Die Metadaten aus Tags können zur Optimierung von Vorgängen verwendet werden. In einem Windpark-Szenario ermöglichen es Ihnen beispielsweise Tags, Turbinen mit bestimmten Attributen wie Standort, Kapazität und Betriebsstatus zu kennzeichnen, was eine schnelle Identifizierung und Verwaltung innerhalb AWS IoT SiteWise der Anlage ermöglicht.

Die Integration von Tags in AWS Identity and Access Management (IAM-) Richtlinien verbessert die Sicherheit und die Betriebskontrolle, indem Regeln für den bedingten Zugriff definiert werden. Das bedeutet, dass Sie angeben können, dass nur Benutzer mit bestimmten Tags angemeldet sind. Beispielsweise können nur Personen, die mit einer bestimmten Rolle oder Abteilung gekennzeichnet sind, auf bestimmte Ressourcen zugreifen oder diese ändern.

Verwenden von Tags in AWS IoT SiteWise

Verwenden Sie Tags, um Ihre AWS IoT SiteWise Ressourcen nach Zweck, Eigentümer, Umgebung oder einer anderen Klassifizierung für Ihren Anwendungsfall zu kategorisieren. Wenn es viele Ressourcen desselben Typs gibt, können Sie eine bestimmte Ressourcen schnell basierend auf ihren Tags identifizieren.

Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, den Sie angeben. Sie können beispielsweise eine Reihe von Tags für Ihre Anlagenmodelle einrichten, um sie entsprechend den industriellen Prozessen, die sie unterstützen, nachzuverfolgen. Es wird empfohlen, für jeden von Ihnen verwalteten Ressourcentyp einen maßgeschneiderten Satz von Tag-Schlüsseln zu entwickeln. Die Verwendung eines konsistenten Satzes von Tag-Schlüsseln kann die Verwaltung von Ressourcen erleichtern.

Taggen mit dem AWS Management Console

Der Tag-Editor im AWS Management Console bietet Ihnen eine zentrale, einheitliche Möglichkeit, Ihre Tags für Ressourcen aus allen AWS Diensten zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Tag-Editor im AWS Resource Groups -Benutzerhandbuch.

Tagging mit der API AWS IoT SiteWise

Die AWS IoT SiteWise API verwendet auch Tags. Beachten Sie vor dem Erstellen von Tags Beschränkungen für Tags. Weitere Informationen finden Sie unter Konventionen für Benennung und Nutzung von Tags in der Allgemeine AWS-Referenz.

- Wenn Sie bei der Erstellung einer Ressource Tags hinzufügen möchten, definieren Sie diese in der Eigenschaft `tags` der Ressource.
- Verwenden Sie den TagResourceVorgang, um einer vorhandenen Ressource Tags hinzuzufügen oder Tag-Werte zu aktualisieren.
- Verwenden Sie den UntagResourceVorgang, um Tags aus einer Ressource zu entfernen.
- Um die mit einer Ressource verknüpften Tags abzurufen, verwenden Sie die ListTagsForResourceOperation oder beschreiben Sie die Ressource und überprüfen Sie ihre `tags` Eigenschaften.

In der folgenden Tabelle sind Ressourcen aufgeführt, die Sie mithilfe der AWS IoT SiteWise API taggen können, sowie die entsprechenden `Create` `Describe` AND-Operationen.

Ressourcen, die markiert AWS IoT SiteWise werden können

Ressource	Operation erstellen	Operation beschreiben
Anlagenmodell oder Komponentenmodell	CreateAssetModel	DescribeAssetModel
Komponente	CreateAsset	DescribeAsset
SiteWise Edge-Gateway	CreateGateway	DescribeGateway
Portal	CreatePortal	DescribePortal
Projekt	CreateProject	DescribeProject
Dashboard	CreateDashboard	DescribeDashboard
Zugriffsrichtlinie	CreateAccessPolicy	DescribeAccessPolicy
Zeitreihen	BatchPutAssetPropertyValue	DescribeTimeSeries

Denn Sie können Ihre Datenquellen so konfigurieren`BatchPutAssetPropertyValue`, dass Industriedaten an AWS IoT SiteWise sie gesendet werden, bevor Sie Anlagenmodelle und Anlagen erstellen. AWS IoT SiteWise erstellt automatisch Datenströme, um Rohdatenströme von Ihren Geräten zu empfangen. Weitere Informationen finden Sie unter Verwaltung der Datenaufnahme.

Mit den folgenden Operationen können Sie Tags für Ressourcen anzeigen und verwalten, die die Markierung mit Tags unterstützen:

- TagResource— Fügt einer Ressource Tags hinzu oder aktualisiert den Wert eines vorhandenen Tags.
- ListTagsForResource— Listet die Tags für eine Ressource auf.
- UntagResource— Entfernt Tags aus einer Ressource.

Sie können jederzeit Tags zu einer Ressource hinzufügen oder daraus entfernen. Um den Wert eines vorhandenen Tag-Schlüssels zu aktualisieren, fügen Sie der Ressource ein neues Tag mit demselben Schlüssel und dem gewünschten neuen Wert hinzu. Diese Aktion ersetzt den alten Wert durch den neuen. Es ist zwar möglich, eine leere Zeichenfolge als Tag-Wert zuzuweisen, aber Sie können keinen Nullwert zuweisen.

Durch das Löschen einer Ressource werden auch alle damit verknüpften Tags entfernt.

Verwenden von Tags mit IAM-Richtlinien

Verwenden Sie Ressourcen-Tags in Ihren IAM-Richtlinien, um den Benutzerzugriff und die Benutzerberechtigungen zu kontrollieren. Richtlinien können es Benutzern beispielsweise ermöglichen, nur Ressourcen zu erstellen, denen ein bestimmtes Tag angehängt ist. Richtlinien können auch verhindern, dass Benutzer Ressourcen mit bestimmten Tags erstellen oder ändern.

> **Note**
>
> Wenn Sie Tags verwenden, um den Zugriff von Benutzern auf Ressourcen zuzulassen oder abzulehnen, sollten Sie Benutzern nicht die Möglichkeit geben, diese Tags diesen Ressourcen hinzuzufügen oder aus diesen Ressourcen zu entfernen. Andernfalls könnte ein Benutzer Ihre Einschränkungen umgehen und Zugriff auf eine Ressource erhalten, indem er deren Tags ändert.

Sie können im Element `Condition` (auch als `Condition`-Block bezeichnet) einer Richtlinienanweisung die folgenden Bedingungskontextschlüssel und -werte verwenden.

`aws:ResourceTag/tag-key: tag-value`

Sie können mithilfe bestimmter Tags Aktionen für Ressourcen zulassen oder ablehnen.

`aws:RequestTag/tag-key: tag-value`

Erfordert, dass beim Erstellen oder Ändern einer markierbaren Ressource ein bestimmtes Tag verwendet (oder nicht verwendet) wird.

`aws:TagKeys: [tag-key, ...]`

Erfordert, dass beim Erstellen oder Ändern einer markierbaren Ressource ein bestimmter Satz von Tag-Schlüsseln verwendet (oder nicht verwendet) wird.

> **Note**
>
> Die Bedingungskontextschlüssel und -werte in einer IAM-Richtlinie gelten nur für Aktionen, für die eine Ressource mit Tags als erforderlichem Parameter angegeben werden kann. Sie können beispielsweise den tagbasierten bedingten Zugriff für einrichten. ListAssets Sie können den tagbasierten bedingten Zugriff nicht aktivieren, PutLoggingOptionsda in der Anfrage auf keine markierbare Ressource verwiesen wird.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Ressourcen-Tags und IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Beispiel für IAM-Richtlinien mithilfe von Tags

- Anzeigen von AWS IoT SiteWise -Komponenten basierend auf Tags

Problembehebung AWS IoT SiteWise

Verwenden Sie die Informationen in diesen Abschnitten, um Probleme mit zu beheben und zu lösen AWS IoT SiteWise.

Themen

Fehlerbehebung bei Massenimport- und Exportvorgängen

Informationen zum Behandeln und Diagnostizieren von Fehlern, die während eines Übertragungsauftrags erzeugt wurden, finden Sie in der AWS IoT TwinMaker GetMetadataTransferJob -API:

1. Nachdem Sie einen Übertragungsauftrag erstellt und ausgeführt haben, rufen Sie die GetMetadataTransferJob-API auf:

   ```
   aws iottwinmaker get-metadata-transfer-job \
   --metadata-transfer-job-id your_metadata_transfer_job_id \
   --region us-east-1
   ```

2. Der Status des Auftrags ändert sich in einen der folgenden Zustände:

   - COMPLETED
   - CANCELLED
   - ERROR

3. Die GetMetadataTransferJob API gibt ein - MetadataTransferJobProgressObjekt zurück.
4. Das -MetadataTransferJobProgressObjekt enthält die folgenden Parameter:

   - failedCount : Gibt die Anzahl der Komponenten an, die während des Übertragungsprozesses fehlgeschlagen sind.

- skippedCount : Gibt die Anzahl der Komponenten an, die während des Übertragungsprozesses übersprungen wurden.
- succeededCount : Gibt die Anzahl der Komponenten an, die während des Übertragungsprozesses erfolgreich waren.
- totalCount: Gibt die Gesamtzahl der am Übertragungsprozess beteiligten Komponenten an.

5. Darüber hinaus wird ein reportUrl-Element vom API-Aufruf zurückgegeben, der eine vorsignierte URL enthält. Wenn Ihr Übertragungsauftrag Fehler enthält, die untersucht werden müssen, können Sie einen vollständigen Fehlerbericht unter dieser URL herunterladen.

Fehlerbehebung bei einem - AWS IoT SiteWise Portal

Beheben Sie häufige Probleme mit Ihren AWS IoT SiteWise Portalen.

Benutzer und Administratoren können nicht auf das Portal zugreifen AWS IoT SiteWise

Wenn Benutzer oder Administratoren nicht auf Ihr AWS IoT SiteWise Portal zugreifen können, verfügen Sie möglicherweise über eingeschränkte Berechtigungen in angehängten AWS Identity and Access Management (IAM)-Richtlinien, die erfolgreiche Anmeldungen verhindern.

Sehen Sie sich die folgenden Beispiele für IAM-Richtlinien an, die zu einem Anmeldefehler führen:

> **Note**
>
> Alle angehängten IAM-Richtlinien, die ein -`"Condition"`Element enthalten, führen zu einem Anmeldefehler.

Beispiel 1: Die Bedingung hier ist eine begrenzte IP, was zu einem Anmeldefehler führt.

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

```
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "REPLACESAMPLEIP"
                    ]
                }
            }
        }
    ]
}
```

Beispiel 2: Die Bedingung hier ist ein enthaltenes Tag, was zu einem Anmeldefehler führt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iotsitewise:DescribePortal"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/project": "*"
                }
            }
        }
    ]
}
```

Vermeiden Sie beim Hinzufügen von Benutzern oder Administratoren zum Portal das Erstellen von IAM-Richtlinien, die Benutzerberechtigungen einschränken, z. B. eingeschränkte IP-Adressen. Alle angehängten Richtlinien mit eingeschränkten Berechtigungen können keine Verbindung zum AWS IoT SiteWise Portal herstellen.

Fehlerbehebung bei einem SiteWise Edge-Gateway

AWS IoT SiteWise Edge-Gateways führen eine Reihe von Komponenten aus. AWS IoT Greengrass Sie können Ihr SiteWise Edge-Gateway so konfigurieren, dass Ereignisse bei Amazon CloudWatch

und im lokalen Dateisystem Ihres SiteWise Edge-Gateways protokolliert werden. Anschließend können Sie die Protokolldateien einsehen, um Probleme mit Ihrem SiteWise Edge-Gateway zu beheben.

Sie können auch CloudWatch Metriken einsehen, die von Ihren SiteWise Edge-Gateways gemeldet wurden, um Probleme mit Konnektivität oder Datenströmen zu beheben. Weitere Informationen finden Sie unter Überwachung AWS IoT SiteWise mit CloudWatch Amazon-Metriken.

Themen

Konfiguration und Zugriff auf SiteWise Edge-Gateway-Protokolle

Bevor Sie SiteWise Edge-Gateway-Protokolle anzeigen können, müssen Sie Ihr SiteWise Edge-Gateway so konfigurieren, dass es CloudWatch Protokolle an Amazon Logs sendet oder Protokolle im lokalen Dateisystem speichert.

- Verwenden Sie CloudWatch Logs, wenn Sie das verwenden möchten AWS Management Console , um die Protokolldateien Ihres SiteWise Edge-Gateways einzusehen. Weitere Informationen finden Sie unter Amazon CloudWatch Logs verwenden.
- Verwenden Sie lokale Dateisystemprotokolle, wenn Sie die Befehlszeile oder lokale Software verwenden möchten, um die Protokolldateien Ihres SiteWise Edge-Gateways anzuzeigen. Weitere Informationen finden Sie unter Verwenden von Serviceprotokollen.

Behebung von Problemen mit dem SiteWise Edge-Gateway

Verwenden Sie die folgenden Informationen, um Probleme mit dem SiteWise Edge-Gateway zu beheben.

Problembereiche

- „Hauptklasse konnte nicht gefunden oder geladen werden“ wird in aws.iot angezeigt. SiteWiseEdgePublisher protokolliert beim Fehler /greengrass/v2/logs

Pakete können nicht für SiteWise Edge-Gateways bereitgestellt werden

Wenn die AWS IoT Greengrass Nucleus-Komponente (`aws.greengrass.Nucleus`) veraltet ist, können Sie möglicherweise keine Packs auf Ihrem SiteWise Edge-Gateway bereitstellen. Sie können die AWS IoT Greengrass V2 Konsole verwenden, um die AWS IoT Greengrass Nucleus-Komponente zu aktualisieren.

Aktualisieren Sie die AWS IoT Greengrass Nucleus-Komponente (Konsole)

1. Navigieren Sie zur AWS IoT Greengrass -Konsole.
2. Wählen Sie im Navigationsbereich unter AWS IoT GreengrassDeployments aus.
3. Wählen Sie in der Liste Bereitstellungen die Bereitstellung aus, die Sie überarbeiten möchten.
4. Wählen Sie Überarbeiten aus.
5. Wählen Sie auf der Seite „Ziel angeben“ die Option Weiter.
6. Geben Sie auf der Seite Komponenten auswählen unter Öffentliche Komponenten in das Suchfeld **`aws.greengrass.Nucleus`** AWS.Greengrass.Nucleus ein und wählen Sie dann aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie auf der Seite Komponenten konfigurieren die Option Weiter aus.
9. Wählen Sie auf der Seite Erweiterte Einstellungen konfigurieren die Option Weiter aus.
10. Wählen Sie auf der Seite Review (Prüfen) die Option Deploy (Bereitstellen) aus.

AWS IoT SiteWise empfängt keine Daten von OPC-UA-Servern

Wenn Ihre Geräte AWS IoT SiteWise keine von Ihren OPC-UA-Servern gesendeten Daten empfangen, können Sie die Protokolle Ihres SiteWise Edge-Gateways durchsuchen, um Probleme zu beheben. Suchen Sie nach `swPublisher` Protokollen auf Informationsebene, die die folgende Meldung enthalten.

```
Emitting diagnostic name=PublishError.SomeException
```

Verwenden Sie je nach Typ *`SomeException`*im Protokoll die folgenden Ausnahmetypen und die entsprechenden Probleme, um Ihr SiteWise Edge-Gateway zu beheben:

- ResourceNotFoundException— Ihre OPC-UA-Server senden Daten, die keinem Eigenschaftsalias für ein Asset entsprechen. Diese Ausnahme kann in zwei Fällen auftreten:
  - Ihre Eigenschaftsaliase stimmen nicht genau mit Ihren OPC-UA-Variablen überein, einschließlich aller von Ihnen definierten Quellpräfixe. Überprüfen Sie, ob Ihre Eigenschaftenaliase und Quellpräfixe korrekt sind.
  - Sie haben Ihre OPC-UA-Variablen keinen Asset-Eigenschaften zugeordnet. Weitere Informationen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.

    Wenn Sie bereits alle OPC-UA-Variablen zugeordnet haben, die Sie verwenden möchten, können Sie filtern AWS IoT SiteWise, welche OPC-UA-Variablen das Edge-Gateway sendet. SiteWise Weitere Informationen finden Sie unter Verwenden von OPC-UA-Knotenfiltern.
- InvalidRequestException— Die Datentypen Ihrer OPC-UA-Variablen stimmen nicht mit den Datentypen Ihrer Anlageneigenschaft überein. Wenn beispielsweise eine OPC-UA-Variable den Datentyp „Integer“ aufweist, muss der Datentyp der entsprechenden Komponenteneigenschaft „Integer“ lauten. Eine Objekteigenschaft mit doppeltem Typ kann keine OPC-UA-Ganzzahlwerte empfangen. Um dieses Problem zu beheben, definieren Sie neue Eigenschaften mit den richtigen Datentypen.
- TimestampOutOfRangeException— Ihr SiteWise Edge-Gateway sendet Daten, die außerhalb des zulässigen Bereichs liegen. AWS IoT SiteWise AWS IoT SiteWise lehnt alle Datenpunkte ab, deren Zeitstempel vor 7 Tagen in der Vergangenheit oder weniger als 5 Minuten in der future liegen. Wenn Ihr SiteWise Edge-Gateway die Stromversorgung oder die Verbindung zur AWS Cloud verloren hat, müssen Sie möglicherweise den Cache Ihres SiteWise Edge-Gateways leeren.
- ThrottlingExceptionoder LimitExceededException— Ihre Anfrage hat ein AWS IoT SiteWise Servicekontingent überschritten, z. B. die Rate der aufgenommenen Datenpunkte oder die Anforderungsrate für API-Operationen mit Objektdaten. Überprüfen Sie, dass Ihre Konfiguration AWS IoT SiteWise Kontingente nicht überschreitet.

Im Dashboard wurden keine Daten angezeigt

Wenn in Ihrem Dashboard keine Daten angezeigt werden, sind die Publisher-Konfiguration und die Datenquelle des SiteWise Edge-Gateways möglicherweise nicht synchron. Wenn sie nicht synchron sind, kann die Aktualisierung des Namens der Datenquelle die Synchronisierung von der Cloud zum Edge beschleunigen und so den Fehler „Nicht synchron“ beheben.

Um den Namen einer Datenquelle zu aktualisieren

1. Navigieren Sie zur AWS IoT SiteWise -Konsole.
2. Wählen Sie im Navigationsbereich Edge-Gateways aus.
3. Wählen Sie das SiteWise Edge-Gateway aus, das mit dem Dashboard verbunden ist.
4. Wählen Sie unter Datenquellen die Option Bearbeiten aus.
5. Wählen Sie einen neuen Quellennamen und klicken Sie auf Speichern, um Ihre Änderung zu bestätigen.
6. Überprüfen Sie Ihre Änderungen, indem Sie in der Tabelle Datenquellen überprüfen, ob der Datenquellenname aktualisiert wurde.

„Hauptklasse konnte nicht gefunden oder geladen werden“ wird in aws.iot angezeigt. SiteWiseEdgePublisher protokolliert beim Fehler /greengrass/v2/logs

Wenn Sie diesen Fehler sehen, müssen Sie möglicherweise die Java-Version Ihres Edge-Gateways aktualisieren. SiteWise

- Führen Sie von einem Terminal folgenden Befehl aus:

```
java -version
```

  Die Version von Java, mit der Ihr SiteWise Edge-Gateway ausgeführt wird, wird unter angezeigt`OpenJDK Runtime Environment`. Sie werden eine Antwort wie die folgende sehen:

```
openjdk version "11.0.20" 2023-07-18 LTS
OpenJDK Runtime Environment Corretto011.0.20.8.1 (build 11.0.20+8-LTS
OpenJDK 64-Bit Server VM Corretto-11.0.20.8.1 (build 11.0.20+8-LTS, mixed node)
```

Wenn Sie die Java-Version 11.0.20.8.1 ausführen, müssen Sie das IoT SiteWise Publisher-Paket auf Version 2.4.1 oder neuer aktualisieren. Nur die Java-Version 11.0.20.8.1 ist betroffen. Umgebungen mit anderen Java-Versionen können weiterhin ältere Versionen der IoT SiteWise Publisher-Komponente verwenden. Weitere Informationen zum Aktualisieren eines Komponentenpakets finden Sie unter. Ändern der Version von SiteWise Edge-Gateway-Komponentenpaketen

Behebung von AWS IoT Greengrass Problemen

Lösungen für viele Probleme bei der Konfiguration oder Bereitstellung Ihres SiteWise Edge-Gateways finden Sie AWS IoT Greengrass im AWS IoT Greengrass Entwicklerhandbuch unter Problembehandlung. AWS IoT Greengrass

Problembehandlung und AWS IoT SiteWise Regelaktion

Um Probleme mit Ihrer AWS IoT SiteWise Regelaktion in zu beheben AWS IoT Core, können Sie eines der folgenden Verfahren ausführen:

- Amazon CloudWatch Logs konfigurieren
- Konfigurieren einer Fehler-Aktion für die erneute Veröffentlichung für Ihre Regel

Vergleichen Sie anschließend die Fehlermeldungen mit den Fehlern in diesem Thema, um Ihr Problem zu beheben.

Themen

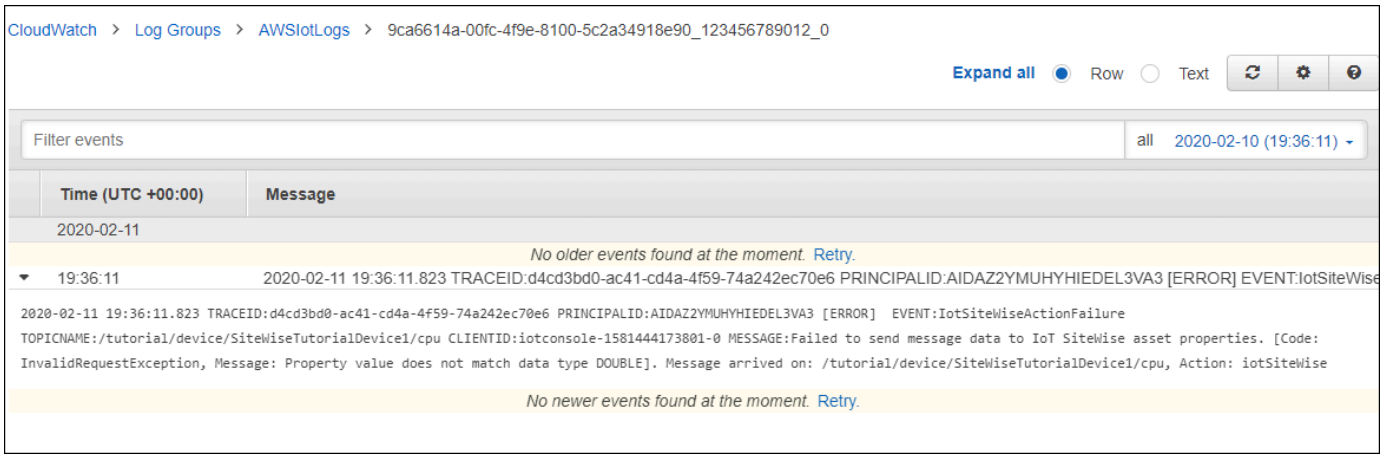
AWS IoT Core Protokolle konfigurieren

Sie können so konfigurieren AWS IoT , dass verschiedene Informationsebenen in CloudWatch Logs protokolliert werden.

Um CloudWatch Protokolle zu konfigurieren und darauf zuzugreifen

1. Informationen zur Konfiguration der Protokollierung finden Sie unter Monitoring with CloudWatch Logs im AWS IoT Developer Guide. AWS IoT Core
2. Navigieren Sie zur CloudWatch -Konsole.
3. Wählen Sie im Navigationsbereich Protokollgruppen aus.
4. Wählen Sie die AWSIotLogsGruppe aus.

5. Wählen Sie einen aktuellen Protokolldatenstrom aus. CloudWatch Zeigt standardmäßig den neuesten Log-Stream zuerst an.
6. Wählen Sie einen Protokolleintrag, um die Protokollmeldung zu erweitern. Ihr Protokolleintrag könnte wie der folgende Screenshot aussehen.



7. Vergleichen Sie die Fehlermeldungen mit den Fehlern in diesem Thema, um Ihr Problem zu beheben.

Konfigurieren einer Aktion für die erneute Veröffentlichung eines Fehlers

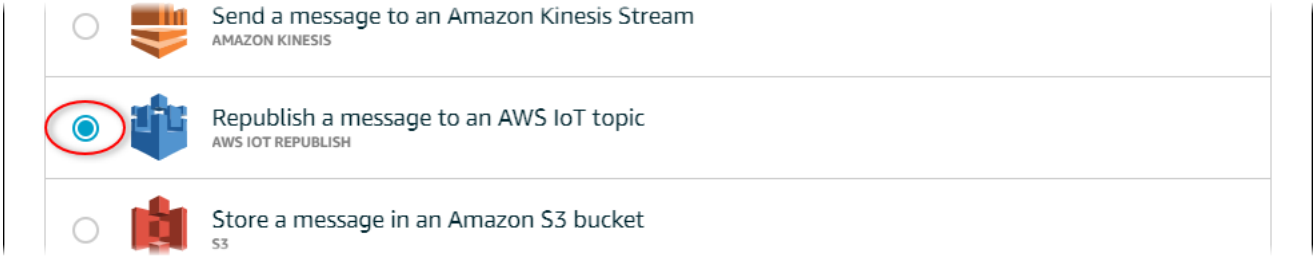
Sie können eine Fehleraktion für Ihre Regel konfigurieren, um Fehlermeldungen zu verarbeiten. In diesem Verfahren konfigurieren Sie die Aktion zur Wiederveröffentlichung der Regel, um Fehlermeldungen im MQTT-Testclient anzuzeigen.

> **Note**
>
> Die Aktion zum erneuten Veröffentlichen eines Fehlers gibt nur das Äquivalent der `ERROR`-Ebenenprotokolle aus. Wenn Sie ausführlichere Protokolle wünschen, müssen Sie CloudWatch Logs konfigurieren.

So fügen Sie einer Regel eine Aktion zur Wiederveröffentlichung eines Fehlers hinzu

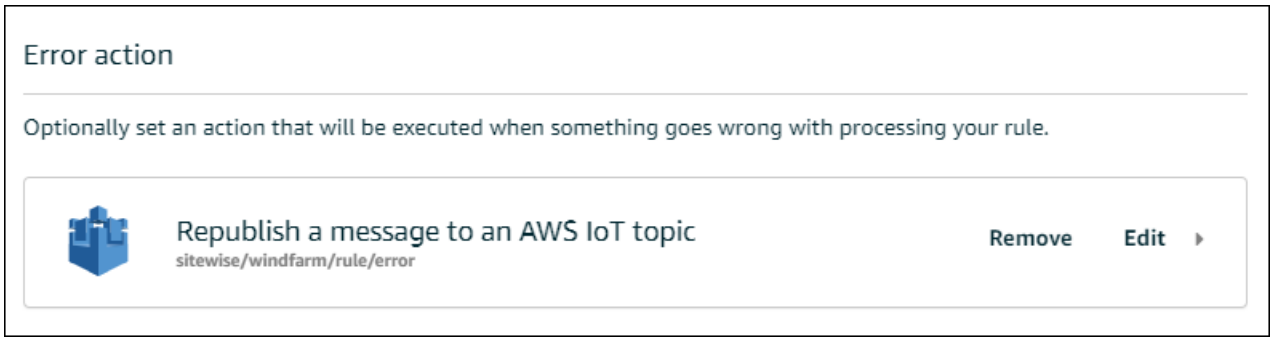
1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Act (Agieren) und dann Rules (Regeln) aus.
3. Wählen Sie Ihre Regel aus.
4. Wählen Sie unter Error action (Fehleraktion) die Option Add action (Aktion hinzufügen)aus.

5. Wählen Sie Nachricht zu einem Thema erneut veröffentlichen aus. AWS IoT



6. Klicken Sie unten auf der Seite auf Configure action (Aktion konfigurieren).
7. Geben Sie im Feld Thema ein eindeutiges Thema ein (z. B.**`sitewise/windfarm/rule/error`**). AWS IoT Core veröffentlicht die Fehlermeldungen zu diesem Thema erneut.
8. Wählen Sie „Auswählen“, um AWS IoT Core Zugriff für die Ausführung der Fehleraktion zu gewähren.
9. Wählen Sie neben der Rolle, die Sie für die Regel erstellt haben, Select (Auswählen).
10. Wählen Sie Update Role (Rolle aktualisieren) aus, um der Rolle die zusätzlichen Berechtigungen hinzuzufügen.
11. Wählen Sie Aktion hinzufügen aus.

    Die Fehleraktion Ihrer Regel sollte dem folgenden Screenshot ähnlich aussehen.



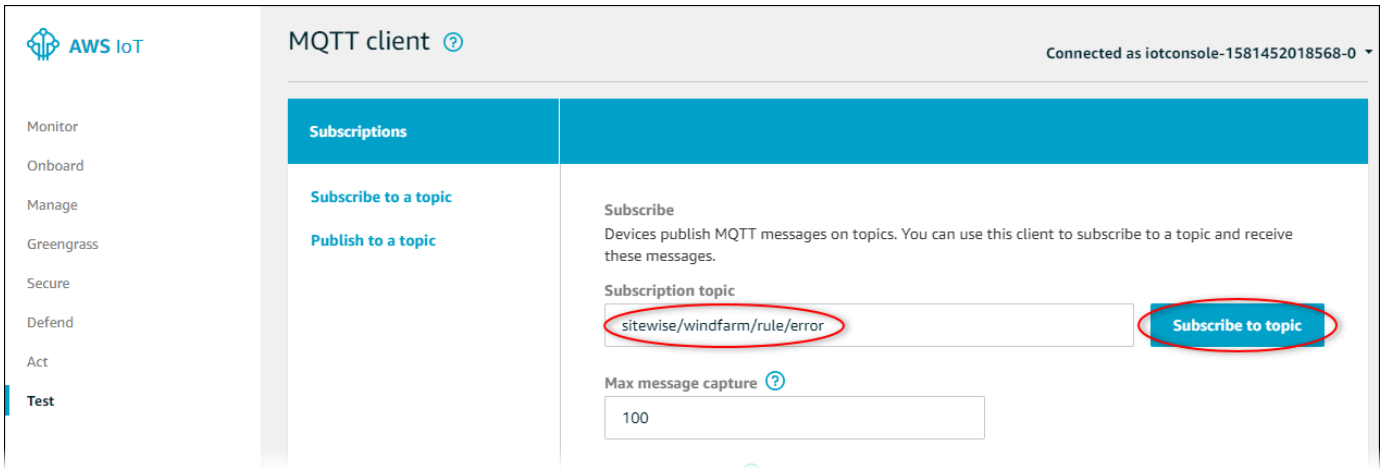
12. Klicken Sie oben links auf der Konsole auf den Zurück-Pfeil, um zur Startseite der AWS IoT Konsole zurückzukehren.

Nachdem Sie die Aktion „Republish error (Fehler wiederveröffentlichen)“ eingerichtet haben, können Sie die Fehlermeldungen in AWS IoT Core im MQTT-Testclient anzeigen.

Im folgenden Verfahren abonnieren Sie das Fehlerthema im MQTT-Testclient. Im MQTT-Testclient können Sie die Fehlermeldungen Ihrer Regel erhalten, um das Problem zu beheben.

So abonnieren Sie das Fehleraktionsthema.

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie auf der linken Navigationsseite Test, um den MQTT-Testclient zu öffnen.
3. Geben Sie im Feld Subscription topic (Abonnementsthema) das zuvor konfigurierte Fehlerthema ein (z. B. **`sitewise/windfarm/rule/error`**), und wählen Sie Subscribe to topic (Thema abonnieren).



4. Achten Sie auf die angezeigten Fehlermeldungen, und erweitern Sie dann das `failures`-Array in einer beliebigen Fehlermeldung.

   Vergleichen Sie anschließend die Fehlermeldungen mit den Fehlern in diesem Thema, um Ihr Problem zu beheben.

Beheben von -Problemen

Verwenden Sie die folgenden Informationen, um Regelprobleme zu beheben.

Problembereiche

- Fehler: Das Mitglied muss innerhalb von 604.800 Sekunden vor und 300 Sekunden nach dem aktuellen Zeitstempel sein
- Fehler: Eigenschaftswert stimmt nicht mit dem Datentyp <type> überein
- Fehler: Benutzer: <role-arn>ist nicht berechtigt, Folgendes auszuführen: iotsitewise: on resource BatchPutAssetPropertyValue
- Fehler: iot.amazonaws.com kann Folgendes nicht ausführen: sts: auf der Ressource: AssumeRole <role-arn>

- Info: Es wurden keine Anforderungen gesendet. PutAssetPropertyValueEntries war nach der Ausführung von Ersatzvorlagen leer.

Fehler: Das Mitglied muss innerhalb von 604.800 Sekunden vor und 300 Sekunden nach dem aktuellen Zeitstempel sein

Ihr Zeitstempel ist älter als 7 Tage oder neuer als 5 Minuten, verglichen mit der aktuellen Unix-Epoche. Gehen Sie wie folgt vor:

- Überprüfen Sie, ob Ihr Zeitstempel in Unix-Epoche (UTC) Zeit angegeben wird. Wenn Sie einen Zeitstempel mit einer anderen Zeitzone angeben, erhalten Sie diesen Fehler.
- Vergewissern Sie sich, dass Ihr Zeitstempel in Sekunden angegeben ist. AWS IoT SiteWise erwartet, dass Zeitstempel in Zeit in Sekunden (in der Unix-Epochenzeit) und Offset in Nanosekunden aufgeteilt sind.
- Vergewissern Sie sich, dass Sie Daten hochladen, die nicht später als 7 Tage in der Vergangenheit mit einem Zeitstempel versehen sind.

Fehler: Eigenschaftswert stimmt nicht mit dem Datentyp <type> überein

Ein Eintrag in der Regelaktion hat einen anderen Datentyp als die Zielkomponenteneigenschaft. Beispielsweise ist Ihre Zielkomponenteneigenschaft `DOUBLE` und Ihr ausgewählter Datentyp ist Integer (Ganzzahl) oder Sie haben den Wert `integerValue` übergeben. Gehen Sie wie folgt vor:

- Wenn Sie die Regel von der AWS IoT Konsole aus konfigurieren, überprüfen Sie, ob Sie für jeden Eintrag den richtigen Datentyp ausgewählt haben.
- Wenn Sie die Regel über die API oder AWS Command Line Interface (AWS CLI) konfigurieren, überprüfen Sie, ob Ihr `value` Objekt das richtige Typfeld verwendet (z. B. `doubleValue` für eine `DOUBLE` Eigenschaft).

Fehler: Benutzer: <role-arn>ist nicht berechtigt, Folgendes auszuführen: iotsitewise: on resource BatchPutAssetPropertyValue

Ihre Regel ist nicht berechtigt, auf die Zielkomponenteneigenschaft zuzugreifen, oder die Zielkomponenteneigenschaft ist nicht vorhanden. Gehen Sie wie folgt vor:

- Überprüfen Sie, ob Ihr Eigenschaftenalias korrekt ist, und ob Sie eine Komponenteneigenschaft mit dem angegebenen Eigenschaftenalias haben. Weitere Informationen finden Sie unter Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften.
- Überprüfen Sie, ob Ihre Regel über eine Rolle verfügt, und ob die Rolle die `iotsitewise:BatchPutAssetPropertyValue`-Berechtigung für die Zielkomponenteneigenschaft zulässt, z. B. über die Hierarchie der Zielkomponente. Weitere Informationen finden Sie unter Gewährung AWS IoT des erforderlichen Zugriffs.

Fehler: iot.amazonaws.com kann Folgendes nicht ausführen: sts: auf der Ressource: AssumeRole <role-arn>

Ihr Benutzer ist nicht berechtigt, die Rolle in Ihrer Regel in (IAM) zu übernehmen. AWS Identity and Access Management

Vergewissern Sie sich, dass Ihr Benutzer `iam:PassRole` Zugriff auf die Rolle in Ihrer Regel hat. Weitere Informationen finden Sie im AWS IoT Entwicklerhandbuch unter Rollenberechtigungen weitergeben.

Info: Es wurden keine Anforderungen gesendet. PutAssetPropertyValueEntries war nach der Ausführung von Ersatzvorlagen leer.

> **Note**
>
> Diese Nachricht ist ein `INFO`-Ebenenprotokoll.

Ihre Anforderung muss mindestens einen Eintrag mit allen erforderlichen Parametern aufweisen.

Überprüfen Sie, ob die Parameter Ihrer Regel, einschließlich der Substitutionsvorlagen, zu nicht-leeren Werten führen. Substitutionsvorlagen können nicht auf Werte zugreifen, die in `AS`-Klauseln in Ihrer Regelabfrageanweisung definiert sind. Weitere Informationen finden Sie unter Substitutionsvorlagen im AWS IoT Entwicklerhandbuch.

Fehlerbehebung bei einer Regel

Folgen Sie den Schritten in diesem Verfahren, um Fehler in Ihrer Regel zu beheben, falls die Daten zur CPU- und Speichernutzung nicht AWS IoT SiteWise wie erwartet angezeigt werden. In diesem

Verfahren konfigurieren Sie die Aktion zur Wiederveröffentlichung der Regel, um Fehlermeldungen im MQTT-Testclient anzuzeigen. Zur Fehlerbehebung können Sie auch die CloudWatch Protokollierung in Logs konfigurieren. Weitere Informationen finden Sie unter Problembehandlung und AWS IoT SiteWise Regelaktion.

So fügen Sie einer Regel eine Aktion zur Wiederveröffentlichung eines Fehlers hinzu

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Nachrichtenweiterleitung und dann Regeln aus.
3. Wählen Sie die Regel aus, die Sie zuvor erstellt haben, und klicken Sie auf Bearbeiten.
4. Wählen Sie unter Fehleraktion — optional die Option Fehleraktion hinzufügen aus.
5. Wählen Sie Eine Nachricht zu einem AWS IoT Thema erneut veröffentlichen aus.
6. Geben Sie im Feld Thema den Pfad zu Ihrem Fehler ein (z. B.**`sitewise/rule/tutorial/error`**). AWS IoT Core veröffentlicht die Fehlermeldungen zu diesem Thema erneut.
7. Wählen Sie die Rolle aus, die Sie zuvor erstellt haben (z. B. SiteWiseTutorialDeviceRuleRole).
8. Wählen Sie Aktualisieren.

Nachdem Sie die Aktion „Republish error (Fehler wiederveröffentlichen)“ eingerichtet haben, können Sie die Fehlermeldungen in AWS IoT Core im MQTT-Testclient anzeigen.

Im folgenden Verfahren abonnieren Sie das Fehlerthema im MQTT-Testclient.

So abonnieren Sie das Fehleraktionsthema.

1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie auf der linken Navigationsseite MQTT-Testclient aus, um den MQTT-Testclient zu öffnen.
3. Geben Sie im Feld Themenfilter den Text Abonnieren ein **`sitewise/rule/tutorial/error`** und wählen Sie Abonnieren.

Wenn Fehlermeldungen angezeigt werden, zeigen Sie das `failures`-Array in einer beliebigen Fehlermeldung an, um Probleme zu diagnostizieren. Weitere Informationen zu möglichen Problemen und deren Behebung finden Sie unter Problembehandlung und AWS IoT SiteWise Regelaktion.

Wenn keine Fehler angezeigt werden, überprüfen Sie, ob Ihre Regel aktiviert ist und ob Sie das in der Aktion „Fehler wiederveröffentlichen“ konfigurierte Thema abonniert haben. Wenn nach dem

Vorgehen weiterhin keine Fehler auftreten, überprüfen Sie, ob das Geräteskript ausgeführt wird und den Schatten des Geräts erfolgreich aktualisiert.

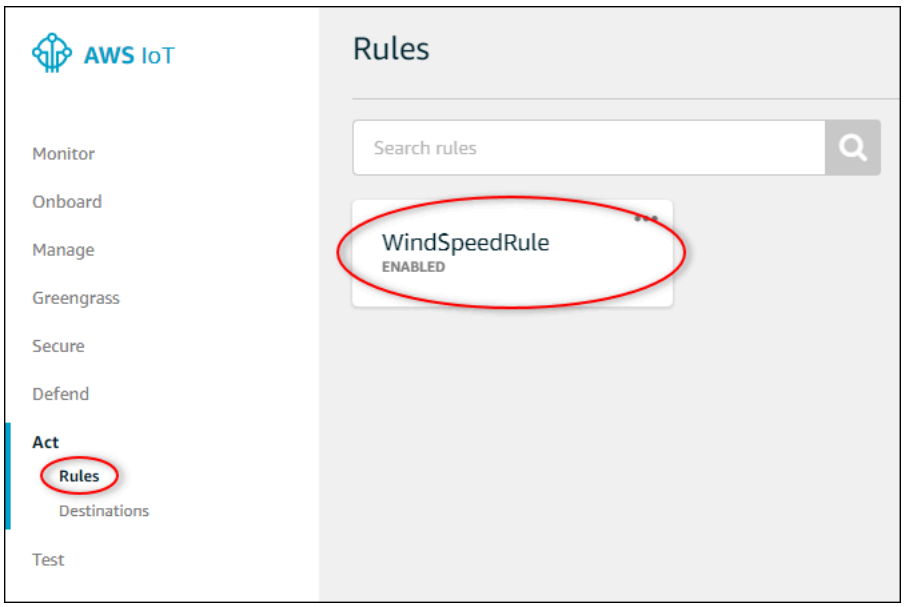
> **Note**
>
> Sie können auch das Shadow-Update-Thema Ihres Geräts abonnieren, um die Payload zu sehen, die Ihre AWS IoT SiteWise Aktion analysiert. Abonnieren Sie dazu das folgende Thema.
>
> ```
> $aws/things/+/shadow/update/accepted
> ```

Fehlerbehebung bei einer Regel

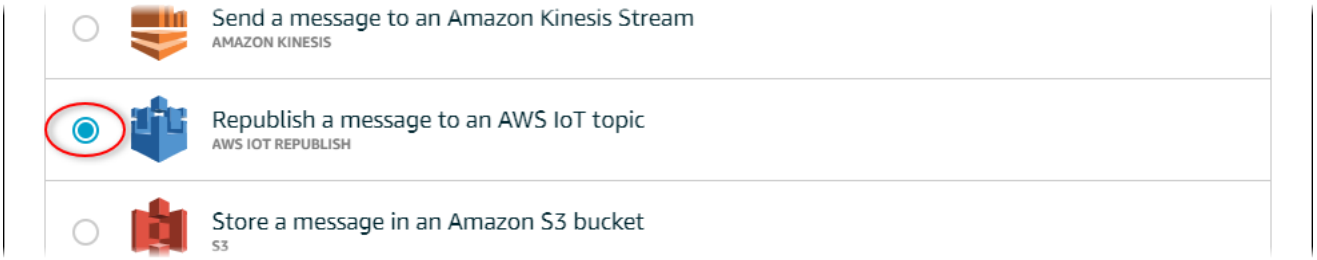
Folgen Sie den Schritten in diesem Verfahren, um Fehler in Ihrer Regel zu beheben, falls die Demo-Asset-Daten nicht wie erwartet in der DynamoDB-Tabelle angezeigt werden. In diesem Verfahren konfigurieren Sie die Aktion zur Wiederveröffentlichung der Regel, um Fehlermeldungen im MQTT-Testclient anzuzeigen. Zur Fehlerbehebung können Sie auch die Protokollierung in CloudWatch Logs konfigurieren. Weitere Informationen finden Sie unter Überwachung mit CloudWatch Protokollen im AWS IoT Entwicklerhandbuch.

So fügen Sie einer Regel eine Aktion zur Wiederveröffentlichung eines Fehlers hinzu

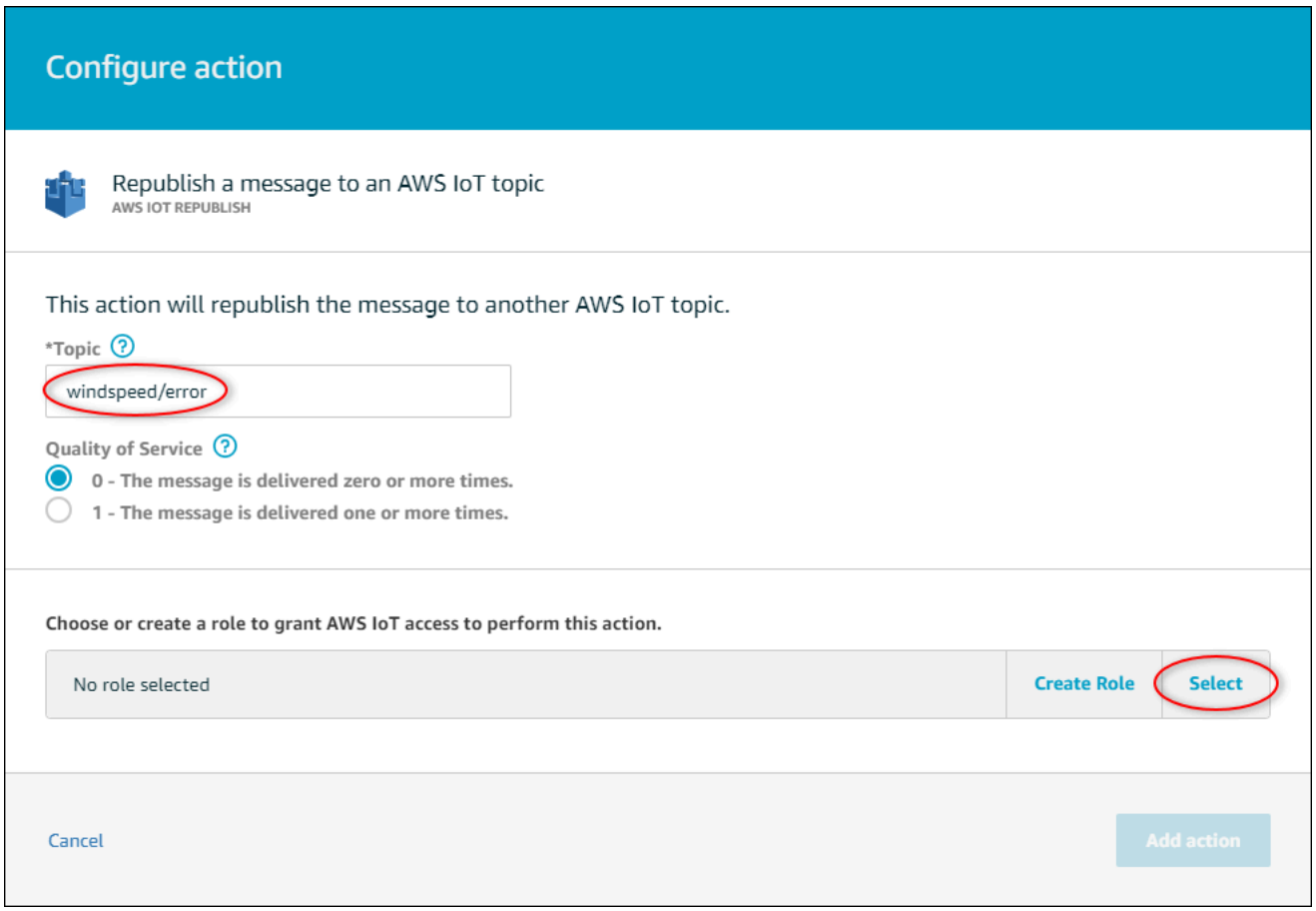
1. Navigieren Sie zur AWS IoT -Konsole.
2. Wählen Sie im linken Navigationsbereich Act (Agieren) und dann Rules (Regeln) aus.
3. Wählen Sie die Regel aus, die Sie zuvor erstellt haben.



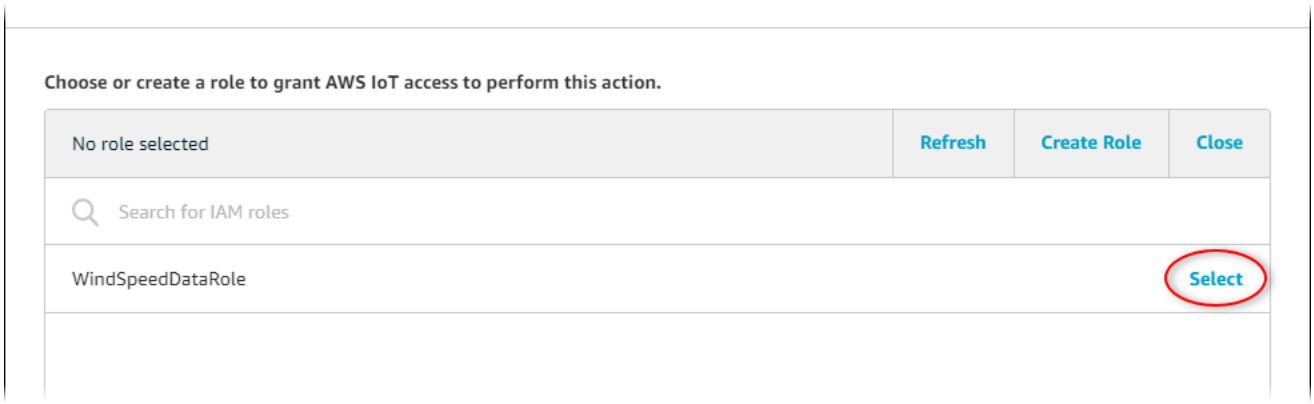
4. Wählen Sie unter Error action (Fehleraktion) die Option Add action (Aktion hinzufügen)aus.
5. Wähle „Nachricht zu einem AWS IoT Thema erneut veröffentlichen“.



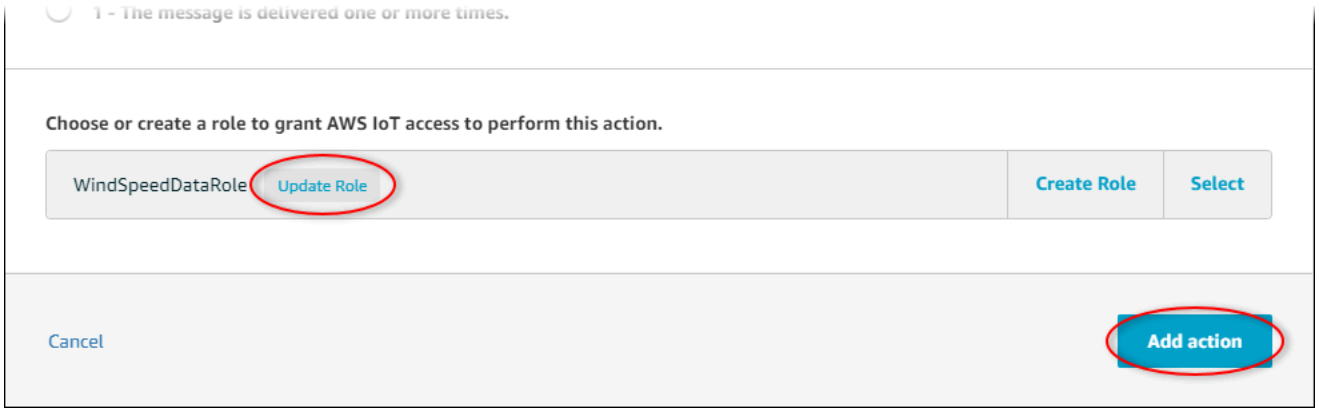
6. Klicken Sie unten auf der Seite auf Configure action (Aktion konfigurieren).
7. Geben Sie im Feld Thema **`windspeed/error`** ein. AWS IoT Core wird die Fehlermeldungen zu diesem Thema erneut veröffentlichen.



8. Wählen Sie „Auswählen“, um AWS IoT Core Zugriff auf die Ausführung der Fehleraktion mithilfe der zuvor erstellten Rolle zu gewähren.
9. Wählen Sie Select (Auswählen) neben Ihrer Rolle aus.



10. Wählen Sie Update Role (Rolle aktualisieren) aus, um der Rolle die zusätzlichen Berechtigungen hinzuzufügen.



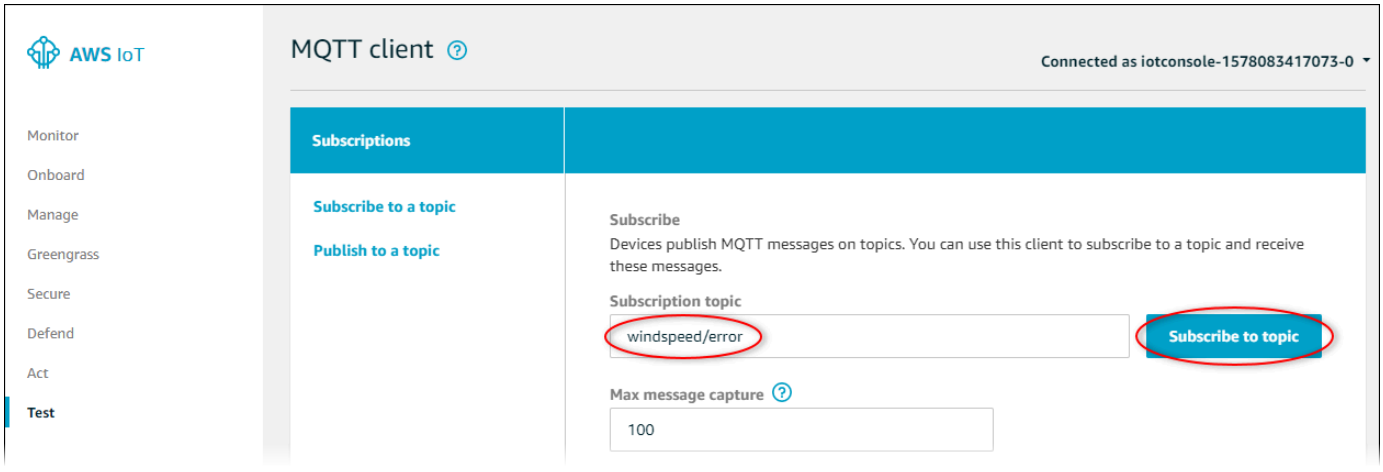
11. Wählen Sie Add action (Aktion hinzufügen) aus, um das Hinzufügen der Fehleraktion abzuschließen.
12. Wählen Sie den Zurück-Pfeil oben links auf der Konsole, um zur Startseite der AWS IoT Core-Konsole zurückzukehren.

Nachdem Sie die Aktion „Fehler erneut veröffentlichen“ eingerichtet haben, können Sie die Fehlermeldungen im MQTT-Testclient in AWS IoT Core anzeigen.

Im folgenden Verfahren abonnieren Sie das Fehlerthema im MQTT-Testclient.

So abonnieren Sie das Fehleraktionsthema.

1. Wählen Sie auf der linken Navigationsseite der AWS IoT Core-Konsole die Option Test aus.
2. Geben Sie im Feld Subscription topic (Abonnementthema) „**`windspeed/error`**“ ein und wählen Sie Subscribe to topic (Thema abonnieren) aus.



3. Achten Sie darauf, dass Fehlermeldungen angezeigt werden, und erkunden Sie das `failures`-Array in einer Fehlermeldung, um die folgenden häufigsten Probleme zu diagnostizieren:

- Tippfehler in der Regelabfrageanweisung
- Unzureichende Rollenberechtigungen

Wenn keine Fehler angezeigt werden, überprüfen Sie, ob Ihre Regel aktiviert ist und ob Sie das in der Aktion „Fehler wiederveröffentlichen“ konfigurierte Thema abonniert haben. Wenn immer noch keine Fehler angezeigt werden, überprüfen Sie, ob Ihre Demo-Windparkkomponenten noch vorhanden sind und ob Sie Benachrichtigungen zu den Windgeschwindigkeitseigenschaften aktiviert haben. Wenn Ihre Demo-Assets abgelaufen sind und nicht mehr verfügbar sind AWS IoT SiteWise, können Sie eine neue Demo erstellen und die Regelabfrageanweisung aktualisieren, sodass sie das aktualisierte Asset-Modell und die aktualisierten Eigenschaften-IDs wiedergibt.

AWS IoT SiteWise Endpunkte und Kontingente

In den folgenden Abschnitten werden die Endpunkte und Kontingente für AWS IoT SiteWise beschrieben.

Inhalt

AWS IoT SiteWise Endpunkte

Um programmgesteuert eine Verbindung herzustellen AWS IoT SiteWise, verwenden Sie einen Endpunkt. Die AWS SDKs und die AWS Command Line Interface (AWS CLI) verwenden automatisch den Standardendpunkt in einer Region. AWS Weitere Informationen zu Regionen, in denen AWS IoT SiteWise es verfügbar ist, finden Sie unter AWS IoT SiteWise Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

AWS IoT SiteWise unterstützt die folgenden Endpunkte.

Verwenden Sie diesen Endpunkt, um auf die folgenden API-Operationen auf Datenebene zuzugreifen:,, und. BatchPutAssetPropertyValueGetAssetPropertyAggregatesGetAssetPropertyValueGetAssetPropertyValueHis
Ersetze es *region* durch deine AWS Region.

AWS IoT SiteWise bietet diesen konsolidierten Endpunkt für API-Operationen auf der Kontrollebene, mit denen Sie Asset-Modelle, Assets, Edge-Gateways, Tags und Kontokonfigurationen verwalten. SiteWise Ersetze es *region* durch deine AWS Region.

> **Note**
>
> - AWS IoT SiteWise Verwendet standardmäßig den konsolidierten Endpunkt, wenn Sie Aufrufe an die unterstützten API-Operationen der Steuerungsebene tätigen.
> - Wir empfehlen, den konsolidierten Endpunkt für die unterstützten API-Operationen auf der Kontrollebene zu verwenden.

- Sie können den konsolidierten Endpunkt nicht für den Zugriff auf die SiteWise Monitor-API-Operationen verwenden.

Zu den unterstützten API-Vorgängen auf der Steuerungsebene gehören AssociateAssetsCreateAssetCreateAssetModelDeleteAssetDeleteAssetModelDeleteDashboardDescribeAss DescribeAssetModel, DescribeAssetProperty, DescribeDashboard, DescribeLoggingOptions, DisassociateAssets, ListAssetModels, ListAssetRelationships, ListAssets, ListAssociatedAssets, PutLoggingOptions, UpdateAsset, UpdateAssetModel, UpdateAssetProperty, CreateGateway, DeleteGateway, DescribeGateway, DescribeGatewayCapabilityConfiguration, ListGateways, UpdateGateway, UpdateGatewayCapabilityConfiguration, DescribeStorageConfiguration, PutStorageConfiguration, DescribeDefaultEncryptionConfiguration, ListTagsForResource, PutDefaultEncryptionConfiguration, TagResource, und UntagResource.

Der VPC-Schnittstellen-Endpunkt für die API-Operationen auf der Kontrollebene unterstützt nur den konsolidierten Endpunkt. Weitere Informationen finden Sie unter VPC-Endpunkte .

Verwenden Sie diesen Endpunkt, um auf die folgenden API-Operationen zuzugreifen:,,,,, und. DescribeStorageConfigurationPutStorageConfigurationDescribeDefaultEncryptionConfigurationListTagsForR Ersetze es *region* durch deine AWS Region.

Verwenden Sie diesen Endpunkt, um auf die folgenden API-Operationen zuzugreifen: AssociateAssets,,,,, CreateAsset,, CreateAssetModel,, DeleteAsset,, DeleteAssetModel, DeleteDashboardDescribeAssetDescribeAssetModelDescribeAssetPropertyDescribeDashboardDescribeLog docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAsset.html, UpdateAssetModel, und UpdateAssetProperty. Ersetze es *region* durch deine AWS Region.

Verwenden Sie diesen Endpunkt, um auf die folgenden API-Operationen zuzugreifen:,,,, und. CreateGatewayDeleteGatewayDescribeGatewayDescribeGatewayCapabilityConfigurationListGatewaysUpda Ersetze es *region* durch deine AWS Region.

Verwenden Sie diesen Endpunkt, um auf die folgenden API-Operationen zuzugreifen: BatchAssociateProjectAssets,,,,,,, BatchDisassociateProjectAssets,, CreateAccessPolicy,, CreateDashboard, CreatePortalCreateProjectDeleteAccessPolicyDeletePortalDeleteProjectDescribeAccessPolicyDescribePorta docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_UpdateAccessPolicy.html, UpdateDashboardUpdatePortal, und UpdateProject. Ersetze es *region* durch deine AWS Region.

AWS IoT SiteWise Kontingente

In den folgenden Tabellen werden Kontingente in beschrieben AWS IoT SiteWise. Weitere Informationen zu Kontingenten und zur Beantragung von Kontingenterhöhungen finden Sie unter AWS Servicekontingenten im Allgemeine AWS-Referenz. Weitere Informationen zu AWS IoT SiteWise Kontingenten finden Sie unter AWS IoT SiteWise Servicekontingenten im Allgemeine AWS-Referenz.

Kontingente für Komponenten und Komponentenmodelle

Ressource	Kontingent	Einstellbar	Hinweise
Anzahl der Asset-Modelle pro Region pro AWS Konto	1000	Ja	
Anzahl der Komponenten pro Komponentenmodell	10.000	Ja	
Anzahl der untergeordneten Komponenten pro übergeordneter Komponente	2000	Ja	
Tiefe der Hierarchiestruktur des Komponentenmodells	30	Ja	
Anzahl der Hierarchiedefinitionen pro Komponentenmodell	30	Ja	
Anzahl der Immobilien auf der Stammebene pro Asset-Modell	500	Ja	Diese maximale Anzahl von `assetModelProperties` für jedes Asset-Modell. Diese

Ressource	Kontingent	Einstellbar	Hinweise
			Anzahl beinhalte t nicht`compositeModelProperties` . Diese Quote gilt auch für jedes einzelne Asset, das mit diesem Asset-Modell erstellt wurde.
Anzahl der Eigenscha ften pro Komponent enmodell	5000	Ja	Die maximale Anzahl von Eigenschaften eines Vermögens modells vom Typ `ASSET_MODEL` oder`COMPONENT_MODEL` . Diese Anzahl wird durch die Kombination der Eigenschaften des Stammobjektmodells und aller enthaltenen component-model-ba sed oder zusammeng esetzten Inline-Mo delle bestimmt. Diese Quote gilt auch für jedes einzelne Asset, das anhand dieses Asset-Modells erstellt wurde.

Ressource	Kontingent	Einstellbar	Hinweise
Anzahl der Eigenschaften pro zusammengesetztem Modell	100	Ja	Die maximal zulässige Anzahl von Eigenschaften für zusammengesetzte Modelle. Außerdem die maximale Anzahl von Eigenschaften, die für ein Objektmodell des Typs zulässig sind`COMPONENT_MODEL` .
Tiefe des Eigenschaftenbaums pro Komponentenmodell	10	Nein	Beispielsweise hat ein Modell mit einer Transformationseigenschaft C, das eine Transformationseigenschaft B verbraucht, die wiederum eine Messeigenschaft A verbraucht, eine Tiefe von 3.
Anzahl der Komponentenmodelle pro Hierarchiebaum	100	Ja	

Ressource	Kontingent	Einstellbar	Hinweise
Anzahl der direkt abhängigen Eigenschaften pro Komponentenmodell	20	Nein	Dieses Kontingent begrenzt die Anzahl der Eigenschaften, die direkt von einer einzelnen Eigenschaft abhängen können, wie in Eigenschaftsformelausdrücken definiert. Die Anzahl der abhängigen Eigenschaften für ein Anlagenmodell muss größer sein als die Anzahl der direkt abhängigen Eigenschaften pro Anlagenmodell. Sie müssen für beide eine Erhöhung der Quote beantragen, wenn der Grenzwert für die Anzahl der direkt abhängigen Immobilien pro Anlagemodell höher ist als der Grenzwert für die Anzahl der abhängigen Immobilien pro Anlagemodell.

Ressource	Kontingent	Einstellbar	Hinweise
Anzahl abhängige r Eigenschaften pro Komponentenmodell	30	Nein	Dieses Kontingent begrenzt die Anzahl der Eigenschaften, die direkt oder indirekt von einer einzelnen Eigenschaft abhängen können, wie in Eigenschaftsformel ausdrücken definiert.
Anzahl der zusammeng esetzten Modelle pro Anlagenmodell	50	Ja	Die maximale Anzahl zusammengesetzter Modelle, die für ein einzelnes Anlagenmo dell zulässig sind.
Tiefe des zusammeng esetzten Modells	2	Ja	Die maximale Tiefe des zusammeng esetzten Modellbau ms pro Anlagenmo dell, einschließlich Inline- und component -model-based zusammengesetzter Modelle.

Ressource	Kontingent	Einstellbar	Hinweise
Anzahl einzigartiger Anlagenmodelle, die dasselbe Komponentenmodell verwenden	20	Ja	Die maximale Anzahl einzigartiger Asset-Modelle, die mindestens ein component-model-based zusammengesetztes Modell haben, das direkt auf ein bestimmtes Asset-Modell vom Typ COMPONENT_MODEL verweist.
Anzahl der Eigenschaftsvariablen pro Eigenschaftsformelausdruck	10	Nein	Der Ausdruck enthält beispielsweise zwei Eigenschaftsvariablen, `power` und`temp`,. `avg(power) + max(temp)` Dies gilt auch für Ergebnisse von Transformationsberechnungen.
Anzahl der Funktionen pro Eigenschaftsformelausdruck	10	Nein	Der Ausdruck `avg(power) + max(temp)` enthält beispielsweise zwei Funktionen`max`, `avg` und,.

Kontingente für Komponenteneigenschaftsdaten

Ressource	Kontingent	Einstellbar	Hinweise
Anforderungsrate für Komponenteneigenschaftsdaten-API-Operationen	1000 Anfragen pro Sekunde pro Region pro AWS Konto	Ja	Dieses Kontingent gilt für API-Operationen wie `GetAssetPropertyValue` und `BatchPutAssetPropertyValue`.
Anzahl der Datenpunkte pro Sekunde, Datenqualität und Komponenteneigenschaft	10 Datenpunkte	Nein	Dieses Kontingent gilt für die maximale Anzahl von timestamp-quality-value (TQV) Datenpunkten mit demselben Zeitstempel in Sekunden pro Datenqualität für jede Anlageneigenschaft. Dies ist die maximale Anzahl von Datenpunkten guter, unsicherer und schlechter Qualität, die Sie für eine bestimmte Sekunde pro Komponenteneigenschaft speichern können.
Anzahl der pro Sekunde aufgenommenen `BatchPutAssetPropertyValue` Einträge pro Anlageobjekt pro	10 Einträge pro Anlageobjekt	Nein	Dieses Kontingent gilt für `BatchPutAssetPropertyValue` Einträge aus allen Quellen, einschließlich

Ressource	Kontingent	Einstellbar	Hinweise
Region pro Konto. AWS			SiteWise Edge-Gateways, AWS IoT Core Regeln und API-Aufrufen.
Rate der übernommenen Datenpunkte	5000 Datenpunkte pro Sekunde pro Region pro Konto AWS	Ja	Timestamp-quality-value (TQV) -Datenpunkte.
Rate anfragen für `BatchGetAssetPropertyAggregates`	200	Ja	Die maximale Anzahl von `BatchGetAssetPropertyAggregates` Anfragen pro Sekunde, die Sie mit diesem Konto in der aktuellen Region ausführen können.
Rate der Anfragen für `BatchGetAssetPropertyValue`	500	Ja	Die maximale Anzahl von `BatchGetAssetPropertyValue` Anfragen pro Sekunde, die Sie mit diesem Konto in der aktuellen Region ausführen können.

Ressource	Kontingent	Einstellbar	Hinweise
Rate der Anfragen für `BatchGetAssetPropertyValueHistory`	200	Ja	Die maximale Anzahl von `BatchGetAssetPropertyValueHistory` Anfragen pro Sekunde, die Sie mit diesem Konto in der aktuellen Region ausführen können.
Anzahl der pro Sekunde pro Vermögenswert, pro Region und AWS Konto aufgenommenen `BatchPutAssetPropertyValue` Einträge.	10 Einträge pro Anlageobjekt	Nein	Dieses Kontingent gilt für `BatchPutAssetPropertyValue` Einträge aus allen Quellen, einschließlich SiteWise Edge-Gateways, AWS IoT Core Regeln und API-Aufrufen.
Rate der `GetAssetPropertyAggregates` Anfragen und `BatchGetAssetPropertyAggregates` Eingabeabfragen pro Objekteigenschaft	50	Nein	Die maximale Gesamtzahl der `GetAssetPropertyAggregates` Anfragen und `BatchGetAssetPropertyAggregates` Einträge für jede Anlageeigenschaft pro Sekunde auf diesem Konto in der aktuellen Region.

Ressource	Kontingent	Einstellbar	Hinweise
Rate der `GetAssetPropertyValue` Anfragen und `BatchGetAssetPropertyValue` Eingabeanfragen pro Anlageobjekt	500	Nein	Die maximale Gesamtzahl der `GetAssetPropertyValue` Anfragen und `BatchGetAssetPropertyValue` Einträge für jede Anlageeigenschaft pro Sekunde auf diesem Konto in der aktuellen Region.
Rate der `GetAssetPropertyValueHistory` Anfragen und `BatchGetAssetPropertyValueHistory` Eingabeanfragen pro Anlageobjekt	30	Nein	Die maximale Gesamtzahl der `GetAssetPropertyValueHistory` Anfragen und `BatchGetAssetPropertyValueHistory` Einträge für jede Anlageeigenschaft pro Sekunde auf diesem Konto in der aktuellen Region.

Ressource	Kontingent	Einstellbar	Hinweise
Rate der `GetInterpolatedAssetPropertyValues` Anfragen	500	Ja	Die maximale Anzahl von `GetInterpolatedAssetPropertyValues` Anfragen pro Sekunde, die Sie mit diesem Konto in der aktuellen Region ausführen können.
Anzahl der Ergebnisse pro `GetInterpolatedAssetPropertyValues` Anfrage	10	Ja	Die maximale Anzahl von Ergebnissen, die pro paginierter `GetInterpolatedAssetPropertyValues` Anfrage zurückgegeben werden.

Ressource	Kontingent	Einstellbar	Hinweise
Rate der abgerufenen Datenpunkte von und `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory`	100 MB Lesereaktion pro Sekunde pro Region und Konto. AWS	Ja	Die maximale Byterate (MB/Sekunde) der pro Sekunde abgerufenen Datenpunkte pro Region pro Konto über und. AWS `GetAssetPropertyValueHistory` `BatchGetAssetPropertyValueHistory` Die für dieses Kontingent ausgewertete Antwortnutzlast verwendet Timestamp-Quality-Value (TQV) -Felder für jeden Datenpunkt und rundet die Bytegröße für jede API-Anfrage auf das nächste 4-KB-Inkrement. Die pro Sekunde abgerufenen Timestamp-quality-value (TQV) -Datenpunkte variieren je nach Datentyp:

Ressource	Kontingent	Einstellbar	Hinweise
			• Ganzzahl — bis zu 5 Millionen TQV pro Sekunde • Doppelt — bis zu 4 Millionen TQV pro Sekunde • Boolean — bis zu 6 Millionen TQV pro Sekunde • Zeichenfolge — variiert je nach Größe der einzelnen Zeichenkettenwerte .

Kontingente für SiteWise Edge-Gateways

Ressource	Kontingent	Einstellbar
Anzahl der SiteWise Edge-Gateways pro Region pro Konto AWS	100	Ja
Anzahl der OPC-UA-Quellen pro Edge-Gateway SiteWise	100	Nein

Kontingente für AWS IoT SiteWise Monitor

Ressource	Kontingent	Einstellbar
Anzahl der Portale pro Region pro AWS Konto	100	Ja

Ressource	Kontingent	Einstellbar
Anzahl der Projekte pro Portal	100	Ja
Anzahl der Dashboards pro Projekt	100	Ja
Anzahl der Root-Komponenten pro Projekt	1	Nein
Anzahl der Visualisierungen pro Dashboard	10	Ja
Anzahl der Metriken pro Dashboard-Visualisierung	5	Ja
Anzahl der Schwellenwerte pro Dashboard-Visualisierung	12	Nein

Kontingente für den AWS IoT SiteWise Massenimport und -export von Metadaten

Ressource	Beschreibung	Kontingent	Einstellbar
Anzahl der Metadatentransferaufträge in der Warteschlange	Die maximale Anzahl von `PENDING` Metadatentransferaufträgen in der Warteschlange.	10	Ja
Größe der Importdatei für den Metadatentransferauftrag	Die maximale Größe der importierten Datei (in MB).	100 MB	Ja
AWS IoT SiteWise Ressourcenkontingent für einen Metadatentransferauftrag	Die maximale Anzahl von Ressourcen, die in einem einzelnen Auftrag importiert oder exportiert werden. Eine Ressource	5000	Nein

Ressource	Beschreibung	Kontingent	Einstellbar
	umfasst Anlagen und Anlagenmodelle.		

Kontingente für den AWS IoT SiteWise Massenimport von Daten

Ressource	Kontingent	Einstellbar
Anzahl der laufenden Massenimportaufträge	100	Nein
Größe der CSV-Datei	10 GB	Nein
Größe der unkomprimierten Parkettdatei	256 MB	Nein
Größe der CSV Datei für die gepufferte Aufnahme	256 MB	Nein
Größe der unkomprimierten Parkett-Reihengruppe	64 MB	Nein
Anzahl der Einzelmessungen pro Parkettreihengruppe	2000	Ja
Anzahl der Tage zwischen dem Zeitstempel in der Vergangenheit und dem heutigen Zeitpunkt für die gepufferte Aufnahme	30	Ja
Anfragerate `CreateBulkImportJobs` für jede Region in jedem Konto AWS	10	Ja
Tarif `ListBulkImportJobs` für jede Region in jedem AWS Konto anfragen	50	Ja

Ressource	Kontingent	Einstellbar
Tarif `DescribeBulkImportJobs` für jede Region in jedem AWS Konto anfragen	50	Ja

Kontingente für die Erkennung von Anomalien

Die Kontingente für die Erkennung von Anomalien werden von Amazon Lookout for Equipment gemeinsam genutzt. AWS IoT SiteWise Weitere Informationen finden Sie unter Kontingente für die Nutzung von Lookout for Equipment.

Dokumentverlauf für das AWS IoT SiteWise - Benutzerhandbuch

Die folgende Tabelle beschreibt die Dokumentation für diese Version von AWS IoT SiteWise.

- API-Version: 02.12.2019

Änderung	Beschreibung	Datum
Unterstützung für die Ausführung von SiteWise Edge auf Industrie Edge hinzugefügt	AWS IoT SiteWise unterstützt jetzt die Ausführung von SiteWise Edge auf.	26. November 2023
Unterstützung für Warm Tier Storage hinzugefügt	AWS IoT SiteWise unterstützt jetzt Warm Storage, eine vollständig verwaltete Speicherebene, die es Kunden erleichtert, industrielle Daten sicher zu speichern und darauf zuzugreifen.	15. November 2023
Unterstützung für benutzerdefinierte eindeutige Kennungen hinzugefügt	AWS IoT SiteWise unterstützt jetzt die Verwendung benutzerdefinierter eindeutiger Kennungen für Komponenten, Komponentenmodelle, Eigenschaften und Hierarchien.	15. November 2023
Unterstützung für die Erkennung von Anomalien mit mehreren Varianten von Industriekomponenten hinzugefügt	AWS IoT SiteWise unterstützt jetzt die Erkennung von Multi-Varianten-Anomalie von Industriekomponenten durch die Integration historischer und Echtzeit-Equipment-	15. November 2023

	Daten mit Amazon Lookout for Equipment.	
Unterstützung für die kosteneffiziente und skalierbare Aufnahme von Zeitreihendaten in hinzugefügt AWS IoT SiteWise	AWS IoT SiteWise unterstützt jetzt die kosteneffiziente und skalierbare Erfassung von Zeitreihendaten, die für analytische Anwendungsfälle benötigt werden.	15. November 2023
Unterstützung für Massenimport, Export und Aktualisierung hinzugefügt	AWS IoT SiteWise unterstützt jetzt Massenimport, Export und Aktualisierung von Metadaten für Industrieanlagen.	15. November 2023
Unterstützung für Komponentenmodellkomponenten hinzugefügt	AWS IoT SiteWise unterstützt jetzt Komponenten des Komponentenmodells, um Industriekunden bei der Erstellung wiederverwendbarer Komponenten zu unterstützen.	15. November 2023
Unterstützung für IoT-Dashboard-Anwendung hinzugefügt	AWS IoT SiteWise unterstützt jetzt eine Open-Source-Dashboard-Anwendung, mit der Sie Betriebsdaten visualisieren und mit ihnen interagieren können.	15. November 2023
Serviceverknüpfte Rollen für aktualisiert AWS IoT SiteWise	AWS IoT SiteWise verfügt über neue serviceverknüpfte Rollen und kann eine Metadatensuchabfrage für die AWS IoT TwinMaker Datenbank ausführen.	6. November 2023

Aktualisierte Markierung für AWS IoT SiteWise Datenstrommressourcen	Unterstützung für das Markieren von Datenstrommressourcen hinzugefügt.	18. August 2022
Aktualisierte SiteWise Edge-Gateways	Sie können den Herausgeber jetzt so konfigurieren, dass er steuert, welche Daten vom Edge an die Cloud gesendet werden und in welcher Reihenfolge sie an die Cloud gesendet werden.	12. Januar 2022
AWS IoT SiteWise Die Demo wurde aktualisiert	Sie können jetzt die Demo verwenden, um ein SiteWise Monitor-Portal zu erstellen.	10. Januar 2022
Aktualisierte Speicherverwaltung	Sie können jetzt einen Aufbewahrungszeitraum definieren, um zu steuern, wie lange Ihre Daten auf der Hot Tier aufbewahrt werden.	29. November 2021
Unterstützung für die Verwaltung von Datenströmen hinzugefügt	Sie können jetzt Daten in aufnehmen, AWS IoT SiteWise bevor Sie Komponentenmodelle und Komponenten erstellen.	24. November 2021
Aktualisierte Komponentenmodellhierarchien	Ein untergeordnetes Komponentenmodell kann jetzt mehreren übergeordneten Komponentenmodellen zugeordnet werden.	28. Oktober 2021
Start der Region	Wird AWS IoT SiteWise in AWS GovCloud (USA-West) gestartet.	29. September 2021

Aktualisierte Funktionen	Die folgenden Funktionen wurden hinzugefügt • In Metriken können Sie verschachtelte Ausdrücke in Aggregationsfunktionen und zeitlichen Funktionen verwenden. • In Transformationen können Sie die Funktion pretrigger() verwenden, um den Wert einer Variablen vor der Eigenschaftsaktualisierung abzurufen, die die aktuelle Transformationsberechnung ausgelöst hat.	10. August 2021
Zeitintervall für benutzerdefinierte Metriken	Unterstützung für benutzerdefinierte Zeitintervalle und Offsets in Metriken hinzugefügt.	3. August 2021
Verwenden von AWS IoT SiteWise am Edge	Das Edge-Verarbeitungsfeature ist jetzt allgemein verfügbar.	29. Juli 2021
Exportieren von Daten nach Amazon S3	AWS IoT SiteWise kann jetzt Daten nach Amazon S3 exportieren.	27. Juli 2021
VPC-Endpunkte (AWS PrivateLink)	Der Schnittstellen-VPC-Endpunkt für die API-Operationen der Steuerebene ist jetzt allgemein verfügbar.	15. Juli 2021
Transformationen	Transformationen können jetzt mehrere Komponenteneigenschaftsvariablen eingeben.	8. Juli 2021

Die Funktion timestamp() wurde aktualisiert	In Transformationen können Sie jetzt eine Variable als Argument für die `timestamp()` Funktion bereitstellen.	16. Juni 2021
Alarmiert die allgemeine Verfügbarkeit	Die Alarmfunktion ist jetzt allgemein verfügbar.	27. Mai 2021
Bol-TCP Protocol Adapter Version 2 veröffentlicht	Version 2 des microSD-TCP Protocol Adapter-Konnektors ist verfügbar. Diese Version hat Unterstützung für ASCII-, UTF8- und ISO8859-codierte Quellzeichenfolgen hinzugefügt.	24. Mai 2021
Aktualisierte Service Quotas	Die folgenden Kontingente für die GetInterpolatedAssetPropertyValues API wurden hinzugefügt: Rate der `GetInterpolatedAssetPropertyValues` Anforderungen, Anzahl der Ergebnisse pro `GetInterpolatedAssetPropertyValues` Anforderung und Anzahl der Tage zwischen dem Startdatum in der Vergangenheit und heute für `GetInterpolatedAssetPropertyValues` .	29. April 2021

Aktualisierte Formelausdrücke	Die folgenden Operatoren und Funktionen wurden hinzugefügt: • Die folgenden Operatoren wurden hinzugefügt: `<`, `>`, `<=`, `>=`, `==`, `!=`, , `!`, `or`, `and` und `not`. • Die folgende Vergleichsfunktion wurde hinzugefügt: `neq(x, y)`. • Die folgenden Zeichenfolgenfunktionen wurden hinzugefügt: `join()`, `format()`, und `f''`.	22. April 2021
VPC-Endpunkte (AWS PrivateLink)	Es wurden Informationen zum Herstellen einer privaten Verbindung zwischen Ihrer Virtual Private Cloud (VPC) und den APIs der AWS IoT SiteWise Steuerebene durch Erstellen eines Schnittstellen-VPC-Endpunkts hinzugefügt.	16. März 2021
IAM-Verbund	Ihre Administratoren und Benutzer des SiteWise Monitor-Portals können sich jetzt mit ihren IAM-Anmeldeinformationen bei ihren zugewiesenen Portalen anmelden.	16. März 2021
Start der Region	Wird AWS IoT SiteWise in China (Peking) gestartet.	3. Februar 2021

IoT SiteWise -Konnektor-Version 10 veröffentlicht	Version 10 des IoT SiteWise -Konnektors ist verfügbar. Diese Version konfiguriert , `StreamManager` um die Handhabung zu verbesser n, wenn die Quellverbindung verloren geht und wiederher gestellt wird. Diese Version akzeptiert auch OPC-UA-We rte mit einem , `ServerTim estamp` wenn kein verfügbar `SourceTimestamp` ist.	22. Januar 2021
Datums- und Uhrzeitfu nktionen	AWS IoT SiteWise unterstüt zt jetzt Datums- und Uhrzeitfu nktionen.	21. Januar 2021
Funktionssyntax	Sie können jetzt UFCS (Uniform Function Call Syntax) für - AWS IoT SiteWise Funktionen verwenden.	11. Januar 2021
Integration in Grafana	Es wurden Informationen zur Visualisierung von AWS IoT SiteWise Daten in Grafana-D ashboards hinzugefügt.	15. Dezember 2020

AWS IoT SiteWise Feature-Version	Sie können Ihre Daten jetzt mit Alarmen überwachen, Industriedaten am Edge verarbeiten, TCP- und Ethernet/IP-Quellen für Ihr SiteWise Edge-Gateway verwenden, eingehende Daten nach Deadbands filtern und vieles mehr. • Der Abschnitt Überwachung von Daten mit Alarmen wurde hinzugefügt, mit dem Sie Alarme in definieren, konfigurieren und darauf reagieren können AWS IoT SiteWise. • Der Abschnitt Edge-Verarbeitung wurde hinzugefügt, mit dem Sie die Verarbeitung Ihrer industriellen Daten auf Ihren Edge-Geräten konfigurieren können. • Die Abschnitte TCP und Ethernet/IP wurden der SiteWise Edge-Gateway-Quelldokumentation hinzugefügt. • Der Abschnitt Quellziel wurde hinzugefügt, mit dem Sie anpassen können, wohin Sie Ihre eingehenden Industriedaten senden. • Der Abschnitt OPC-UA-Filterung wurde hinzugefügt, mit dem Sie die Häufigkeit	15. Dezember 2020

	und Art der Daten steuern können, die von Ihrem lokalen Industrieserver an Ihr SiteWise Edge-Gateway gesendet werden.	
AWS IoT SiteWise unterstützt jetzt vom Kunden verwaltete CMKs.	AWS IoT SiteWise unterstützt jetzt die Verschlüsselung mit vom Kunden verwalteten CMKs .	24. November 2020
IoT SiteWise -Konnektor Version 8 veröffentlicht	Version 8 des IoT SiteWise -Konnektors ist verfügbar. Diese Version verbessert die Stabilität, wenn der Konnektor zeitweilige Netzwerkkonnektivität aufweist.	19. November 2020
Verwenden von Zeichenfolgen und Bedingungen in Formelausdrücken	Es wurden Informationen zur Verwendung von Zeichenfolgen und bedingten Funktionen in Formelausdrücken für Transformationen und Metriken hinzugefügt.	16. November 2020
Erfassen von Daten mit AWS IoT Greengrass Stream Manager	Es wurden Informationen zur Aufnahme von IoT-Daten mit hohem Volumen aus lokalen Datenquellen mithilfe eines AWS IoT Greengrass Edge-Geräts hinzugefügt.	16. September 2020

VPC-Endpunkte (AWS PrivateLink)	Es wurden Informationen zum Herstellen einer privaten Verbindung zwischen Ihrer Virtual Private Cloud (VPC) und den AWS IoT SiteWise Daten-APIs durch Erstellen eines Schnittstellen-VPC-Endpunkts hinzugefügt.	4. September 2020
IoT SiteWise -Konnektor Version 7 veröffentlicht	Version 7 des IoT SiteWise -Konnektors ist verfügbar . Diese Version behebt ein Problem mit SiteWise Edge-Gateway-Metriken.	14. August 2020
Erstellen von IAM-Identity-Center-Benutzern über die AWS IoT SiteWise Konsole	Es wurden Informationen darüber hinzugefügt, wie Sie IAM-Identity-Center-Benutzer in der AWS IoT SiteWise Konsole erstellen können. Sie können jetzt IAM-Identity-Center-Benutzer erstellen, wenn Sie Benutzer einem neuen oder vorhanden en Portal zuweisen. Das Tutorial Visualisieren und Freigeben von Archivdaten wurde aktualisiert, um dieses Feature zu verwenden. Diese Änderung reduziert die Anzahl der Schritte im Tutorial.	4. August 2020

Verbesserte SiteWise Edge-Gateway-Fehlerbehebung	Zusätzliche Informationen zur Fehlerbehebung bei einem SiteWise Edge-Gateway und zum Exportieren des OPC-UA-Clientzertifikats für eine Quelle wurden hinzugefügt.	18. Juni 2020
Dokumentation zu Konsolenaufgaben	Konsolenaufgabendokumentation für Modellieren von industriellen Komponenten, Abfragen von Komponenteneigenschaftsdaten und Interaktion mit anderen Services hinzugefügt. Sie können diese Anweisungen befolgen, um Aufgaben in der AWS IoT SiteWise -Konsole durchzuführen.	11. Juni 2020
Tutorial zum Analysieren exportierter Daten	Es wurde ein Tutorial hinzugefügt, dem Sie folgen können, um zu erfahren, wie Sie mit Amazon Athena Komponentendaten analysieren, die Sie mit der AWS CloudFormation Exportfunktionsvorlage nach S3 exportiert haben.	27. Mai 2020
Verbesserung durch Formelausdrücke	Es wurden detaillierte Informationen zum Verhalten von AWS IoT SiteWise Formeleigenschaften und ein Beispiel für das Zählen gefilterter Datenpunkte hinzugefügt.	18. Mai 2020

IoT SiteWise -Konnektor Version 6 veröffentlicht	Version 6 des IoT SiteWise -Konnektors ist verfügbar. Diese Version bietet Unterstützung für CloudWatch Metriken und die automatische Erkennung neuer OPC-UA-Tags. Das bedeutet, dass Sie Ihr SiteWise Edge-Gateway nicht neu starten müssen, wenn sich die Tags für Ihre OPC-UA-Quellen ändern. Für diese Version des Konnektors sind Stream Manager und AWS IoT Greengrass Core-Software v1.10.0 oder höher erforderlich.	29. April 2020

AWS IoT SiteWise Feature-Version	AWS IoT SiteWise Feature-Version. Sie können jetzt SiteWise Edge-Gateways mit der API verwalten, Ihr Logo zu Portalen hinzufügen, SiteWise Edge-Gateway-Metriken anzeigen und vieles mehr. • Der Abschnitt Exportieren von Daten nach Amazon S3 wurde mit einer - AWS CloudFormation Vorlage hinzugefügt, mit der Sie neue Datenwerte in einen S3-Bucket exportieren können. • Der Abschnitt Konfigurieren von Datenquellen wurde hinzugefügt, der die Dokumentation zur SiteWise Edge-Gateway-Quelle verbessert und die neuen SiteWise Edge-Gateway-APIs enthält. • Der Abschnitt SiteWise Edge-Gateway-Metriken wurde hinzugefügt, der die CloudWatch Metriken beschreibt, die SiteWise Edge-Gateways veröffentlichen. • Der Abschnitt Konfigurieren eines SiteWise Edge-Gateways auf Amazon EC2 wurde mit einer - AWS CloudFormation Vorlage	29. April 2020

	hinzugefügt, mit der Sie schnell SiteWise Edge-Gateway-Abhängigkeiten auf einer Amazon EC2-Instance konfigurieren können. • Der Abschnitt Portalservicerollen wurde hinzugefügt, der die neue Berechtigungsfunktion von Portale SiteWise überwachen beschreibt. • Aktualisierung der Portaldokumentation für Portal-Servicerollen und Portal-Logos. • Der Abschnitt Markieren Ihrer - AWS IoT SiteWise Ressourcen wurde hinzugefügt. • Aktualisierung des Abschnitts Erstellung von Dashboards (CLI) für die neue Dashboard-Definitionsstruktur. • Hinzufügung des Abschnitts Sicherheit.	
Erfassen von Daten aus AWS IoT Events	Es wurden Informationen zur Aufnahme von Daten aus hinzugefügt AWS IoT Events , wenn ein Ereignis eintritt.	20. April 2020

Visualisieren und Freigeben von Daten aus der Jungfernfarm im SiteWise Monitor-Tutorial	Es wurde ein Tutorial hinzugefügt, dem Sie folgen können, um zu erfahren, wie Sie verwenden, um Komponentendaten AWS IoT SiteWise Monitor zu visualisieren und gemeinsam zu nutzen.	12. März 2020
AWS IoT SiteWise -Konzepte	Es wurde ein Glossar mit AWS IoT SiteWise Konzepten hinzugefügt, mit denen Sie mehr über den Service und seine gängigen Begriffe erfahren können.	5. März 2020
AWS IoT Greengrass Installationsanweisungen entfernt	Die Anweisungen zur Installation der AWS IoT Greengrass Core-Software wurden aus dem AWS IoT SiteWise -Benutzerhandbuch entfernt. Das -AWS IoT Greengrass Entwicklerhandbuch bietet ein Geräteeinrichtungsskript und Anweisungen zum Einrichten von AWS IoT Greengrass auf anderen Plattformen wie Amazon EC2 und Docker.	14. Februar 2020
Verbesserte Aufnahme von Daten mithilfe von AWS IoT Core Regeln	Es wurden detaillierte Informationen zur Verwendung von und zur Fehlerbehebung bei der AWS IoT SiteWise Regelaktion hinzugefügt, mit der Sie Daten aus MQTT-Nachrichten über aufnehmen können AWS IoT Core.	14. Februar 2020

IoT SiteWise -Konnektor Version 5 veröffentlicht	Version 5 des IoT SiteWise -Konnektors ist verfügbar . Diese Version behebt ein Kompatibilitätsproblem mit AWS IoT Greengrass Core-Software v1.9.4.	12. Februar 2020
IoT SiteWise -Konnektor Version 4 veröffentlicht	Version 4 des IoT SiteWise -Konnektors ist verfügbar . Diese Version behebt ein Problem mit der erneuten Verbindung des OPC-UA Servers.	7. Februar 2020
Neustrukturierung von Industriekomponenten für die Modellierung	Der Abschnitt „Aktualisieren von Komponenten und Modellen“ wurde in mehrere Themen innerhalb von „Modellierung industrieller Komponenten“ umstrukturiert. • Komponenten- und Modellzustände • Zuordnen von industriellen Datenströmen zu Komponenteneigenschaften • Aktualisieren von Attributwerten • Zuordnen und Aufheben der Zuordnung von Komponenten • Aktualisieren von Komponenten und Modellen • Löschen von Komponenten und Modellen	4. Februar 2020

Tutorial zum Aufnehmen von Daten aus AWS IoT Objekten	Es wurde ein Tutorial hinzugefügt, dem Sie folgen können, um zu erfahren, wie Sie eine - AWS IoT SiteWise Regelaktion konfigurieren, um Daten aus einer neuen oder vorhandenen AWS IoT Objektflotte aufzunehmen.	4. Februar 2020
Umstrukturiertes Abrufen von Daten aus AWS IoT SiteWise	Der Abschnitt Daten abrufen wurde in zwei Abschnitte der obersten Ebene umstruktu riert: Abfragen von Komponent eneigenschaftswerten und - aggregaten und Interaktion mit anderen - AWS Services.	21. Januar 2020
Veröffentlichen von Eigenscha ftswertaktualisierungen im Amazon-DynamoDB-Tutorial	Es wurde ein Tutorial hinzugefügt, dem Sie folgen können, um zu erfahren, wie Sie Eigenschaftswertbe nachrichtigungen verwenden , um Komponentendaten in DynamoDB zu speichern.	8. Januar 2020
Verwenden von Formelaus drücken	Es wurde die Formelaus drucksreferenz hinzugefü gt, um die Konstanten und Funktionen zu organisie ren, die für die Verwendun g in Transformations- und Metrikeigenschaften verfügbar sind. Umstrukturierung von Komponenteneigenschaften zu separaten Themen für jeden Eigenschaftstyp.	7. Januar 2020

Verwenden von OPC-UA-Kn otenfiltern	Es wurden Informationen zur Verwendung von OPC-UA-Kn otenfiltern zur Verbesserung der SiteWise Edge-Gateway-Leistung beim Hinzufügen von SiteWise Edge-Gateway-Quell en hinzugefügt.	3. Januar 2020
Aktualisieren eines Konnektors	Es wurden Informationen zum Aktualisieren eines SiteWise Edge-Gateways hinzugefügt, wenn eine neue Konnektor-Version veröffentlicht wird.	30. Dezember 2019
IoT SiteWise -Konnektor Version 3 veröffentlicht	Version 3 des IoT SiteWise -Konnektors ist verfügbar. Diese Version entfernt die Berechtigungsvoraussetzung für iot:*.	17. Dezember 2019
IoT SiteWise -Konnektor Version 2 veröffentlicht	Version 2 des IoT SiteWise -Konnektors ist verfügbar. Diese Version bietet Unterstüt zung für mehrere OPC-UA-Se cret-Ressourcen.	10. Dezember 2019
Erstellen von Dashboards (AWS CLI)	Es wurden Informationen zum Erstellen eines Dashboards in AWS IoT SiteWise Monitor mithilfe der hinzugefügt AWS CLI.	6. Dezember 2019

AWS IoT SiteWise Version 2 veröffentlicht	Vorschau für Version 2 von veröffentlicht AWS IoT SiteWise. Sie können jetzt Daten über OPC-UA, MQTT und HTTP aufnehmen, Ihre Daten in Komponentenhierarchien modellieren und Ihre Daten mit SiteWise Monitor visualisieren. • Der Abschnitt Komponentenmodellierung wurde im Hinblick auf Änderungen an Komponenten, Komponentenmodellen und Komponentenhierarchien neu geschrieben. • Der Abschnitt zur Datenaufnahme wurde aktualisiert, um AWS IoT Greengrass Konnektor-Schritte und Abschnitte zur Datenaufnahme ohne Gateway aufzunehmen. • Der AWS IoT SiteWise Monitor Abschnitt und ein separates Anwendungshandbuch wurden hinzugefügt, das zeigt, wie die SiteWise Monitor-Webanwendung verwendet wird. • Es wurden die Abschnitte Daten abfragen von AWS IoT SiteWise und Interaktion	02. Dezember 2019

	mit anderen AWS Diensten hinzugefügt. • Der Abschnitt Erste Schritte wurde umgeschrieben, um der Erfahrung der aktualisierten Demo zu entsprechen.	
AWS IoT SiteWise Version 1 veröffentlicht	Die erste Vorschau für Version 1 von wurde veröffentlicht AWS IoT SiteWise.	25. Februar 2019

AWS-Glossar

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

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