Leitfaden für die AWS IoT Geräteverwaltung mit Fleet Hub

Fleet Hub für AWS IoT Gerätemanagement

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Fleet Hub für AWS IoT Gerätemanagement: Leitfaden für die AWS IoT Geräteverwaltung mit Fleet Hub

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

... v
Was ist Fleet Hub for AWS IoT Device Management? ... 1
So funktioniert Fleet Hub for AWS IoT Device Management ... 1
So funktioniert die Fleet-Hub-Datenindexierung ... 2
So funktionieren Fleet-Hub-Alarme ... 2
So funktionieren Fleet-Hub-Jobs ... 3
Fleet Hub für AWS IoT Gerätemanagement für Administratoren ... 4
Erste Schritte ... 4
Erstellen Sie Ihre erste Fleet-Hub-Anwendung. ... 4
Verwaltung der Flottenindexierung für Fleet-Hub-Anwendungen ... 7
Fügen Sie Benutzer zu Fleet-Hub-Anwendungen hinzu ... 8
AWS und AWS IoT Core Dienste, die mit Fleet Hub for AWS IoT Device Management interagieren ... 8
Fehlerbehebung ... 10
Fleet Hub für AWS IoT Gerätemanagement für Benutzer ... 13
Erste Schritte ... 13
Erstellen Ihrer ersten Abfrage ... 13
Erstellen Ihres ersten Alarms ... 14
Aufrufen von Gerätedetails ... 18
Abfragen und Filter ... 22
Dashboard anzeigen ... 22
Erstellen Sie Abfragen mit Filtern ... 24
Arbeiten mit Aufträgen und Auftragsvorlagen in Fleet Hub for AWS IoT Device Management ... 26
Ausführen von Aufgaben ... 26
Anzeigen und Verwalten von Jobs ... 27
Alarme ... 28
Erstellen von Alarmen ... 30
Fehlerbehebung ... 31
Überwachung von Fleet Hub für AWS IoT Gerätemanagement ... 33
Protokollierung von API-Aufrufen von Fleet Hub for AWS IoT Device Management mit AWS CloudTrail ... 33
Informationen zu Fleet Hub in CloudTrail ... 34
Grundlegendes zu den Einträgen in der Protokolldatei von Fleet Hub for AWS IoT Device Management ... 35

Sicherheit ... 37
Datenschutz ... 38
Verschlüsselung im Ruhezustand ... 39
Verschlüsselung während der Übertragung ... 39
Identitäts- und Zugriffsverwaltung ... 39
Zielgruppe ... 39
Authentifizierung mit Identitäten ... 40
Verwalten des Zugriffs mit Richtlinien ... 44
Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM ... 47
Beispiele für identitätsbasierte Richtlinien ... 54
Fehlerbehebung ... 58
Compliance-Validierung ... 60
Ausfallsicherheit ... 61
AWS verwaltete Richtlinien ... 62
AWSIoTFleetHubFederationAccess ... 63
Richtlinienaktualisierungen ... 65
Sicherheit der Infrastruktur ... 67
Serviceübergreifende Confused-Deputy-Prävention ... 67
Fleet Hub end-of-life (EOL) FAQs ... 69
Wann geht Fleet Hub end-of-life? ... 69
Was passiert mit meinen Fleet Hub-Anwendungen an dem end-of-life Tag? ... 70
Was passiert mit meinen zugrunde liegenden AWS Ressourcen am und nach dem end-of-life Datum? ... 70
Wie lösche ich Fleet Hub-Anwendungen vor dem Datum? end-of-life ... 70
Werden beim Löschen von Fleet Hub-Anwendungen automatisch die zugrunde liegenden Ressourcen gelöscht? ... 72
Wie lösche ich meine zugrunde liegenden AWS Ressourcen? ... 72
Wie lösche ich Jobs? ... 72
Wie lösche ich Fleet Hub-Alarme? ... 73
Wie lösche ich IAM Identity Center-Benutzer, die in Fleet Hub erstellt wurden? ... 74
Was APIs funktioniert am und nach dem Datum nicht mehr? end-of-life ... 74
Was sind die bestehenden Funktionen von Fleet Hub und wie greife ich über die Konsole darauf zu? ... 75
Dokumentationsverlauf ... 77

AWS wird die AWS IoT Device Management Fleet Hub-Funktion am 18. Oktober 2025 einstellen und nimmt keine neuen Kunden mehr auf. Bestehende AWS IoT Device Management Fleet Hub-Kunden können Fleet Hub bis zum 17. Oktober 2025 nutzen. Weitere Informationen finden Sie unter Fleet Hub end-of-life (EOL) FAQs.

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.

Was ist Fleet Hub for AWS IoT Device Management?

Mit Fleet Hub for AWS IoT Device Management (Fleet Hub) können Sie eigenständige Webanwendungen zur Überwachung des Zustands Ihrer Geräteflotten erstellen. Sie können diese Anwendungen Benutzern in Ihrer Organisation zur Verfügung stellen, auch wenn diese keine AWS Konten haben. Verwenden Sie Fleet Hub, um allgemeine Flottenaufgaben wie die Untersuchung und Behebung von Betriebs- und Sicherheitsproblemen zu verwalten.

Fleet Hub bietet die folgenden Funktionen.

- Überwachung von Geräteflotten nahezu in Echtzeit.
- Einrichtung von Warnmeldungen, um Ihre Techniker über ungewöhnliches Verhalten zu informieren.
- Ausführen von Aufgaben

> **Note**
>
> Damit Fleet Hub Daten zum Konnektivitätsstatus indexieren kann, müssen Ihre Things eine Verbindung herstellen, AWS IoT Core deren Client-ID dem Namen des Dings entspricht.

So funktioniert Fleet Hub for AWS IoT Device Management

Administratoren können Fleet Hub for AWS IoT Device Management verwenden, um in wenigen Minuten sichere Webanwendungen zu erstellen, ohne Ressourcen bereitstellen oder Code schreiben zu müssen. Webanwendungen, die Sie mithilfe von Fleet Hub erstellen, lassen sich in Ihre vorhandenen Identitätssysteme wie Active Directory integrieren. Auf diese Weise können Ihre Administratoren ihre eigenen Authentifizierungs- und Autorisierungsmodelle anwenden.

Fleet Hub-Webanwendungen lassen sich in die AWS IoT Core Flottenindizierung und Geräteüberwachung integrieren. Diese Integrationen bieten die Möglichkeit, Gerätezustandsdaten zu überwachen und Alarme zu erstellen, wenn Geräte in Ihrer Flotte einen festgelegten Zustand erreichen.

Fleet-Hub-Anwendungen verwenden die `AWSIoTFleetHubFederationAccess`-verwaltete Richtlinie. Weitere Informationen finden Sie unter ???.

Beispielanwendungsfälle:

- Visualisieren Sie Probleme mit der Gerätekonnektivität – Sie können die Anzahl der getrennten Geräte in Ihrer Flotte, den letzten Verbindungsstatus für ein Gerät und den Grund oder die Gründe für die Trennung der Geräte sehen.
- Alarme einrichten – Sie können Schwellenwerte festlegen, die Alarme auslösen, wenn bei einer bestimmten Anzahl von Geräten die Verbindung unterbrochen wird. Alarme können Sie auch benachrichtigen, wenn ein oder mehrere Geräte aus einem bestimmten Grund die Verbindung trennen. Sie können sich dann detaillierte Gerätedaten ansehen, um Nachforschungen anzustellen und Fehler zu beheben.
- Jobs ausführen – Sie können Fernoperationen (wie Firmware-Updates) auf einem oder mehreren Geräten ausführen.

So funktioniert die Fleet-Hub-Datenindexierung

Sie können die Fleet-Hub-Konsole verwenden, um die Flottenindexierung für Ihre Geräteflotte zu aktivieren. Wenn Sie die Flottenindexierun in Fleet Hub aktivieren, aktivieren Sie sie für die gesamte Flotte und stellen sie allen Fleet-Hub-Anwendungen zur Verfügung.

Wenn sie aktiviert ist, indexiert die Fleet-Indexierung alle AWS IoT Core verwalteten Felder automatisch. Sie können die Flottenindexierung auch verwenden, um benutzerdefinierte Daten hinzuzufügen, mit denen Sie Daten in Fleet-Hub-Anwendungen abfragen und aggregieren können.

So funktionieren Fleet-Hub-Alarme

Fleet-Hub-Webanwendungen bieten eine Oberfläche, über die Ihre Benutzer Alarme erstellen können. Nachfolgend wird beschrieben, wie Benutzer Alarme in Fleet Hub erstellen.

1. Eine Abfrage zum Aggregieren von Daten erstellen – Legen Sie eine Abfrage fest, die die Geräte, auf die Ihre Benutzer abzielen möchten, mithilfe von durchsuchbaren Feldern aggregiert.
2. Schwellenwert konfigurieren – Legen Sie einen Schwellenwert fest, der Alarme auslöst, wenn ein Zustand in den indizierten Daten (z. B. der Verbindungsstatus über ein bestimmtes Intervall) erreicht wird.
3. Benachrichtigung konfigurieren – Geben Sie eine Gruppe von Empfängern an, die Fleet Hub benachrichtigt, wenn bei den angegebenen Geräten ein Alarm ausgelöst wird.

So funktionieren Fleet-Hub-Jobs

Sie können die Fleet-Hub-Konsole verwenden, um Fernoperationen auf Geräten auszuführen.

Wenn Jobvorlagen aktiviert sind, können Sie anhand der Vorlagen in Ihren Fleet-Hub-Anwendungen bestimmte Jobs erstellen.

Fleet Hub für AWS IoT Gerätemanagement für Administratoren

Dieser Abschnitt enthält Anleitungen für Administratoren zur Erstellung und Verwaltung von Fleet Hub for AWS IoT Device Management-Webanwendungen.

Themen

- Erste Schritte
- AWS und AWS IoT Core Dienste, die mit Fleet Hub for AWS IoT Device Management interagieren
- Fehlerbehebung

Erste Schritte

In diesem Abschnitt wird erklärt, wie Fleet Hub for AWS IoT Device Management-Webanwendungen erstellt und eingerichtet werden.

Themen

- Erstellen Sie Ihre erste Fleet-Hub-Anwendung.
- Verwaltung der Flottenindexierung für Fleet-Hub-Anwendungen
- Fügen Sie Benutzer zu Fleet-Hub-Anwendungen hinzu

Erstellen Sie Ihre erste Fleet-Hub-Anwendung.

Voraussetzungen

Die folgende Liste enthält die Ressourcen, die Sie zum Erstellen einer Fleet-Hub-Webanwendung benötigen.

- Ein AWS -Konto.
- AWS IAM Identity Center aktiviert für Ihr Konto. (Wenn Sie diesen Dienst noch nicht aktiviert haben, werden Sie von der AWS IoT Core Konsole (https://console.aws.amazon.com/iot/) dazu aufgefordert.)

Erstellen Sie Ihre erste Fleet-Hub-Anwendung.

In den folgenden Schritten wird beschrieben, wie Fleet Hub for AWS IoT Device Management-Webanwendungen erstellt werden.

1. Navigieren Sie zur AWS IoT Core Konsole (https://console.aws.amazon.com/iot/) und wählen Sie im linken Bereich Fleet Hub und dann Anwendungen aus.
2. Wählen Sie auf der Seite Anwendungen die Option Anwendung erstellen aus.
3. Wenn Sie AWS IAM Identity Center (IAM Identity Center) nicht aktiviert haben, folgen Sie auf der Seite „IAM Identity Center einrichten“ den Schritten zur Aktivierung. AWS Organizations sendet Ihnen eine E-Mail. Wählen Sie den Link in der E-Mail, um die Aktivierung von IAM Identity Center abzuschließen.

   > **Note**
   >
   > Sie können Ihren eigenen Identitätsanbieter mit IAM Identity Center verbinden. Weitere Informationen finden Sie unter Was ist AWS IAM Identity Center? und Connect zu Ihrem externen Identitätsanbieter her.
   > Wenn Sie eine Fleet Hub-Anwendung erstellen, müssen Sie eine Organisationsinstanz von IAM Identity Center erstellen, falls Sie noch keine haben. Die Fleet Hub-Anwendung, die Sie erstellen, muss sich ebenfalls in derselben Organisationsinstanz AWS-Region von IAM Identity Center befinden. Weitere Informationen finden Sie unter IAM Identity Center aktivieren und Organisationsinstanzen von IAM Identity Center.

   Auf der Seite erfahren Sie, ob Sie IAM Identity Center bereits aktiviert haben.

   Wählen Sie Weiter aus.
4. Lesen Sie auf der Seite AWS IoT Indexdaten die Informationen im Abschnitt So funktioniert der Datenfluss von AWS IoT zu Fleet Hub. Auf dieser Seite gelangen Sie zu den Seiten in der AWS IoT Core Konsole, auf denen Sie die AWS IoT Core Flottenindizierung aktivieren und verwalten können. Sie können diesen Dienst verwenden, um Ihre Registrierungsdaten, Schattendaten, Geräteverbindungsinformationen (Ereignisse im Gerätelebenszyklus) sowie Daten zu Geräteverletzungen zu indexieren, zu durchsuchen und zu aggregieren. Sie können zusätzlich zu den verwalteten Feldern, die bei der AWS IoT Core Flottenindizierung standardmäßig indexiert werden, auch benutzerdefinierte Felder erstellen.

- Wenn Sie die Flottenindexierung aktiviert haben, werden auf dieser Seite Ihre Flottenindexierungseinstellungen und benutzerdefinierten Felder angezeigt.

- Wenn Sie die Indexierung und Konnektivität von Dingen nicht aktiviert haben, müssen Sie dies tun, um Fleet Hub verwenden zu können.

Wenn Sie mit der Verwaltung und Überprüfung Ihrer Flottenindexierungseinstellungen fertig sind, wählen Sie Weiter.

Weitere Informationen zur Aktivierung der Flottenindexierung für Fleet-Hub-Anwendungen finden Sie unter Verwaltung der Flottenindexierung für Fleet-Hub-Anwendungen.

5. Erstellen Sie auf der Seite Anwendung konfigurieren im Abschnitt Anwendungsrolle eine neue Servicerolle oder wählen Sie eine vorhandene Servicerolle aus. Ihre Fleet-Hub-Webanwendung übernimmt diese Rolle, wenn sie Fleet-Hub-Ressourcen verwendet. Verbundbenutzer haben dieselben Berechtigungen wie die Rolle, wenn sie die Webanwendung verwenden.

   - Wenn Sie eine neue Rolle erstellen, muss der Rollenname mit der folgenden Zeichenfolge beginnen: `AWSIotFleetHub_`*`random_string`*.

   - Wenn Sie eine vorhandene Rolle auswählen, stellen Sie sicher, dass sie über die im Richtliniendokument aufgeführten Berechtigungen verfügt. Um die Berechtigungen zu sehen, die Ihre Fleet-Hub-Webanwendung benötigt, wählen Sie Rollendetails anzeigen. Es öffnet sich ein Fenster, in dem Ihnen das Richtliniendokument angezeigt wird, das der Service für jede neue Rolle gilt, die Sie auf dieser Seite erstellen.

6. Geben Sie auf der Seite Anwendung konfigurieren im Abschnitt Anwendungseigenschaften einen Namen für Ihre Anwendung ein. Optional können Sie auch eine Beschreibung eingeben.

   Wählen Sie Anwendung erstellen aus.

7. Wählen Sie auf der Registerkarte Anwendungen die Anwendung aus, die Sie in erstellt haben, und klicken Sie dann auf Details anzeigen. Überprüfen Sie die Details des Antrags.

> **Note**
>
> Weitere Informationen zu möglichen Lösungen für die Lösung von Problemen als Administrator von Fleet Hub finden Sie unter Problembehandlung.

Verwaltung der Flottenindexierung für Fleet-Hub-Anwendungen

Sie können die AWS IoT Core Konsole oder die verwenden, AWS CLI um die Flottenindizierung zu aktivieren und die folgenden Datenquellen für die Indizierung zu konfigurieren: AWS IoT Registrierungsdaten, AWS IoT Device Shadow-Daten, AWS IoT Konnektivitätsdaten und Daten zu AWS IoT Device Defender Verstößen. In den folgenden Schritten wird beschrieben, wie Sie die Flottenindizierung für Fleet Hub for AWS IoT Device Management-Anwendungen in AWS IoT Core der Konsole aktivieren. Eine Anleitung zur Verwendung AWS CLI finden Sie unter Verwaltung der Indizierung von Objekten.

> **Important**
>
> Am 20. Juli 2022 ist die allgemein verfügbare Version der Integration von AWS IoT Device Management Fleet Indexing mit AWS IoT Core Named Shadows und AWS IoT Device Defender Detect Verstößen verfügbar. Mit dieser GA-Version können Sie bestimmte benannte Schatten indizieren, indem Sie Schattennamen angeben. Wenn Sie Ihre benannten Schatten während der öffentlichen Vorschauphase dieser Funktion vom 30. November 2021 bis 19. Juli 2022 für die Indizierung hinzugefügt haben, empfehlen wir Ihnen, Ihre Einstellungen für die Flottenindexierung neu zu konfigurieren und spezifische Schattennamen auszuwählen, um die Indexierungskosten zu senken und die Leistung zu optimieren. Weitere Informationen zur Neukonfiguration Ihrer Flottenindexierungseinstellungen finden Sie unter Verwaltung der Flottenindexierung.

1. Navigieren Sie zur AWS IoT Core Konsole (https://console.aws.amazon.com/iot/) und wählen Sie im linken Bereich Einstellungen aus.
2. Navigieren Sie auf der Seite Einstellungen zum Abschnitt Flottenindexierung und wählen Sie dann Indexierung verwalten aus.
3. Wählen Sie auf der Seite Flottenindizierung verwalten im Abschnitt Konfiguration die Option Thing-Indizierung und die Datenquellen aus, die Sie indizieren AWS IoT möchten. Sie müssen die Ding-Indexierung und die Ding-Konnektivität aktivieren, um Fleet Hub verwenden zu können.

4. (Optional) Erstellen Sie auf der Seite Flottenindexierung verwalten im Abschnitt Benutzerdefinierte Felder für die Aggregation optional benutzerdefinierte Felder zusätzlich zu den verwalteten Feldern, die bei der Flottenindexierung standardmäßig indexiert werden.

   Wenn Sie mit der Verwaltung und Überprüfung Ihrer Flottenindexierungseinstellungen fertig sind, wählen Sie Weiter.

   Es kann einen Moment dauern, bis die Einstellungen für die Flottenindexierung aktualisiert sind. Weitere Informationen zur Verwaltung der Flottenindexierung finden Sie unter Verwaltung der Flottenindexierung.

Fügen Sie Benutzer zu Fleet-Hub-Anwendungen hinzu

Ihre Webanwendung Fleet Hub for AWS IoT Device Management enthält keine Benutzer, wenn sie neu erstellt wird. Sie müssen Benutzer hinzufügen, bevor Sie und Mitglieder Ihrer Organisation die Anwendung verwenden können. In den Schritten in diesem Thema wird beschrieben, wie Sie Benutzer zu Ihrer Anwendung hinzufügen.

Sie fügen Benutzer aus Ihrem vorhandenen Identitätssystem hinzu, indem Sie AWS IAM Identity Center (IAM Identity Center) für Ihr Konto einrichten. Sie können Ihren eigenen Identitätsanbieter mit IAM Identity Center verbinden. Weitere Informationen unter Was Ist IAM Identity Center?.

1. Wählen Sie auf der Seite Anwendungen Ihre Webanwendung aus der Fleet-Hub-Anwendungsliste aus. Wählen Sie die Option Details anzeigen aus.
2. Wählen Sie auf der Seite Details der Anwendung die Option Benutzer hinzufügen aus.
3. Wählen Sie im Fenster Fleet-Hub-Benutzer hinzufügen die Benutzer aus Ihrer Organisation aus, die Zugriff auf die Anwendung haben sollen. Wählen Sie Ausgewählte Benutzer hinzufügen.
4. Vergewissern Sie sich, dass Sie auf der Seite mit den Anwendungsdetails die von Ihnen ausgewählten Benutzer in der Fleet-Hub-Benutzer-Liste sehen.

AWS und AWS IoT Core Dienste, die mit Fleet Hub for AWS IoT Device Management interagieren

In diesem Thema wird erklärt, wie die Funktionen von Fleet Hub for AWS IoT Device Management mit anderen AWS Diensten interagieren, um die Funktionen in Ihren Fleet Hub-Webanwendungen bereitzustellen.

Die folgende Tabelle zeigt, welche AWS Dienste Fleet Hub for AWS IoT Device Management zur Implementierung der einzelnen Funktionen verwendet.

Funktion	AWS Dienst	Beschreibung
Integrieren Sie bestehende Identitätssysteme wie Active Directory.	AWS IAM Identity Center (IAM Identity Center)	Sie fügen Benutzer aus Ihrem vorhandenen Identitätssystem hinzu, indem Sie AWS IAM Identity Center (IAM Identity Center) für Ihr Konto einrichte n. Sie können Ihren eigenen Identitätsanbieter mit IAM Identity Center verbinden. Weitere Informationen finden Sie unter Was ist AWS IAM Identity Center? und Identität en der Belegschaft.
Erstellen Sie Abfragen mithilfe von AWS verwalteten Feldern, benutzerdefinierten Feldern und beliebigen Attributen in Ihren indizierten Datenquellen.	AWS IoT Flottenindizierung	Verwenden Sie den Flottenin dexdienst, um Ihre Registrie rungsdaten, Schattendaten und Geräteverbindungsd aten (Ereignisse im Geräteleb enszyklus) zu indexiere n, zu durchsuchen und zu aggregieren. Sie können zusätzlich zu den verwalteten Feldern, die von der AWS IoT Flottenindizierung standardm äßig indexiert werden, auch benutzerdefinierte Felder für die Aggregation erstellen. Weitere Informationen zur Flottenindexierung finden Sie unter Flottenindexierung.

Funktion	AWS Dienst	Beschreibung
Erstellen Sie Alarme für eine Reihe von Geräten, die in einer Abfrage angegeben wurden.	Amazon CloudWatch (CloudWatch)	Die Dashboards von Fleet Hub enthalten CloudWatch Kennzahlen, die Sie in Kombination mit durchsuchbaren Feldern verwenden können, um alarmierende Schwellenwerte festzulegen. Sie können beispielsweise einen CloudWatch Alarm einrichten, der eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung generiert, wenn die Anzahl der angeschlossenen Geräte eine bestimmte Menge unterschreitet. Weitere Informationen dazu CloudWatch finden Sie unter Was ist Amazon CloudWatch? Informationen darüber, wie das Erstellen von Metriken und Alarmen AWS IoT Core funktioniert, finden Sie unter Überwachen von AWS IoT Alarmen und Messwerten mithilfe von CloudWatch. CloudWatch

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung und zu möglichen Lösungen für Administratoren bei Problemen mit Fleet Hub.

Symptom	Lösung
Mein Link zur Webanwendung funktioniert nicht.	Es kann nach dem Erstellen eines Antrags einige Stunden dauern, bis der Link funktioniert.
Ich kann mich nicht bei meiner Webanwendung anmelden.	Stellen Sie sicher, dass Sie mindestens einen Benutzer zu Ihrer Anwendung hinzugefügt haben. Stellen Sie sicher, dass Ihre Rolle über die entsprechende Vertrauensbeziehung verfügt, z. B. die folgende: JSON `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` Weitere Informationen darüber, wie Sie die Vertrauensbeziehung in IAM bearbeiten können, finden Sie unter Bearbeiten der Vertrauensbeziehung für eine vorhandene Rolle.
Ich kann keine Webanwendung erstellen.	Stellen Sie sicher, dass Sie Ihr Limit für die Gesamtzahl der Webanwendungen nicht erreicht haben.

Symptom	Lösung
Ich sehe ein benutzerdefiniertes Feld nicht, das ich erwartet habe.	Stellen Sie sicher, dass die Flottenindexierung korrekt konfiguriert ist. Weitere Informationen zur Flottenindexierung finden Sie unter Flottenindexierung.

Fleet Hub für AWS IoT Gerätemanagement für Benutzer

Dieser Abschnitt enthält Informationen für Benutzer von Fleet Hub for AWS IoT Device Management-Webanwendungen. Weitere Informationen zum Hinzufügen von Benutzern zu Fleet-Hub-Webanwendungen finden Sie unter Fleet Hub für AWS IoT Gerätemanagement für Administratoren.

Themen

- Erste Schritte
- Abfragen und Filter
- Arbeiten mit Aufträgen und Auftragsvorlagen in Fleet Hub for AWS IoT Device Management
- Alarme
- Fehlerbehebung

Erste Schritte

Dieser Abschnitt enthält Informationen zu den ersten Schritten mit der Nutzung der Funktionen der Webanwendungen Fleet Hub for AWS IoT Device Management.

Themen

- Erstellen Ihrer ersten Abfrage
- Erstellen Ihres ersten Alarms
- Aufrufen von Gerätedetails

Erstellen Ihrer ersten Abfrage

In diesem Thema werden Sie Schritt für Schritt durch die Erstellung einer einfachen Fleet Hub for AWS IoT Device Management-Abfrage geführt. Abfragen werden mit einer Abfragesyntax angegeben.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die einem AWS IoT Core Konto zugeordnet ist, das Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das berechtigt ist, die Fleet-Hub-Anwendung zu verwenden.

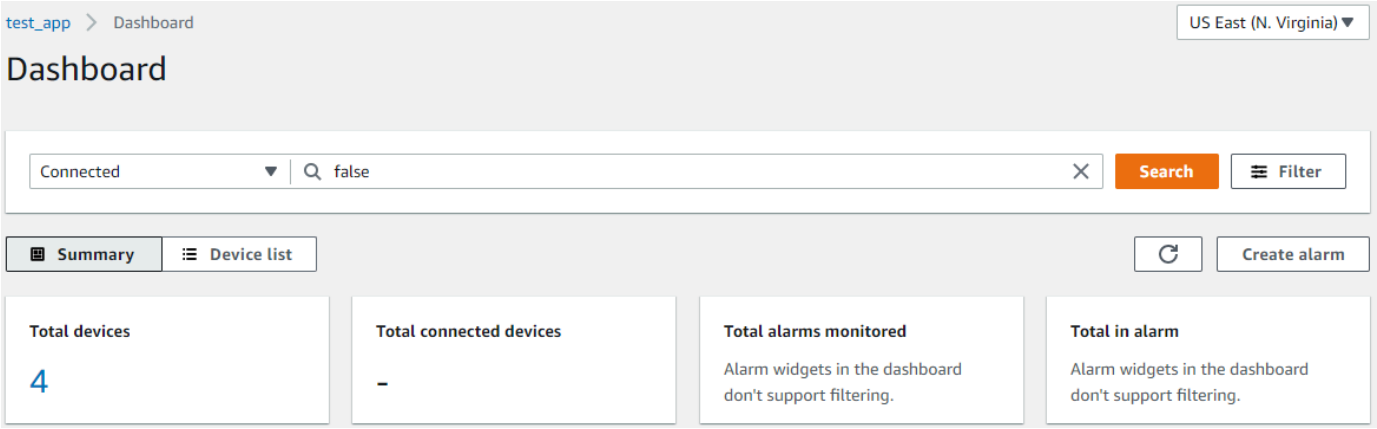
Erstellen Ihrer ersten Abfrage

Erstellen Ihrer ersten Abfrage

1. Navigieren Sie zu Ihrer Fleet-Hub-Anwendung.

   In der Standard-Dashboard-Ansicht wird eine Liste aller Geräte angezeigt, die die verwalteten und benutzerdefinierten Attribute enthält. Die Attribute, die das Attributpräfix enthalten, sind benutzerdefinierte Attribute.

2. Wählen Sie im Menü oben auf der Seite die Option Verbunden aus Alle Felder aus. Geben Sie **`false`** in das Textfeld neben dem Drop-down-Menü ein.



3. Um die Suche durchzuführen, wählen Sie Suchen. Sie sehen eine Liste aller Geräte, mit denen keine Verbindung besteht AWS IoT Core.

Weitere Informationen zur Abfragesyntax und Beispielabfragen finden Sie unter Abfragesyntax, Beispiel-Dingabfragen und Beispiel-Ding-Gruppen-Abfragen.

Erstellen Ihres ersten Alarms

In diesem Thema werden Sie Schritt für Schritt durch die Erstellung eines einfachen Alarms für Fleet Hub for AWS IoT Device Management geführt.

Voraussetzungen

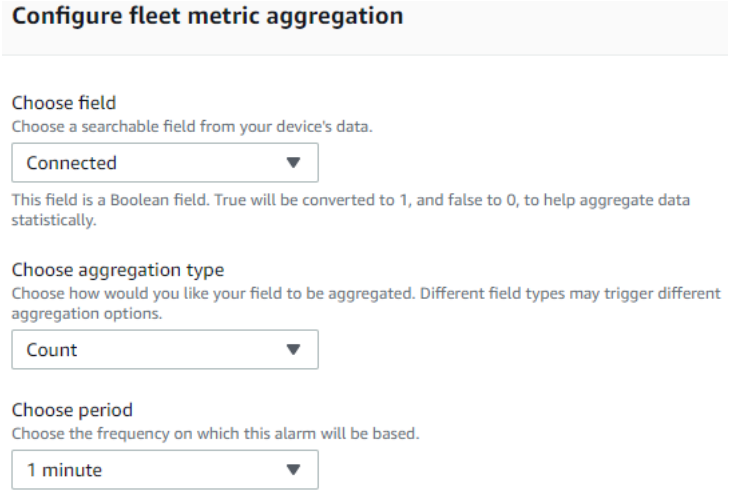
- Eine Fleet Hub-Anwendung, die einem AWS IoT Core Konto zugeordnet ist, das Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das berechtigt ist, die Fleet-Hub-Anwendung zu verwenden.

Erstellen Ihres ersten Alarms

Erstellen Ihrer ersten Abfrage

1. Navigieren Sie zu Ihrer Fleet-Hub-Anwendung.
2. Wenn Sie auf eine bestimmte Gruppe von Geräten abzielen möchten, erstellen Sie eine Abfrage. Eine Anleitung zur Erstellung eines Themas finden Sie unter the section called “Erstellen Ihrer ersten Abfrage”. Wenn Sie keine Abfrage erstellen, gilt Ihr Alarm für alle Geräte in Ihrer Flotte.
3. Wählen Sie auf der Standard-Dashboard-Seite die Option Alarm erstellen aus.
4. Vergewissern Sie sich, dass Ihre Abfrage auf der Seite Aggregationsmetrik erstellen unter Zielabfrage angezeigt wird. Wählen Sie im Abschnitt Flottenmetrikaggregation konfigurieren im Menü Feld auswählen die Option Verbunden aus. Dieses AWS verwaltete Feld gibt an, ob ein Gerät angeschlossen AWS IoT Core ist. Das Menü „Feld auswählen“ enthält die von AWS-verwalteten Felder und die benutzerdefinierten Felder, die Ihr Administrator bei der AWS IoT Flottenindizierung erstellt hat.
5. Wählen Sie unter Aggregationstyp eine der folgenden Optionen aus.
   - Maximum – Konfigurieren Sie einen maximalen Schwellenwert.
   - Anzahl – Konfigurieren Sie eine bestimmte Anzahl als Schwellenwert.
   - Summe – Konfigurieren Sie eine Summe als Schwellenwert.
   - Minimum – Konfigurieren Sie einen Mindestschwellenwert.
   - Durchschnitt – Konfigurieren Sie einen durchschnittlichen Schwellenwert.
6. Wählen Sie unter Zeitraum die Dauer der in den vorherigen Menüs angegebenen Bedingung aus, die den Alarm auslösen soll.

   Eine Beispieleinstellung für Aggregation von Flottenmetriken konfigurieren kann wie folgt aussehen:



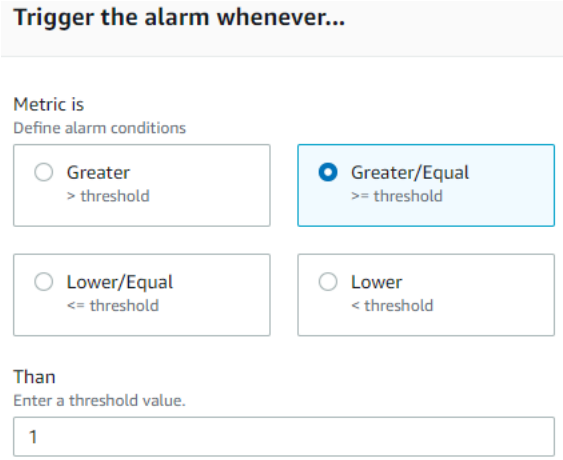
Wählen Sie Weiter aus.

7. Auf der Seite Schwellenwert festlegen unter Alarm auslösen, wenn … Wählen Sie im Abschnitt eine der folgenden Optionen aus.

   - Größer – Alarmiert, wenn die Aggregationsmetrik und der Aggregationstyp den angegebenen Wert überschreiten.
   - Größer/Gleich — Alarmt, wenn die Aggregationsmetrik und der Aggregationstyp dem angegebenen Wert entsprechen oder diesen überschreiten.
   - Niedriger – Alarmiert, wenn die Aggregationsmetrik und der Aggregationstyp unter den angegebenen Wert fallen.
   - Niedriger/Gleich — Alarmt, wenn die Aggregationsmetrik und der Aggregationstyp dem angegebenen Wert entsprechen oder ihn unterschreiten.

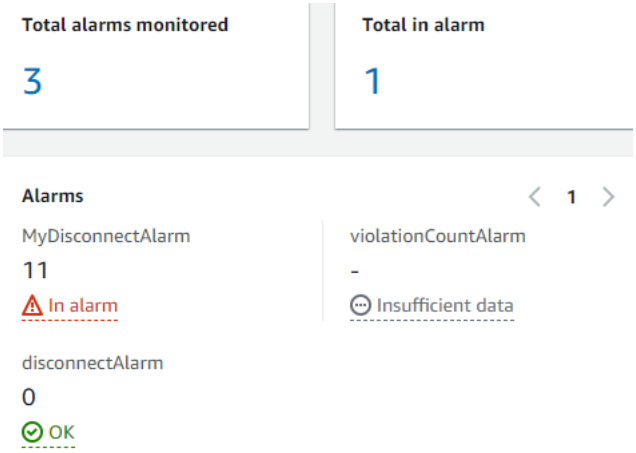
8. Geben Sie im Textfeld Als den Wert an, der als Schwellenwert für den Alarm verwendet werden soll.

   Eine Beispieleinstellung für Schwellenwert festlegen kann wie folgt aussehen:

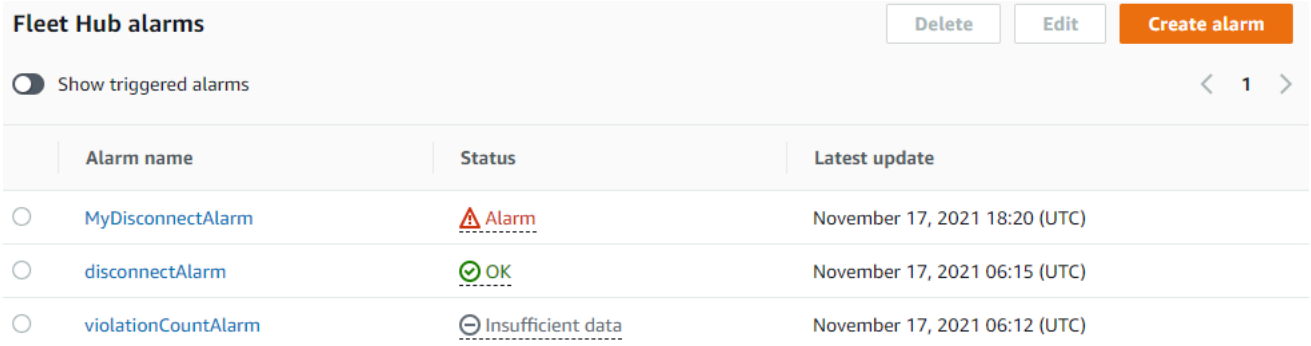


Wählen Sie Weiter aus.

9. Geben Sie auf der Seite Benutzer benachrichtigen im Abschnitt Benachrichtigen – optional einen Namen für die E-Mail-Liste ein, die die Benutzer in Ihrer Organisation enthält, die Benachrichtigungen erhalten, wenn der Alarm aktiv ist. Geben Sie eine durch Komma getrennte Liste der E-Mail-Adressen ein, um diese Liste zu füllen.
10. Geben Sie im Abschnitt Alarmdetails einen Namen für Ihren Alarm und optional eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Überprüfen und erstellen die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wählen Sie Absenden aus. Sie kehren zum Standard-Dashboard zurück.
12. Auf dem Standard-Dashboard zeigen die Alarm-Widgets Informationen zu allen Alarmen an, die Sie erstellt haben.



Um Details zu den von Ihnen erstellten Alarmen zu sehen, wählen Sie im linken Navigationsbereich Fleet-Hub-Alarme aus.



Aufrufen von Gerätedetails

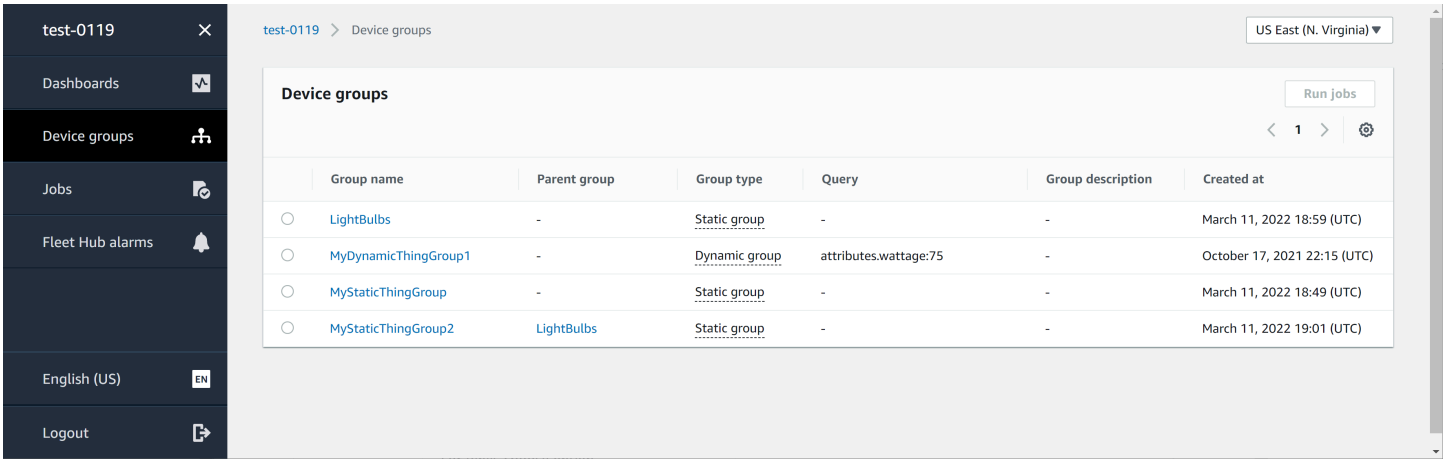
In diesem Thema erfahren Sie Schritt für Schritt, wie Sie Details zu Ihren Gerätegruppen und Ihren Geräten einsehen können.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die mit einem AWS IoT Core Konto verknüpft ist und Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das berechtigt ist, die Fleet-Hub-Anwendung zu verwenden.

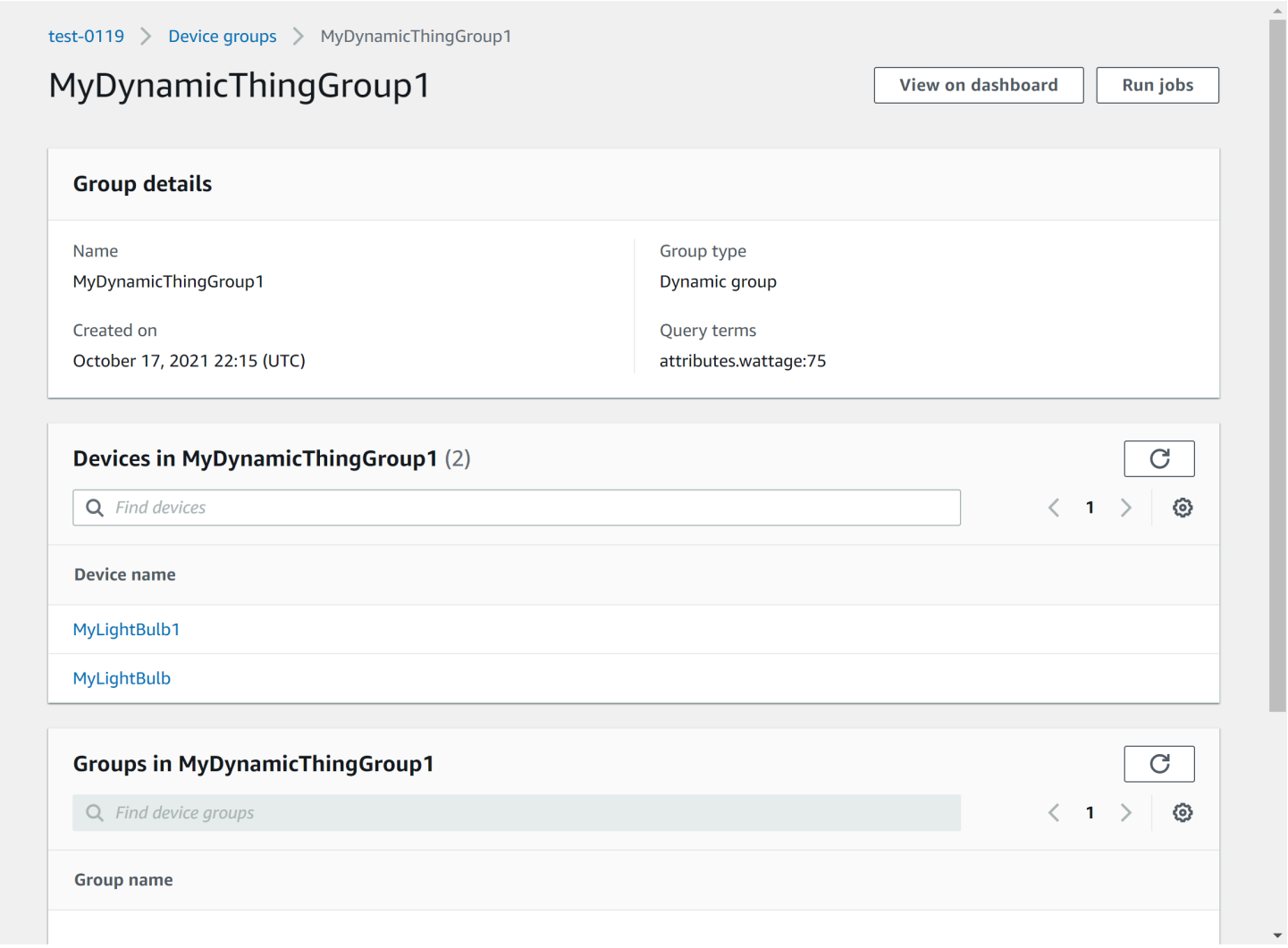
Gerätegruppen

Wenn Sie sich bei Ihrer Fleet-Hub-Webanwendung anmelden, sehen Sie Gerätegruppen im linken Navigationsbereich. Auf der Seite Gerätegruppen werden alle Gerätegruppen in Ihrer Fleet-Hub-Webanwendung aufgeführt. Um die Details einer Gerätegruppe anzuzeigen, wählen Sie eine bestimmte Gerätegruppe aus der Spalte Gruppenname aus.



Details zur Gerätegruppe

Die Seite mit den Gerätegruppendetails enthält Informationen zu Ihrer ausgewählten Gerätegruppe. Um die Details eines Geräts anzuzeigen, wählen Sie im ***XXX*** Abschnitt Geräte in der Spalte Gerätename ein bestimmtes Gerät aus.



Gerätedetails

Die Seite mit den Gerätegruppendetails enthält Informationen zu Ihrer ausgewählten Gerätegruppe.

> **Note**
>
> Wenn Ihr Kunde eine andere Client-ID als Thing Name verwendet AWS IoT, um eine Verbindung herzustellen, wird der Verbindungsstatus Ihres „Dings“ nicht von Fleet Indexing indexiert.

Details

Der Abschnitt Details enthält die folgenden Informationen zu Ihrem Gerät:

- Gerätename – Der Name der Ding-Ressource, die für Ihr Gerät steht. Weitere Informationen finden Sie unter So verwalten Sie Dinge mit der Registrierung.
- Dingtyp – Der Ding-Typ, der Ihrem Gerät zugeordnet ist. Sie können den Ding-Typ verwenden, um Informationen zu speichern, die allen Dingen desselben Ding-Typs gemeinsam sind. Weitere Informationen finden Sie unter API-Typen.
- Zeitstempel der letzten Verbindung — Der Zeitstempel, zu dem Ihr Gerät zuletzt eine Verbindung hergestellt hat. AWS IoT
- Link zum gemeinsam nutzbaren Gerät – Ein gemeinsam nutzbarer Link, der auf die Seite mit den Gerätedetails des ausgewählten Geräts verweist.
- Letzter Verbindungsstatus — Der Verbindungsstatus Ihres Geräts zu. AWS IoT Wenn Ihr Gerät verbunden ist, ist der Wert `true`. Wenn es nicht verbunden ist, ist der Wert `false`.
- Grund der Trennung – Der Grund, warum Ihr Gerät getrennt wurde.

Gemeldete Daten

Der Abschnitt Gemeldete Daten enthält Informationen zu den Registrierungsdaten, Geräteshadowdaten und Dinggruppen Ihres Geräts.

- Gerätefelder — Die indizierten Felder Ihres Geräts bei der AWS IoT Flottenindizierung. Weitere Informationen finden Sie unter Verwalten der Flottenindexierung.
- Geräteschatten – Die Schatten, die Ihrem Gerät zugeordnet sind. Die Geräteschatten können sowohl klassische unbenannte Schatten als auch benannte Schatten enthalten. Weitere Informationen finden Sie unter AWS IoT Geräteschatten.

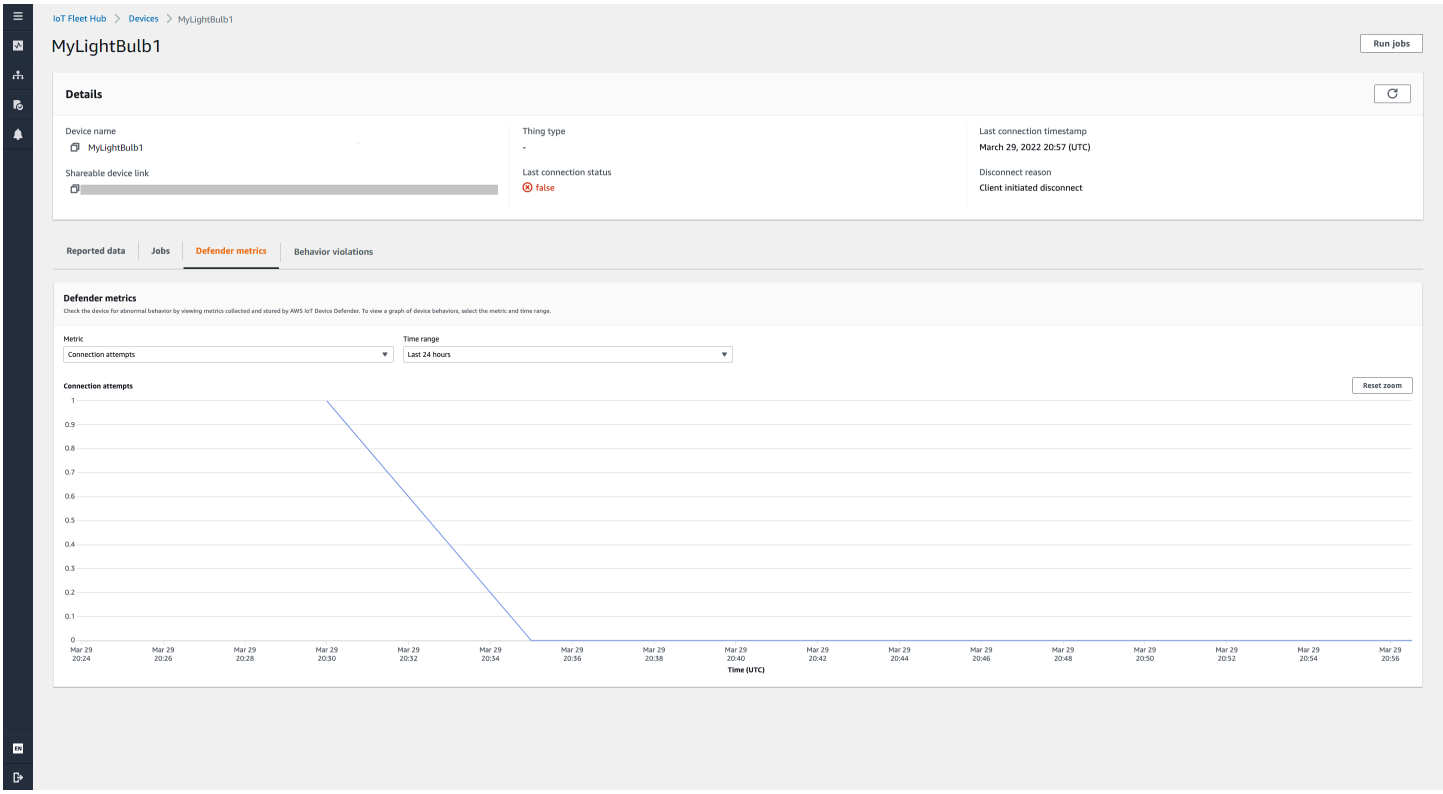
- Gerätegruppen – Die Gerätegruppen, die Ihrem Gerät zugeordnet sind. Die Gerätegruppen können sowohl statische als auch dynamische Ging-Gruppen umfassen. Weitere Informationen zu Objektgruppen finden Sie Statische Ding-Gruppen and Dynamische Ding-Gruppen.

Aufträge

Im Bereich Jobs werden alle Jobs angezeigt, die auf dem Gerät ausgeführt werden. Jeder Job hat eine Detailseite, auf der zusammenfassende Informationen über den Job, einschließlich Ziel- und Laufzeitinformationen, angezeigt werden. Weitere Informationen finden Sie unter Arbeiten mit Aufträgen und Auftragsvorlagen in Fleet Hub für AWS IoT Geräteverwaltung und Jobs.

Defender-Metriken

Im Bereich AWS IoT Device Defender Defender-Metriken werden Messwerte angezeigt, die mit Ihrem aktuell ausgewählten Gerät verknüpft sind. Sie können die angezeigten Metrikdaten verwenden, um den Betrieb Ihres Geräts über einen von Ihnen ausgewählten Zeitraum zu visualisieren. Um die Defender-Metrikdaten in Ihrer Fleet-Hub-Anwendung anzuzeigen, muss Ihr Fleet Hub-Administrator zunächst AWS IoT Device Defender -Messwerte einrichten, die dem ausgewählten Gerät zugeordnet sind. Weitere Informationen zum Erstellen und Einrichten von AWS IoT Device Defender Metriken für Ihre Geräte finden Sie unter Benutzerdefinierte Metriken, Geräteseitige Metriken und Cloud-seitige Metriken.



Verhaltensverstöße

Im Abschnitt Verhaltensverstöße werden die indexierten Daten AWS IoT Device Defender zur Erkennung von Verstößen angezeigt, die Ihrem aktuell ausgewählten Gerät zugeordnet sind. Die Daten zu Verhaltensverstößen können die Anzahl der Verstöße, den Zeitpunkt des letzten Verstoßes und den Metrikwert des letzten Verstoßes umfassen. Um die Daten zu Verhaltensverstößen in Ihrer Fleet Hub-Anwendung einzusehen, sollte Ihr Fleet Hub-Administrator AWS IoT Device Defender Verhaltensverletzungen in einem Sicherheitsprofil einrichten und Verstöße in der AWS IoT Device Defender Flottenindizierung konfigurieren. Weitere Informationen zum Einrichten von Verhaltensverstößen in einem AWS IoT Device Defender Sicherheitsprofil finden Sie unter AWS IoT Device Defender Erkennen. Weitere Informationen zur Konfiguration von AWS IoT Device Defender -Verstößen finden Sie unter Verwaltung der Flottenindizierung für Fleet-Hub-Anwendungen und Verwaltung der Ding-Indexierung.

Abfragen und Filter

Sie können Fleet Hub for AWS IoT Device Management-Abfragen verwenden, um Listen mit Dingen in Ihrer Geräteflotte zu erstellen und anzuzeigen. Alle AWS verwalteten Felder, benutzerdefinierten Felder und alle Attribute in Ihren indizierten Datenquellen stehen Ihnen als Abfragefilter zur Verfügung. Mithilfe AWS IoT der Flottenindizierung können Sie auch benutzerdefinierte Felder erstellen, für die die Aggregation aktiviert the section called “Alarme” werden soll. Weitere Informationen zur Flottenindexierung finden Sie unter Flottenindexierung.

Themen

- Dashboard anzeigen
- Erstellen Sie Abfragen mit Filtern

Dashboard anzeigen

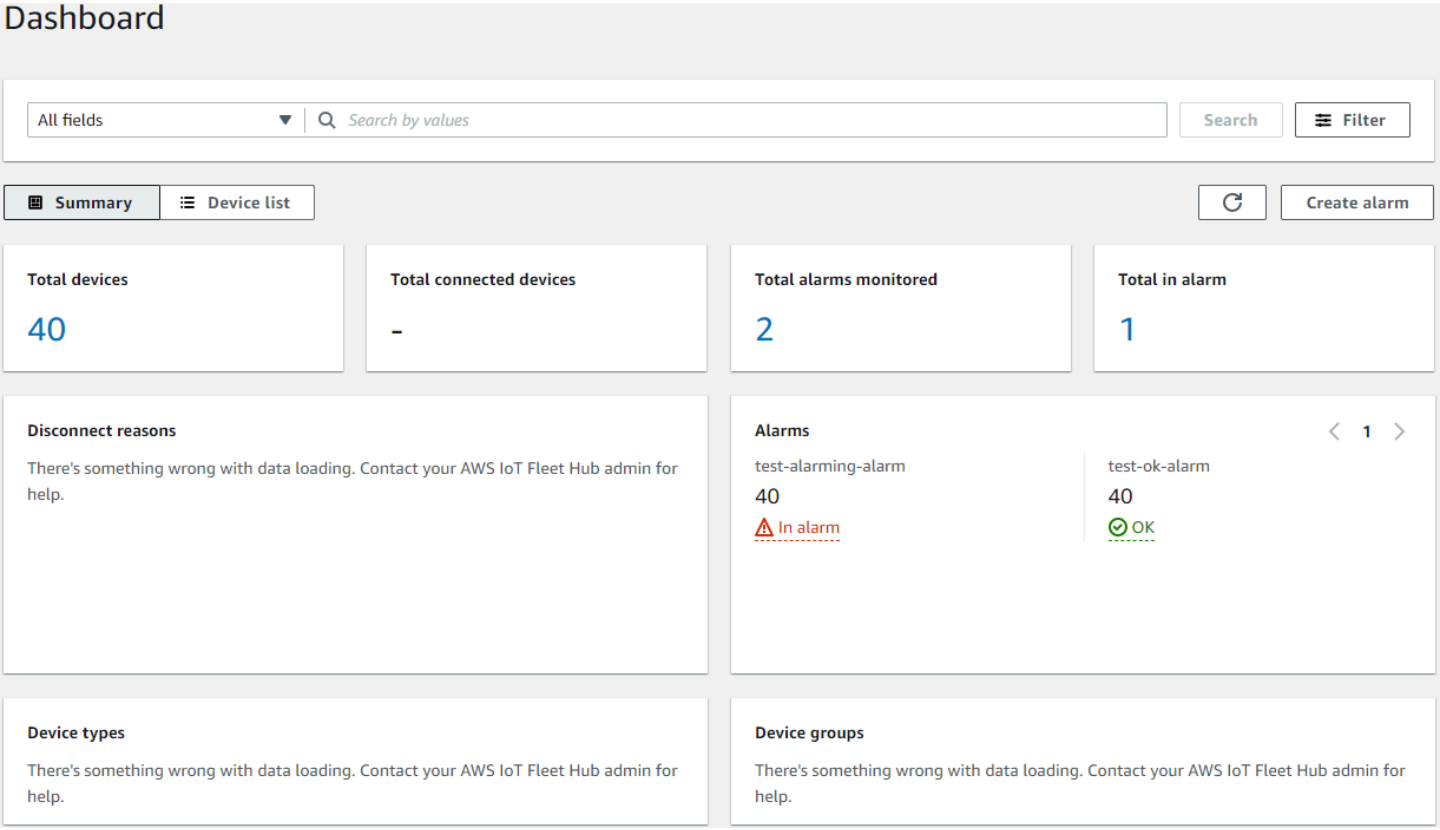
Wenn Sie sich bei Ihrer Webanwendung Fleet Hub for AWS IoT Device Management anmelden, sehen Sie ein Dashboard, das Daten zu den Geräten in Ihrer Flotte in zwei Ansichten anzeigt.

Übersicht

In der Ansicht Übersicht wird eine zusammengefasste Ansicht der Daten zu allen Geräten in Ihrer Flotte angezeigt. Es enthält die folgenden Informationen.

- Anzahl der Geräte

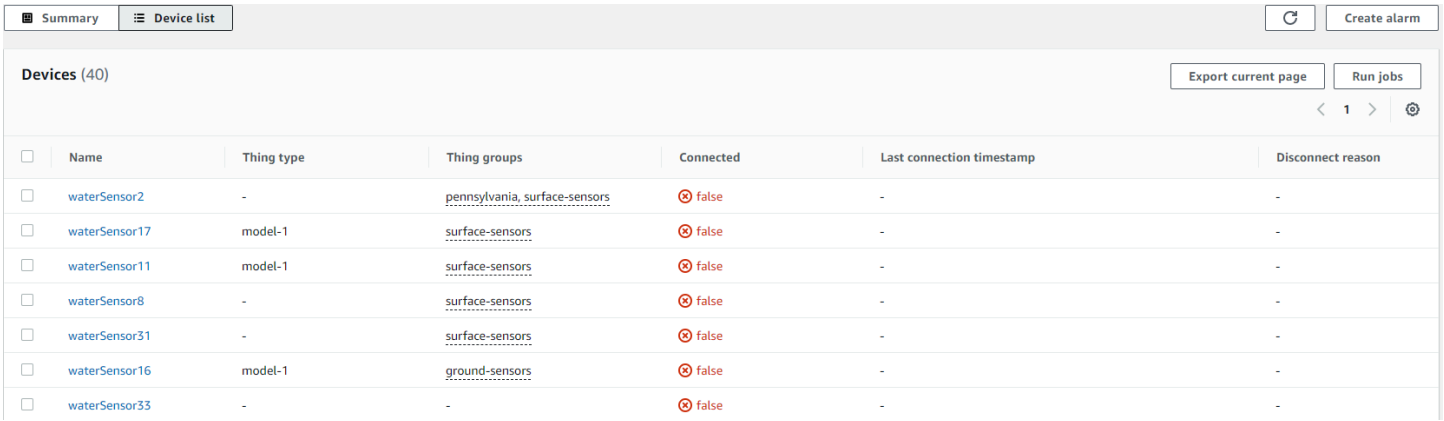
- Anzahl der verbundenen Geräte
- Eine Liste der Gründe, warum die Verbindung zu Geräten unterbrochen wurde
- Die Objekttypen, die Sie für Ihre Flotte erstellt haben, und die Anzahl der Geräte für jeden Typ
- Die Objekttypen, die Sie für Ihre Flotte erstellt haben, und die Anzahl der Geräte in jeder Gruppe



Geräteliste

In der Ansicht Geräteliste wird eine Tabelle angezeigt, in der die Geräte in Ihrer Flotte aufgeführt sind. Die Tabelle bietet die folgenden Informationen für jedes Gerät in der Liste.

- Der Gerätename
- Der Verbindungsstatus des Geräts
- Der Zeitstempel für die letzte Verbindung des Geräts
- Für ein Gerät, das nicht verbunden ist; der Grund, warum die Verbindung unterbrochen wurde
- Der Ding-Typ des Geräts
- Die Ding-Gruppe des Geräts
- Die benutzerdefinierten Felder, die Sie im Flottenindexdienst erstellt haben



Um eine CSV-Datei herunterzuladen, die die auf der Seite angezeigten Geräte enthält, wählen Sie in der Geräteliste die Option Aktuelle Seite exportieren. Beachten Sie, dass bei einer paginierten Liste nur Daten heruntergeladen werden, die auf der aktuellen Seite angezeigt werden, nicht auf nachfolgenden Seiten.

Sie können Abfragen und Filter verwenden, um die Anzahl der Geräte einzuschränken, die die Übersichtsdaten in der ersten Ansicht generieren und in der Geräteliste angezeigt werden. Weitere Informationen zur Verwendung von Abfragen und Filtern, um genauere Informationen zu Geräten in Ihrer Flotte zu erhalten, finden Sie unter the section called “Abfragen erstellen”.

Erstellen Sie Abfragen mit Filtern

In diesem Thema wird erklärt, wie Fleet Hub for AWS IoT Device Management-Abfragen funktionieren, und Sie werden durch die Schritte geführt, die zum Erstellen einer Abfrage mit Filtern erforderlich sind.

Mithilfe von Abfragen können Sie die Anzahl und die Typen der Geräte steuern, die in Ihren Übersichts- und Listenansichten auf Ihrem Dashboard angezeigt werden. Sie filtern Abfragen mithilfe von AWS verwalteten Feldern, benutzerdefinierten Feldern und beliebigen Attributen aus Ihren indizierten Datenquellen aus der AWS IoT Flottenindizierung. Weitere Informationen zur Flottenindexierung finden Sie unter Flottenindexierung.

Sie können auch Schlüsselwörter zu Ihren Abfragen hinzufügen. Schlüsselwörter gelten für alle durchsuchbaren Felder. Sie werden auch auf die Obergrenze von drei Filtern angerechnet, die Sie in einer einzigen Abfrage anwenden können.

Im folgenden Abschnitt werden die Schritte beschrieben, die zum Erstellen einer typischen Abfrage erforderlich sind.

Abfragen erstellen

In den folgenden Schritten wird erklärt, wie eine typische Abfrage erstellt wird.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die mit einem AWS IoT Core Konto verknüpft ist und mehrere Geräte (Dinge) enthält
- Ein Konto, das berechtigt ist, die Fleet-Hub-Anwendung zu verwenden.

Erstellen Sie Ihre erste Fleet-Hub-Abfrage mit einem Filter in der Konsole.

1. Navigieren Sie zu Ihrer Fleet-Hub-Anwendung.
2. Vergewissern Sie sich, dass Sie auf dem Standard-Dashboard die Registerkarte Geräteliste und die Gesamtzahl der Geräte (Dinge) im AWS IoT Core Partnerkonto sehen können.
3. Wählen Sie im Standard-Dashboard die Registerkarte Geräteliste. Vergewissern Sie sich, dass Sie eine Liste aller Geräte sehen, die die verwalteten und benutzerdefinierten Attribute enthalten. Die benutzerdefinierten Attribute enthalten das Attribut-Präfix.
4. Geben Sie oben auf der Seite ein beliebiges Schlüsselwort ein, das Sie in die Abfrage aufnehmen lassen möchten. Stichwortabfragen gelten für alle Felder.
5. Wählen Sie oben auf der Seite Filter.
6. Wählen Sie im Filter-Modal unter Feld das Feld aus, das Sie als Filter verwenden möchten. Wählen Sie unter Operator eine Option aus. Wählen Sie abschließend unter Wert den Feldwert aus, der in Ihrem Filter verwendet werden soll.

   Sie können bis zu drei Filter hinzufügen. Eine Stichwortabfrage wird auf diese Zahl angerechnet.
7. Um Ihre Abfrage durchzuführen, wählen Sie Filter anwenden. In den Ergebnissen werden alle Geräte angezeigt, die Ihrer Abfrage entsprechen.

Arbeiten mit Aufträgen und Auftragsvorlagen in Fleet Hub for AWS IoT Device Management

> **Note**
>
> Die Funktion Jobvorlagen befindet sich in der Vorschau und unterliegt möglichen Änderungen.

Ein Job ist eine Remote-Operation, die an ein oder mehrere mit AWS IoT verbundene Geräte gesendet und dort ausgeführt werden. Sie können beispielsweise einen Auftrag definieren, der eine Reihe von Geräten anweist, Anwendungs- oder Firmware-Updates herunterzuladen und zu installieren, einen Neustart vorzunehmen, die Zertifikate zu rotieren oder Remote-Fehlerbehebungsvorgänge auszuführen. Sie können vorkonfigurierte Jobs von Fleet Hub for AWS IoT Device Management-Webanwendungen aus ausführen. Die Administratoren Ihres Unternehmens erstellen Jobvorlagen in der AWS IoT Konsole und fügen Richtlinien hinzu, die die Vorlagen für Fleet Hub-Benutzer verfügbar machen. In Ihrer Fleet-Hub-Anwendung geben Sie die Geräte oder eine Gerätegruppe an, auf denen der Job ausgeführt wird.

Administratoren erstellen auch Gerätegruppen, die Sie in Ihrer Anwendung anzeigen können. Um die Gruppen anzuzeigen, wählen Sie im Navigationsbereich Gerätegruppen aus. Wenn Sie eine Gerätegruppe als Ziel angeben, können Sie eine der folgenden zwei Arten von Optionen für die Ausführung des Jobs angeben.

- Snapshot: Der Job wird einmal ausgeführt.
- Kontinuierlich: Nach der ersten Ausführung wird der Job auf jedem Gerät ausgeführt, das der Gruppe hinzugefügt wurde.

Weitere Informationen zum Anlegen und Verwalten von Auftragsvorlagen finden Sie unter Jobvorlagen. Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Jobs.

Ausführen von Aufgaben

Sie können einen Job in einer Fleet-Hub-Anwendung von mehreren Standorten aus ausführen, aber die folgenden Schritte sind immer dieselben.

1. Wählen Sie eine Gruppe oder ein oder mehrere Geräte als Ziel aus.
2. Wählen Sie Auftrag ausführen aus.
3. Wählen Sie unter Jobzielauswahl entweder kontinuierlich oder Snapshot aus.
4. Wählen Sie eine Jobvorlage aus. Vergewissern Sie sich, dass der Text unter Jobübersicht den Jobtyp beschreibt, den Sie ausführen möchten.
5. Geben Sie optional einen Namen für die Aufgabe ein.
6. Wählen Sie Ausführen aus.

Sie können Ziele auswählen und diese Schritte von den folgenden Stellen in Ihrer Fleet-Hub-Anwendung aus ausführen.

- Die Registerkarte Geräteliste auf dem Dashboard.
- Die Detailseite eines bestimmten Geräts.
- Seite Gerätegruppen
- Die Detailseite eines bestimmten Geräts.

Anzeigen und Verwalten von Jobs

Sie können Jobs, die in Ihrer Flotte ausgeführt werden, an den folgenden Orten sehen.

- Die Seite mit der Jobliste – Auf dieser Seite werden alle Jobs angezeigt, die in Ihrer Flotte ausgeführt werden. Um diese Seite zu sehen, wählen Sie im Navigationsbereich Jobs aus.
- Die Detailseite für ein bestimmtes Gerät – Auf dieser Seite werden alle Jobs angezeigt, die auf dem Gerät ausgeführt werden.

Jeder Job hat eine Detailseite, auf der zusammenfassende Informationen über den Job, einschließlich Ziel- und Laufzeitinformationen, angezeigt werden. Auf dieser Seite wird der Laufzeitstatus des Jobs auf jedem Gerät angezeigt. Außerdem werden die folgenden Gesamtwerte angezeigt.

- Anzahl der Läufe.
- Anzahl der stornierten Läufe.
- Anzahl erfolgreicher Läufe.
- Anzahl der fehlgeschlagenen Läufe.

- Anzahl der abgelehnten Läufe.
- Anzahl der Läufe in der Warteschlange.
- Anzahl der aktiven Läufe.
- Anzahl der abgelehnten Läufe.
- Anzahl der Läufe mit Zeitüberschreitung.

Um einen Job abzubrechen, wählen Sie den Job aus und klicken Sie auf Abbrechen.

Alarme

In diesem Abschnitt wird erklärt, wie Fleet Hub for AWS IoT Device Management-Alarme funktionieren, und Sie werden durch die Schritte geführt, die zum Erstellen eines Alarms erforderlich sind.

Wenn Sie einen Fleet-Hub-Alarm erstellen, gilt dieser für alle Geräte, die derzeit in Ihrem Dashboard angezeigt werden. Wenn Sie keine Abfrage stellen, gilt der Alarm für alle Geräte in Ihrer Flotte. Weitere Informationen zur Verwendung Ihres Dashboards und zum Erstellen von Abfragen finden Sie unter the section called “Abfragen und Filter”.

Alarme verwenden Amazon CloudWatch (CloudWatch) -Metriken in Kombination mit durchsuchbaren Feldern aus dem AWS IoT Flottenindexdienst, um Alarme zu erstellen CloudWatch . Sie können zum Beispiel einen Alarm erstellen, der eine Amazon-SNS-Nachricht (Amazon Simple Notification Service) generiert, sobald der durchschnittliche Akkuladestand der Geräte Ihrer Flotte unter 50 % fällt.

Fleet Hub-Alarme nutzen die GetPercentilesFunktionen GetStatisticsund Funktionen des Flottenindexierungsdienstes, um aggregierte Daten abzufragen. Wenn Sie beispielsweise einen Alarm erstellen, der ein benutzerdefiniertes numerisches Feld verfolgt, können Sie Alarmschwellenwerte erstellen, die für die folgenden Werte des angegebenen Attributs gelten.

- Maximum
- Anzahl
- Summe
- Minimum
- Durchschnitt
- Werte im 10., 50., 90., 95. oder 99. Perzentil

Weitere Informationen zum Abfragen aggregierter Daten im Fleet Indexing Service finden Sie unter Abfragen aggregierter Daten.

In der folgenden Tabelle sind einige Beispiele für Aggregationstypen aufgeführt, die für AWS-verwaltete und benutzerdefinierte Felder verfügbar sind.

Feld	Aggregationstyp
Ding-Typ (AWS-verwaltetes Zeichenkettenfeld)	Anzahl
Ding-Gruppe (AWS-verwaltetes Zeichenke ttenfeld)	Anzahl
Verbunden (AWS-verwaltetes boolesches Feld) Der Wert von `true` ist 1. Der Wert von `false` ist 0.	• Maximum • Anzahl • Summe • Minimum • Durchschnitt
shadow.reported d.batterylevel (numerisches Aggregationsfeld, das im Flottenindexdienst erstellt wurde)	• Maximum • Anzahl • Summe • Minimum • Durchschnitt • 10. Perzentil (P10) • 50. Perzentil (P50) • 90. Perzentil (P90) • 95. Perzentil (P95) • 99. Perzentil (P99)

Zusätzlich zur Angabe von Aggregationsfeldern und -typen geben Sie auch die folgenden Werte an.

- Die Zeitdauer (1 Minute oder 5 Minuten), die der angegebene Alarmschwellenwert benötigt, um den Alarm auszulösen.

- Einer der folgenden Vergleichsoperatoren, der auf das angegebene Aggregationsfeld und den angegebenen Aggregationstyp angewendet werden soll.
  - Größer
  - Größer/Gleich
  - Geringer
  - Geringer/Gleich
- Der Wert, der mit dem angegebenen Vergleichsoperator verwendet werden soll.
- Eine Liste mit E-Mail-Adressen von Personen in Ihrer Organisation, die Amazon-SNS-Nachrichten erhalten, wenn Ihr Alarm ausgelöst wird.
- Ein Alarmname.

Informationen zum Erstellen eines Fleet-Hub-Alarms finden Sie unter the section called “Erstellen von Alarmen”.

Erstellen von Alarmen

Dieses Thema führt Sie durch die Schritte, die zum Erstellen eines Fleet Hub-Alarms für die AWS IoT Geräteverwaltung erforderlich sind. Es wird davon ausgegangen, dass Ihr Administrator aus einem Geräteschattenfeld mit dem Namen shadow.reported d.batterylevel ein Aggregationsfeld erstellt hat. Dieses benutzerdefinierte Feld gibt den Akkuladestand eines Geräts an. Sie müssen Ihren Administrator bitten, durchsuchbare benutzerdefinierte Felder im AWS IoT Flottenindexdienst zu erstellen.

Der Alarm, den Sie erstellen, sendet eine Nachricht über Amazon Simple Notification Service (Amazon SNS) an eine Liste von Personen in Ihrer Organisation, wenn der durchschnittliche Akkuladestand der Geräte in Ihrer Flotte innerhalb von 1 Minute unter 50 % fällt.

Erstellen Sie eine Fleet-Hub-Abfrage

1. Navigieren Sie zu Ihrer Fleet-Hub-Anwendung.
2. Wenn Sie auf eine bestimmte Gruppe von Geräten abzielen möchten, erstellen Sie eine Abfrage. Eine Anleitung zur Erstellung eines Themas finden Sie unter the section called “Erstellen Sie Abfragen mit Filtern”. Wenn Sie keine Abfrage erstellen, gilt Ihr Alarm für alle Geräte in Ihrer Flotte.
3. Wählen Sie auf der Standard-Dashboard-Seite die Option Alarm erstellen aus.

4. Vergewissern Sie sich, dass Ihre Abfrage auf der Seite Aggregationsmetrik erstellen unter Zielabfrage angezeigt wird. Wählen Sie im Abschnitt Flottenmetrikaggregation konfigurieren für Feld auswählen die Option shadow.reported d.batterylevel aus. Dieses Menü enthält die AWS verwalteten Felder und die benutzerdefinierten Felder, die Ihr Administrator im AWS IoT Flottenindexdienst erstellt hat.
5. Wählen Sie für Aggregationstyp wählen die Option Durchschnitt aus Bei dieser Auswahl wird der Alarm auf der Grundlage des durchschnittlichen Akkustands in Ihrer Geräteflotte ausgelöst.
6. Wählen Sie unter Zeitraum wählen die Option 1 Minute aus. Dadurch wird der Alarm ausgelöst, wenn sich Ihre Geräteflotte eine Minute lang im angegebenen Alarmzustand befindet.

   Wählen Sie Weiter.
7. Auf der Seite Schwellenwert festlegen unter Alarm auslösen, wenn ... Wählen Sie im Abschnitt Geringer/Gleich aus. Dadurch wird der Alarm ausgelöst, wenn der durchschnittliche Akkustand unter einen von Ihnen angegebenen Wert fällt.
8. Geben Sie 50 in das Than Textfeld ein.

   Wählen Sie Weiter.
9. Geben Sie auf der Seite Benutzer benachrichtigen im Abschnitt Benachrichtigen – optional einen Namen für die E-Mail-Liste ein, die die Benutzer in Ihrer Organisation enthält, die Benachrichtigungen erhalten, wenn der Alarm aktiv ist. Geben Sie eine durch Komma getrennte Liste der E-Mail-Adressen ein, um diese Liste zu füllen.
10. Geben Sie im Abschnitt Alarmdetails einen Namen für Ihren Alarm und optional eine Beschreibung für Ihren Alarm ein. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Überprüfen und erstellen die Informationen, die Sie auf den vorherigen Seiten eingegeben oder ausgewählt haben. Wählen Sie Absenden aus. Sie kehren zum Standard-Dashboard zurück.
12. Wählen Sie auf dem Standard-Dashboard im linken Navigationsbereich die Option Fleet-Hub-Alarme aus. Vergewissern Sie sich, dass der von Ihnen erstellte Alarm angezeigt wird.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung und zu möglichen Lösungen für Administratoren bei Problemen mit Fleet Hub.

Symptom	Lösung
Ich kann meiner Anfrage keine weiteren Filter oder Begriffe hinzufügen.	Stellen Sie sicher, dass Sie das Limit von vier Abfragebegriffen und Filtern nicht erreicht haben.
Ich kann keine benutzerdefinierte Metrik finden.	Bitten Sie Ihren Administrator, die Metrik im Fleet Indexing Service zu erstellen.
Mein Alarm zeigt keine Daten an.	Das Laden der Alarmdaten nimmt einige Minuten in Anspruch.
Ich muss die Geräte, auf die mein Alarm abzielt, ändern.	Gehen Sie zu Ihrem Dashboard und ändern Sie die Abfrage.
Ich sehe eine Fehlermeldung, wenn ich die Region in meinem Dashboard ändere.	Bitten Sie Ihren Administrator, sicherzustellen, dass die Flottenindizierung in der von Ihnen ausgewählten Region aktiviert ist.
Der Konnektivitätsstatus meines „Dings“ wird nicht von Flottenindexierung indexiert.	Stellen Sie sicher, dass Ihr Client dieselbe Client-ID wie den Thing-Namen verwendet , wenn er eine Verbindung herstellt AWS IoT. Wenn Ihr Kunde eine andere ID als den Dingnamen verwendet AWS IoT, um eine Verbindung herzustellen, wird der Verbindun gsstatus Ihres „Dings“ nicht von Fleet Indexing indexiert.

Überwachung von Fleet Hub für AWS IoT Gerätemanagement

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Fleet Hub und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Fleet Hub zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen.

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

- Protokollierung von API-Aufrufen von Fleet Hub for AWS IoT Device Management mit AWS CloudTrail

Protokollierung von API-Aufrufen von Fleet Hub for AWS IoT Device Management mit AWS CloudTrail

Fleet Hub for AWS IoT Device Management ist integriert in AWS CloudTrail. Der CloudTrail Service bietet eine Aufzeichnung der Aktionen, die ein Benutzer, eine Rolle oder ein AWS Dienst in Fleet Hub ausführt. CloudTrail erfasst alle API-Aufrufe für Fleet Hub als Ereignisse. Zu den aufgezeichneten Aufrufen gehören Aufrufe über die Fleet-Hub-Konsole und Codeaufrufe der Fleet-Hub-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Fleet Hub. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der CloudTrail gesammelten Informationen können Sie die Anfrage, die an Fleet Hub gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage wann gestellt hat und weitere Einzelheiten ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Fleet Hub in CloudTrail

AWS CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in Fleet Hub eine CloudTrail Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Fleet Hub, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon Simple Storage Service (Amazon S3) -Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket.

Sie können auch andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

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

CloudTrail protokolliert alle Fleet Hub-Aktionen. Sie werden in der AWS IoT -API-Referenz dokumentiert. Beispielsweise generieren Aufrufe der `CreateApplication` und `UpdateApplication` -Aktionen Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde

- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in der Protokolldatei von Fleet Hub for AWS IoT Device Management

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden.

CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter.

CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Example

Der folgende CloudTrail Protokolleintrag enthält Informationen über die `CreateApplication` Aktion.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal-id",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user-name",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principal-id",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
```

```
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2020-12-04T19:59:53Z"
                }
            }
        },
        "eventTime": "2020-12-04T20:02:38Z",
        "eventSource": "iotfleethub.amazonaws.com",
        "eventName": "CreateApplication",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "72.22.186.61",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
            "applicationDescription": "Test application description",
            "applicationName": "Test application name",
            "clientToken": "c9bc7f45-3737-4ee9-9b0f-5de1aab169b2"
        },
        "responseElements": {
            "applicationUrl": "https://application-id.app.iotfleethub.aws",
            "applicationArn": "arn:aws:iotfleethub:us-
east-1:123456789012:application/application-id",
            "applicationId": "application-id"
        },
        "requestID": "5456304e-31c5-4336-9bbe-a375e3728eee",
        "eventID": "9ffb5d72-9267-4f4e-88e6-d26051133c8c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "recipientAccountId": "123456789012"
    }
```

Sicherheit in Fleet Hub für die AWS IoT Geräteverwaltung

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 . Weitere Informationen zu den Compliance-Programmen, die für Fleet Hub gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung anwenden können, wenn Sie Fleet Hub for AWS IoT Device Management verwenden. Die folgenden Themen veranschaulichen, wie Sie Fleet Hub zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Fleet Hub-Ressourcen helfen.

Themen

- Datenschutz in Fleet Hub
- Identity and Access Management für Fleet Hub for AWS IoT Device Management
- Konformitätsprüfung für Fleet Hub for AWS IoT Device Management
- Ausfallsicherheit in Fleet Hub für AWS IoT Gerätemanagement
- AWS verwaltete Richtlinien für Fleet Hub for AWS IoT Device Management
- Infrastruktursicherheit in Fleet Hub für AWS IoT Gerätemanagement
- Serviceübergreifende Confused-Deputy-Prävention

Datenschutz in Fleet Hub

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

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Fleet Hub oder anderen Geräten AWS-Services über die Konsole, API oder arbeiten. AWS CLI AWS SDKs 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.

Verschlüsselung im Ruhezustand

Fleet Hub schützt durch serverseitige Verschlüsselung Daten im Ruhezustand. Weitere Informationen finden Sie unter Datenverschlüsselung in AWS IoT im AWS IoT Entwicklerhandbuch.

Verschlüsselung während der Übertragung

Fleet Hub schützt in Cloud-Bereitstellungen von Flows Daten während der Übertragung mithilfe des Transport Layer Security (TLS)-Protokolls. Weitere Informationen finden Sie unter Transportsicherheit AWS IoT im AWS IoT -Entwicklerhandbuch.

Identity and Access Management für Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren steuern, wer für die Nutzung von Fleet-Hub-Ressourcen authentifiziert (angemeldet) und autorisiert (mit Berechtigungen) werden kann. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM
- Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management
- Problembehandlung bei Fleet Hub for AWS IoT Device Management Identität und Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Fleet Hub ausführen.

Service-Benutzer – Wenn Sie den Fleet-Hub-Service zur Ausführung Ihres Jobs verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Fleet-Hub-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter Problembehandlung bei Fleet Hub for AWS IoT Device Management Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in Fleet Hub haben.

Service administrator (Service-Administrator) – Wenn Sie in Ihrem Unternehmen für Fleet-Hub-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Fleet Hub. Es ist Ihre Aufgabe, zu bestimmen, auf welche Fleet-Hub-Funktionen und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Fleet Hub verwenden kann, finden Sie unter Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM.

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

Authentifizierung mit Identitäten

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

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

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

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. 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 AWS Multi-Faktor-Authentifizierung (MFA) in IAM 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. Verwenden Sie diese nur, 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.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung

zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

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

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - 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 ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine 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 Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 Inline-Richtlinie wählen, finden Sie unter Auswählen 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.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

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.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich

auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.

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

Mehrere Richtlinientypen

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

Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Fleet Hub verwenden, erfahren Sie, welche IAM-Funktionen Sie mit Fleet Hub verwenden können.

IAM-Funktionen, die Sie mit verwenden können Fleet Hub for AWS IoT Device Management

IAM-Feature	Fleet-Hub-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja

IAM-Feature	Fleet-Hub-Unterstützung
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Fleet Hub und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Fleet-Hub-Richtlinien

Unterstützt Richtlinien auf Identitätsbasis: Ja

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Fleet Hub

Beispiele für identitätsbasierte Fleet-Hub-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management.

Ressourcenbasierte Richtlinien in Fleet Hub

Unterstützt ressourcenbasierte Richtlinien: Nein

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

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Fleet Hub

> **Note**
>
> Fleet-Hub-Anwendungen verwenden die `AWSIoTFleetHubFederationAccess`-verwaltete Richtlinie. Weitere Informationen finden Sie unter ???.

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. 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.

Eine Liste der ACM-Aktionen finden Sie unter Von Fleet Hub for AWS IoT Device Management definierte Aktionenin der Service-Autorisierungs-Referenz.

Richtlinienaktionen in Fleet Hub verwenden das folgende Präfix vor der Aktion:

```
iotfleethub
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "iotfleethub:action1",
      "iotfleethub:action2"
         ]
```

Beispiele für identitätsbasierte Fleet-Hub-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management.

Richtlinienressourcen für Fleet Hub

Unterstützt Richtlinienressourcen: Ja

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. 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": "*"
```

Eine Liste der Fleet Hub-Ressourcentypen und ihrer Eigenschaften ARNs finden Sie unter Ressourcen definiert von Fleet Hub for AWS IoT Device Management in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Fleet Hub for AWS IoT Device Management definierte Aktionen.

Beispiele für identitätsbasierte Fleet-Hub-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management.

Richtlinien-Bedingungsschlüssel für Fleet Hub

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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 `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.

Eine Liste von ACM-Bedingungsschlüsseln finden Sie unter Bedingungsschlüssel für Fleet Hub for AWS IoT Device Management in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von Fleet Hub for AWS IoT Device Management.

Beispiele für identitätsbasierte Fleet-Hub-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management.

Zugriffskontrolllisten (ACLs) in Fleet Hub

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (Attribute-Based Access Control, ABAC) mit Fleet Hub

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

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.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden Temporärer Anmeldeinformationen mit Fleet Hub

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für Fleet Hub

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.

Servicerollen für Fleet Hub

Unterstützt Servicerollen: Ja

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.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die Feet-Hub-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Fleet Hub dazu anleitet, es zu tun.

Serviceverknüpfte Rollen für Fleet Hub

Unterstützt serviceverknüpfte Rollen: Ja

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. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Fleet Hub for AWS IoT Device Management

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, Fleet-Hub-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console,

AWS Command Line Interface (AWS CLI) oder AWS API ausführen. 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.

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

Einzelheiten zu den von Fleet Hub definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Fleet Hub for AWS IoT Device Management in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Fleet-Hub-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

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

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads 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 mit 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 Sicherer API-Zugriff mit MFA 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 Fleet-Hub-Konsole

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

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

Um sicherzustellen, dass Benutzer und Rollen die Fleet Hub-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den Fleet Hub `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie 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": "*"
        }
    ]
}
```

Problembehandlung bei Fleet Hub for AWS IoT Device Management Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit ACM und IAM auftreten könnten.

Themen

- Ich bin nicht autorisiert, eine Aktion in Fleet Hub auszuführen.
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Fleet Hub-Ressourcen ermöglichen

Ich bin nicht autorisiert, eine Aktion in Fleet Hub auszuführen.

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

> **Note**
>
> Fleet-Hub-Anwendungen verwenden die `AWSIoTFleetHubFederationAccess`-verwaltete Richtlinie. Weitere Informationen finden Sie unter ???.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `iotfleethub:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotfleethub:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *my-example-widget* auf die Ressource `iotfleethub:`*GetWidget* zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Fleet Hub übergeben 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 Fleet Hub auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

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

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

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Fleet Hub-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Fleet Hub diese Funktionen unterstützt, finden Sie unter Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie gehören.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsprüfung für Fleet Hub for AWS IoT Device Management

Externe Prüfer bewerten die Sicherheit und Konformität von Fleet Hub im Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

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

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

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

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit in Fleet Hub für AWS IoT Gerätemanagement

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.

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

AWS verwaltete Richtlinien für Fleet Hub for AWS IoT Device Management

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AWSIo TFleet HubFederationAccess

Sie können die `AWSIoTFleetHubFederationAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Verbundbenutzern von Fleet Hub for AWS IoT Device Management die Berechtigungen, die sie benötigen, um Aktionen in Fleet Hub-Webanwendungen AWS IoT und anderen AWS Diensten von Fleet Hub-Webanwendungen aus durchzuführen.

Weitere Informationen zum Hinzufügen von Benutzern zu Fleet-Hub-Webanwendungen finden Sie unter ???.

Sie können diese Richtlinie in der AWS -Konsole anzeigen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `iot`- Rufen Sie AWS IoT Gerätedaten ab und führen Sie Aktionen auf Flottenebene durch.
- `iotfleethub` - Rufen Sie die Metadaten der Fleet-Hub-App ab.
- `cloudwatch`- Rufen Sie CloudWatch Alarm- und Messdaten ab. Ermöglicht auch das Erstellen und Löschen von Aktionen, die auf Fleet-Hub-Alarme beschränkt sind.
- `sns` - Führen Sie Vorgänge zum Erstellen, Lesen, Löschen, Abonnieren und Abbestellen durch. Diese Operationen beziehen sich auf Fleet-Hub-SNS-Themen.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeIndex",
                "iot:DescribeThingGroup",
                "iot:GetBucketsAggregation",
                "iot:GetCardinality",
                "iot:GetIndexingConfiguration",
                "iot:GetPercentiles",
```

```
                "iot:GetStatistics",
                "iot:SearchIndex",
                "iot:CreateFleetMetric",
                "iot:ListFleetMetrics",
                "iot:DeleteFleetMetric",
                "iot:DescribeFleetMetric",
                "iot:UpdateFleetMetric",
                "iot:DescribeCustomMetric",
                "iot:ListCustomMetrics",
                "iot:ListDimensions",
                "iot:ListMetricValues",
                "iot:ListThingGroups",
                "iot:ListThingsInThingGroup",
                "iot:ListJobTemplates",
                "iot:DescribeJobTemplate",
                "iot:ListJobs",
                "iot:CreateJob",
                "iot:CancelJob",
                "iot:DescribeJob",
                "iot:ListJobExecutionsForJob",
                "iot:ListJobExecutionsForThing",
                "iot:DescribeJobExecution",
                "iot:ListSecurityProfiles",
                "iot:DescribeSecurityProfile",
                "iot:ListActiveViolations",
                "iot:GetThingShadow",
                "iot:ListNamedShadowsForThing",
                "iot:CancelJobExecution",
                "iot:DescribeEndpoint",
                "iotfleethub:DescribeApplication",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:Subscribe",
```

```
                "sns:Unsubscribe"
            ],
            "Resource": "arn:aws:sns:*:*:iotfleethub*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory"
            ],
            "Resource": "arn:aws:cloudwatch:*:*:iotfleethub*"
        }
    ]
}
```

Fleet Hub aktualisiert die AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für Fleet Hub seit Beginn der Erfassung dieser Änderungen durch diesen Service. Weitere Informationen finden Sie in der Dokumentationshistorien-Seite von Fleet Hub.

Änderung	Beschreibung	Datum
AWSIoTFleetHubFederationAccess – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat neue Berechtigungen hinzugefügt, damit App-Benutzer Metrikdaten in Fleet-Hub-Apps abrufen können. AWS IoT Device Defender	4. April 2022
AWSIoTFleetHubFederationAccess – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat neue Berechtigungen hinzugefügt, damit App-Benutzer zusätzliche Datenquellen für die Indizierung abrufen können. Außerdem wurde eine Berechtigung	15. November 2021

Änderung	Beschreibung	Datum
	hinzugefügt, die es App-Benutzern ermöglicht, die Ausführung eines AWS IoT Jobs innerhalb der App abzubrechen.	
AWSIoTFleetHubFederationAccess – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat neue Berechtigungen für App-Benutzer hinzugefügt, um Thing Group-Daten abzurufen und CRUD-Operationen für AWS IoT Jobs auszuführen.	24. Mai 2021
AWSIoTFleetHubFederationAccess – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat die Berechtigungen für das nicht unterstützte Fleet Hub-Dashboard entfernt. APIs	12. April 2021
AWSIoTFleetHubFederationAccess – Neue Richtlinie	Fleet Hub hat eine neue Richtlinie hinzugefügt, die Benutzern der Fleet Hub-Anwendung Berechtigungen gewährt, die sie benötigen, um Gerätedaten abzurufen und AWS IoT Aktionen auszuführen.	12. April 2021
Fleet Hub hat damit begonnen, Änderungen zu verfolgen	Fleet Hub hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	12. April 2021

Infrastruktursicherheit in Fleet Hub für AWS IoT Gerätemanagement

Als verwalteter Service ist Fleet Hub for AWS IoT Device Management durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Fleet Hub zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.2 oder höher unterstützen. Wir empfehlen die Verwendung von TLS 1.3. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

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

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. Ein AWS dienstübergreifender Identitätswechsel kann zu einem Problem mit dem verwirrten Stellvertreter 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.

Um die Berechtigungen, die Fleet Hub einem anderen Dienst für die Ressource gibt, einzuschränken, empfehlen wir die Verwendung der globalen Bedingungskontextschlüssel in Ressourcenrichtlinien. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der effektivste Weg, um sich vor dem Verwirrter-Stellvertreter-Problem zu schützen, ist die Verwendung des `aws:SourceArn` globalen Bedingungskontextschlüssels mit dem vollständigen Amazon-Ressourcenname (ARN) der Ressource. Für Fleet Hub `aws:SourceArn` müssen Sie das folgende Format einhalten: `arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Vergewissern Sie sich, dass das *`region`* mit Ihrer Fleet Hub-Region und das *`account-id`* mit Ihrer Kundenkonto-ID übereinstimmt.

Im folgenden Beispiel werden die globalen Bedingungskontextschlüssel `aws:SourceArn` und `aws:SourceAccount` in der Vertrauensrichtlinie der Fleet-Hub-Rolle verwendet, um das Verwirrter-Stellvertreter-Problem zu verhindern. Um den ARN für Ihre Fleet Hub-Rolle zu finden, gehen Sie in der AWS IoT Konsole zum Bereich Fleet Hub und wählen Sie Ihre Fleet Hub-Anwendung aus, um die Seite mit den Anwendungsdetails aufzurufen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotfleethub.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iot:us-east-1:123456789012:*"
        }
      }
    }
  ]
}
```

Fleet Hub end-of-life (EOL) FAQs

Fleet Hub end-of-life FAQs

- Wann geht Fleet Hub end-of-life?
- Was passiert mit meinen Fleet Hub-Anwendungen an dem end-of-life Tag?
- Was passiert mit meinen zugrunde liegenden AWS Ressourcen am und nach dem end-of-life Datum?
- Wie lösche ich Fleet Hub-Anwendungen vor dem Datum? end-of-life
- Werden beim Löschen von Fleet Hub-Anwendungen automatisch die zugrunde liegenden Ressourcen gelöscht?
- Wie lösche ich meine zugrunde liegenden AWS Ressourcen?
- Was APIs funktioniert am und nach dem Datum nicht mehr? end-of-life
- Was sind die bestehenden Funktionen von Fleet Hub und wie greife ich über die Konsole darauf zu?

Wann geht Fleet Hub end-of-life?

AWS wird Fleet Hub for AWS IoT Device Management am 18. Oktober 2025 einstellen. Fleet Hub wird schrittweise in sein EOL übergehen. Die von Fleet Hub zur Verfügung gestellten Funktionen sind auch in der AWS IoT Device Management Konsole verfügbar, um Ihre Geschäftsanforderungen weiterhin zu unterstützen.

1. Am 17. Oktober 2024 AWS wird die Aufnahme neuer Kunden in Fleet Hub eingestellt. Wenn Sie vor dem 17. Oktober 2024 noch keine Fleet Hub-Anwendungen haben, gelten Sie als neuer Fleet Hub-Kunde. Andernfalls werden Sie als bestehender Fleet Hub-Kunde identifiziert.
2. Bestehende Fleet Hub-Kunden können Fleet Hub-Anwendungen bis zum 17. Oktober 2025 weiterhin nutzen. Vom 17. Oktober 2024 bis 17. Oktober 2025 wird es keine neuen Funktionsupdates für Fleet Hub AWS geben und es werden kritische Bugfixes unterstützt.
3. Am 18. Oktober 2025 AWS wird die Unterstützung für Fleet Hub for AWS IoT Device Management eingestellt. An diesem Tag erreicht Fleet Hub sein Limit end-of-life und Sie können Fleet Hub nicht mehr nutzen. Die Einstellung von Fleet Hub hat keine Auswirkungen auf andere AWS IoT Device Management Funktionen. Sie können die vorhandenen Funktionen von AWS IoT Device Management weiterhin verwenden. Weitere Informationen finden Sie unter ???.

Was passiert mit meinen Fleet Hub-Anwendungen an dem end-of-life Tag?

Am EOL-Datum, dem 18. Oktober 2025, werden Ihre Fleet Hub-Anwendungen gelöscht und Sie können nicht mehr auf Fleet Hub zugreifen. Ihre mit Fleet Hub verknüpften AWS Ressourcen werden nicht automatisch gelöscht. Zu diesen Ressourcen gehören AWS IoT Device Management Jobs, Fleet Hub-Alarmkomponenten wie AWS IoT Device Management Flottenkennzahlen, CloudWatch Alarme und Amazon SNS SNS-Themen. Sie können für Ihre Überwachungsanforderungen weiterhin unabhängig vom AWS Management Console AWS CLI, oder AWS SDK auf diese Ressourcen zugreifen. Informationen zum Löschen Ihrer zugrunde liegenden AWS Ressourcen finden Sie unter???.

Was passiert mit meinen zugrunde liegenden AWS Ressourcen am und nach dem end-of-life Datum?

Sie können weiterhin unabhängig von AWS Management Console Ihren Überwachungsanforderungen auf Ihre zugrunde liegenden AWS Ressourcen zugreifen, die mit Fleet Hub verknüpft sind. Zu diesen Ressourcen gehören AWS IoT Device Management Jobs, Fleet Hub-Alarmkomponenten wie AWS IoT Device Management Flottenkennzahlen, CloudWatch Alarme und Amazon SNS SNS-Themen. Benutzer der Fleet Hub-Anwendung werden von Ihnen aus Ihrem IAM Identity Center-Benutzerpool zugewiesen. Wenn Ihre IAM Identity Center-Benutzer ausschließlich für den Zugriff auf Fleet Hub-Anwendungen erstellt wurden und Sie sie nicht für andere AWS Dienste verwenden, können Sie sie von den Registerkarten Benutzer und Anwendungen in IAM Identity Center in der Konsole löschen. Weitere Informationen finden Sie unter ???.

Wie lösche ich Fleet Hub-Anwendungen vor dem Datum? end-of-life

Um Ihre Fleet Hub-Anwendungen vor dem EOL-Datum zu löschen, verwenden Sie die AWS IoT Konsole oder den `--delete-application` AWS CLI Befehl.

> **Note**
>
> Durch das Löschen von Fleet Hub-Anwendungen werden die zugrunde liegenden AWS Ressourcen, die Fleet Hub zugeordnet sind, nicht gelöscht. Informationen zum Löschen

dieser Ressourcen finden Sie unter the section called “Wie lösche ich meine zugrunde liegenden AWS Ressourcen?”

Gehen Sie wie folgt vor, um Fleet Hub-Anwendungen mithilfe der AWS IoT Konsole zu löschen.

1. Gehen Sie zur AWS IoT Konsole, wählen Sie in der linken Navigationsleiste Fleet Hub und dann Anwendungen aus.
2. Wählen Sie auf der Anwendungsseite die Fleet Hub-Anwendung aus, die Sie löschen möchten. Wählen Sie Löschen aus. In einem Fenster werden Sie aufgefordert, das Löschen der Anwendung zu bestätigen. Geben Sie „Löschen“ ein, um den Löschvorgang zu bestätigen, und wählen Sie dann Löschen.

Gehen Sie wie folgt vor AWS CLI, um Fleet Hub-Anwendungen mit zu löschen.

1. Um Ihre Fleet Hub-Anwendung mit zu löschen AWS CLI, müssen Sie die Anwendungs-ID kennen. Führen Sie zuerst den `--list-applications`CLI-Befehl aus, um alle Ihre Fleet Hub-Anwendungen und deren Anwendungen aufzulisten IDs.

   Führen Sie den folgenden Befehl aus IDs, um Ihre Fleet Hub-Anwendungen mit ihren aufzulisten.

   ```
   aws iotfleethub --list-applications --region us-west-2
   ```

   Die Ausgabe des Befehls kann wie folgt aussehen.

   ```
   {
    "applicationSummaries": [
     {
      "applicationId": "68d0603a-66c9-43bf-b93f-a90e7ee5cf76",
      "applicationName": "test_app1",
      "applicationUrl": "https://12ad0603a-66c9-43bf-b93f-
   a90e7ee5cf76.app.iotfleethub.aws",
      "applicationCreationDate": 1698174116,
      "applicationLastUpdateDate": 1698174117,
      "applicationState": "ACTIVE"
     },
     {
      "applicationId": "b6198497-cd5b-400c-9b82-1c82b69cb66c",
      "applicationName": "test_app2",
   ```

```
    "applicationUrl": "https://c6198490-
cd5a-400c-9b82-1c82b69cb66c.app.iotfleethub.aws",
    "applicationCreationDate": 1684355213,
    "applicationLastUpdateDate": 1684355214,
    "applicationState": "ACTIVE"
   }
  ]
}
```

2. Führen Sie den folgenden AWS CLI Befehl aus, um Ihre Fleet Hub-Anwendung zu löschen.

```
aws iotfleethub --delete-application --application-id b6198497-
cd5b-400c-9b82-1c82b69cb66c --region us-west-2
```

Der Befehl erzeugt keine Ausgabe. Sie können den `--list-applications` CLI-Befehl ausführen, um zu überprüfen, ob die angegebene Anwendung gelöscht wurde oder nicht.

Werden beim Löschen von Fleet Hub-Anwendungen automatisch die zugrunde liegenden Ressourcen gelöscht?

Nein. Durch das Löschen von Fleet Hub-Anwendungen werden die zugrunde liegenden Ressourcen nicht automatisch gelöscht. Informationen zum Löschen Ihrer mit Fleet Hub verknüpften AWS Ressourcen finden Sie unter???.

Wie lösche ich meine zugrunde liegenden AWS Ressourcen?

Mit Fleet Hub können Kunden AWS Ressourcen wie AWS IoT Device Management Jobs und Fleet Hub-Alarme erstellen. Durch das Löschen von Fleet Hub-Anwendungen werden diese Ressourcen nicht gelöscht, und Sie können weiterhin darauf zugreifen, um Ihre Geschäftsanforderungen zu erfüllen, wie unter beschrieben???. Gehen Sie wie folgt vor, um diese zugrunde liegenden Ressourcen zu löschen.

Wie lösche ich Jobs?

Um einen Job zu löschen, müssen Sie den Job zuerst stornieren. Sie können Aufträge vor dem EOL-Datum direkt von Fleet Hub aus stornieren. Sie können die AWS IoT Konsole auch verwenden, um Jobs zu stornieren und zu löschen, wann immer Sie möchten.

Um Jobs in Ihrer Fleet Hub-Anwendung zu stornieren

1. Gehen Sie zu Ihrer Fleet Hub-Anwendung und wählen Sie den Tab Jobs.
2. Wählen Sie einen Job aus, den Sie stornieren möchten.
3. Wählen Sie Job stornieren.

Um Jobs von der AWS IoT Konsole aus abzubrechen und zu löschen

1. Gehen Sie zu Remote-Aktionen und wählen Sie die Registerkarte Jobs.
2. Wählen Sie einen Job aus, den Sie stornieren möchten.
3. Klicken Sie auf Abbrechen.
4. Wählen Sie auf derselben Registerkarte „Jobs“ den Job aus, den Sie löschen möchten.
5. Wählen Sie Löschen aus.

Wie lösche ich Fleet Hub-Alarme?

Sie können die Fleet Hub-Alarme direkt in der Fleet Hub-Anwendung löschen. Dadurch werden automatisch alle zugrunde liegenden Komponenten wie Flottenkennzahlen, CloudWatch Alarme und Amazon SNS SNS-Themen gelöscht. Navigieren Sie in Ihrer Fleet Hub-Anwendung zur Registerkarte Fleet Hub-Alarme, wählen Sie die Alarme aus, die Sie löschen möchten, und wählen Sie Löschen. Alternativ können Sie die Fleet Hub-Alarme mit löschen AWS Management Console. Möglicherweise möchten Sie diese Schritte ausführen, um mehrere Anwendungen in verschiedenen AWS Regionen zu löschen.

Um Fleet Hub-Alarme aus der Fleet Hub-Anwendung zu löschen

1. Navigieren Sie in der Fleet Hub-Anwendung zur Registerkarte Fleet Hub-Alarme.
2. Wählen Sie die Alarme aus, die Sie löschen möchten, und wählen Sie Löschen. Durch diese Aktion werden alle zugrunde liegenden Komponenten gelöscht.

Um Flottenkennzahlen von der AWS IoT Konsole zu löschen

1. Gehen Sie in der linken Navigationsleiste der AWS IoT Konsole zu Verwalten. Wählen Sie unter Alle Geräte die Option Fleet Metrics aus.
2. Wählen Sie alle Flottenkennzahlen aus, deren Namen das Präfix „iotfleethub“ vorangestellt ist.

3. Wählen Sie Löschen aus.

Um Alarme von der Konsole zu löschen CloudWatch CloudWatch

1. Gehen Sie in der CloudWatch Konsole zur Registerkarte Alle Alarme.
2. Wählen Sie alle Metriken aus, deren Namen das Präfix „iotfleethub“ vorangestellt ist.
3. Gehen Sie zu Aktionen und wählen Sie Löschen.

Um Amazon SNS SNS-Themen zu löschen, die Alarme empfangen, die über die Amazon SNS SNS-Konsole erstellt wurden

1. Gehen Sie in der Amazon SNS SNS-Konsole zur Registerkarte Themen.
2. Wählen Sie alle Themen aus, deren Namen das Präfix „iotfleethub“ haben.
3. Wählen Sie Löschen aus.

Wie lösche ich IAM Identity Center-Benutzer, die in Fleet Hub erstellt wurden?

Wenn Ihre IAM Identity Center-Benutzer ausschließlich für den Zugriff auf Fleet Hub-Anwendungen erstellt wurden und Sie sie nicht für andere AWS Dienste verwenden, können Sie sie von den Registerkarten Benutzer und Anwendungen in IAM Identity Center in der Konsole löschen.

Was APIs funktioniert am und nach dem Datum nicht mehr? end-of-life

Wir werden am 18. Oktober 2025 alle mit dem Lifecycle-Management des Fleet Hubs APIs verbundenen Anwendungen einstellen. Beachten Sie, dass diese nur mit Fleet Hub verknüpft APIs sind und keine anderen AWS IoT Device Management Funktionen beeinträchtigen. Bestehende Fleet Hub-Kunden können diese APIs bis zum 17. Oktober 2025 weiter nutzen.

- CreateApplication
- DeleteApplication
- DescribeApplication
- ListApplication

- ListTagsForResource
- TagResource
- UntagResource
- UpdateApplication

Was sind die bestehenden Funktionen von Fleet Hub und wie greife ich über die Konsole darauf zu?

Fleet Hub bietet die folgenden wichtigen Überwachungs- und Verwaltungsfunktionen, die auf AWS IoT Device Management Funktionen basieren. Diese Funktionen sind alle außerhalb der Fleet Hub-Anwendungen verfügbar. Sie befinden sich direkt in der AWS IoT Device Management Konsole, auf die Sie weiterhin zugreifen können, um Ihre Geschäftsanforderungen zu unterstützen.

Zusammenfassung des Status der Flottenkonnektivität

Das Fleet Hub-Dashboard fasst den Konnektivitätsstatus Ihrer IoT-Flotte mit Verbindungsdetails zusammen. Es zeigt die Anzahl der verbundenen und getrennten Geräte und die Verteilung der getrennten Geräte nach Grund der Unterbrechung. Ein entsprechendes Dashboard zur Überwachung des Konnektivitätsstatus ist in der AWS IoT Konsole unter der Registerkarte Monitor verfügbar. Dort können Sie Widgets aktivieren, um die Anzahl der verbundenen Geräte, die Häufigkeit von Verbindungsabbrüchen und die Gründe für die Unterbrechung zu überwachen. Weitere Informationen finden Sie unter AWS IoT Device Management Fügt ein einheitliches Dashboard zur Überwachung von Konnektivitätsmetriken hinzu.

Fleet Hub-Alarme

Mit Fleet Hub-Alarmen können Sie auf Schwellenwerten basierende Alarme erstellen und überwachen. Fleet Hub-Alarme nutzen Flottenkennzahlen, die durch AWS IoT Device Management Flottenindizierung und CloudWatch Amazon-Alarme bereitgestellt werden. Sie können diese Flottenkennzahlen direkt in der CloudWatch Amazon-Konsole überwachen und sie in der AWS IoT Konsole neu konfigurieren. Die Flottenkennzahlen und CloudWatch Alarme, deren Namen das Präfix „iotfleethub“ haben, sind mit Fleet Hub verknüpft. Sie können weiterhin von der Konsole aus auf sie zugreifen. Sie können Amazon verwenden CloudWatch, um diese Metriken im Laufe der Zeit zu überwachen und Trends zu verfolgen. Sie können auch zusätzliche Flottenkennzahlen von der AWS IoT Konsole aus erstellen, diese dann überwachen und Alarme in Amazon einrichten CloudWatch. Weitere Informationen finden Sie unter Flottenkennzahlen anzeigen in CloudWatch.

Gerätesuche

Mit Fleet Hub können Sie mithilfe von Kriterien aus indizierten Datenquellen mehrere Filter anwenden, um Ihre Gerätesuche zu verfeinern. Diese Funktion nutzt die Suchfunktion der Flottenindexierung. Die Gerätesuche kann direkt über die AWS IoT Device Management Konsole auf der Seite Erweiterte Suche nach Objekten verwendet werden. Um die Seite für die erweiterte Suche nach Dingen zu finden, wählen Sie unter „Verwalten“ die Option „Dinge“ und anschließend „Alle Geräte“. Wähle in der oberen rechten Ecke der Seite „Dinge“ die Option Erweiterte Suche aus.

Auftragsausführung

Sie können Jobs direkt von Fleet Hub aus ausführen, indem Sie ein Ding oder eine Gruppe als Ziel auswählen. Sie können Jobs auch auf der Seite Jobs in der AWS IoT Device Management Konsole ausführen, wo Sie ein Ding, eine statische Gruppe oder eine dynamische Gruppe als Ziel für die Jobausführung definieren können.

Ansicht der Gerätedetails

Fleet Hub bietet auf der Seite „Alle Geräte“ eine detaillierte Ansicht auf Geräteebene. Eine ähnliche Detailansicht auf Geräteebene ist direkt auf der Registerkarte „Dinge“ in der AWS IoT Device Management Konsole verfügbar oder wenn Sie auf ein bestimmtes Objekt klicken, das in den Ergebnissen der Flottenindexierungs-Suchanfrage angezeigt wird.

Dokumentationsverlauf

In der folgenden Tabelle werden die Aktualisierungen der Fleet-Hub-Dokumentation beschrieben. Änderungen der AWS verwalteten Richtlinien für Fleet Hub finden Sie unter AWS Verwaltete Richtlinien für Fleet Hub for AWS IoT Device Management.

Änderung	Beschreibung	Datum
Version für allgemeine Verfügbarkeit von Fleet Hub for AWS IoT Device Management	Der Inhalt wurde aktualisiert, um den Verbesserungen Rechnung zu tragen, die in der Vorschauphase an Fleet Hub for AWS IoT Device Management vorgenommen wurden.	25. Mai 2021
Vorschauversion von Fleet Hub for AWS IoT Device Management	Die Vorabversion des Benutzerleitfadens Fleet Hub for AWS IoT Device Management wurde veröffentlicht.	16. Dezember 2020