



Leitfaden für die AWS IoT Geräteverwaltung mit Fleet Hub

Fleet Hub für AWS IoT Gerätemanagement



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

Copyright © 2024 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

Wofür ist Fleet HubAWS IoTGeräteverwaltung?	1
Wie Fleet Hub fürAWS IoTDie Geräteverwaltung funktioniert	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
AWSund 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 Anfrage	13
Erstellen Ihres ersten Alarms	14
Anzeigen von Gerätedetails Details Details anzeigen	18
Abfragen und Filter	22
Dashboard anzeigen	22
Erstellen Sie Abfragen mit Filtern	24
Arbeiten mit Jobs und Job-Vorlagen in Fleet Hub fürAWS IoTGerätemanagement	26
Ausführen von Aufgaben	26
Anzeigen und Verwalten von Aufträgen	27
Alarme	28
Erstellen von Alarmen	30
Fehlerbehebung	31
Fuhrpark fürAWS IoT Gerätemanagement	33
Protokollierung von Fleet Hub fürAWS IoT Gerätemanagement-API-Aufrufe mitAWS CloudTrail	33
Fleet Hub-Informationen in CloudTrail	34
Grundlegendes zu den Protokolldateieinträgen von Fleet Hub forAWS 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
AWSIoT FleetHub Federation Access	63
Richtlinienaktualisierungen	65
Sicherheit der Infrastruktur	66
Serviceübergreifende Confused-Deputy-Prävention	67
Dokumentationsverlauf	69
.....	lxx

Wofür ist Fleet Hub AWS IoT Geräteverwaltung?

Mit Fleet Hub für AWS IoT Geräteverwaltung (Fleet Hub), Sie können eigenständige Webanwendungen erstellen, um den Zustand Ihrer Geräteflotten zu überwachen. Sie können diese Anwendungen Benutzern in Ihrer Organisation zur Verfügung stellen, auch wenn sie dies nicht getan haben AWS Konten. Verwenden Sie Fleet Hub, um allgemeine flottenweite Aufgaben wie die Untersuchung und Behebung von Betriebs- und Sicherheitsproblemen zu verwalten.

Fleet Hub bietet die folgenden Funktionen.

- Überwachen Sie Geräteflotten nahezu in Echtzeit.
- Richten Sie Warnmeldungen ein, um Ihre Techniker über ungewöhnliches Verhalten zu informieren.
- Jobs ausführen.

Note

Damit Fleet Hub Konnektivitätsstatusdaten indexieren kann, müssen sich Ihre Things mit AWS IoT Core wobei die Client-ID dem Dingnamen entspricht.

Wie Fleet Hub für AWS IoT Die Geräteverwaltung funktioniert

Administratoren können Fleet Hub verwenden für AWS IoT Geräteverwaltung zur Erstellung sicherer Webanwendungen in wenigen Minuten, 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 integrieren in AWS IoT Core Flottenindexierung und Geräteüberwachung. Diese Integrationen bieten die Möglichkeit, Gerätezustandsdaten zu überwachen und Alarme auszulösen, wenn Geräte in Ihrer Flotte einen bestimmten Zustand erreichen.

Fleet Hub-Anwendungen verwenden den `AWSIoT FleetHub Federation Access` verwaltete Richtlinie. Weitere Informationen finden Sie unter [???](#).

Beispielhafte Anwendungsfälle:

- 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 eine bestimmte Anzahl von Geräten die Verbindung trennt. Alarme können Sie auch benachrichtigen, wenn ein Gerät oder mehrere Geräte aus einem bestimmten Grund getrennt werden. Sie können sich dann detaillierte Gerätedaten ansehen, um dies zu untersuchen und Fehler zu beheben.
- Jobs ausführen — Sie können Remote-Operationen (z. B. 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 Flottenindexierung in Fleet Hub aktivieren, aktivieren Sie sie für die gesamte Flotte und stellen sie für alle Fleet Hub-Anwendungen zur Verfügung.

Wenn es aktiviert ist, indexiert Fleet Indexing alle AWS IoT Core-verwaltete Felder automatisch. Sie können die Flottenindizierung auch verwenden, um benutzerdefinierte Daten hinzuzufügen, die Sie verwenden können, um Daten in Fleet Hub-Anwendungen abzufragen und zu aggregieren.

So funktionieren Fleet Hub-Alarme

Fleet Hub-Webanwendungen bieten eine Schnittstelle, über die Ihre Benutzer Alarme erstellen können. Die folgenden Schritte zeigen, wie Benutzer Alarme in Fleet Hub erstellen.

1. Erstellen Sie eine Abfrage, um Daten zu aggregieren — Geben Sie eine Abfrage an, die mithilfe von durchsuchbaren Feldern die Geräte zusammenfasst, auf die Ihre Benutzer abzielen möchten.
2. Schwellenwert konfigurieren — Legen Sie einen Schwellenwert fest, der die Alarme auslöst, wenn eine Bedingung 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 die angegebenen Geräte in Alarmbereitschaft sind.

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 Applications 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.

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: `AWSIoT FleetHub_ 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-Indizierung 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 View details 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 erläutert, 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 verwendet, um die einzelnen Funktionen zu implementieren.

Funktion	AWS-Service	Beschreibung
<p>Integrieren Sie bestehende Identitätssysteme wie Active Directory.</p>	<p>AWS IAM Identity Center(IAM-Identitätszentrum)</p>	<p>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 dem IAM Identity Center verbinden.</p> <p>Weitere Informationen finden Sie unter Was ist AWS IAM Identity Center? und Identitäten der Belegschaft.</p>
<p>Erstellen Sie Abfragen, indem Sie AWS verwaltete Felder, benutzerdefinierte Felder und beliebige Attribute in Ihren indizierten Datenquellen verwenden.</p>	<p>AWS IoT Flottenindexierung</p>	<p>Verwenden Sie den Fleet Indexing Service, um Ihre Registrierungsdaten, Schattendaten und Gerätekonnektivitätsdaten (Ereignisse im Gerätelebenszyklus) zu indexieren, zu durchsuchen und zu aggregieren. Sie können zusätzlich zu den verwalteten Feldern, die AWS IoT Fleet Indexing standardmäßig indexiert, auch benutzerdefinierte Felder für die Aggregation erstellen.</p> <p>Weitere Informationen zur Flottenindizierung finden Sie unter Flottenindizierung.</p>

Funktion	AWS-Service	Beschreibung
Erstellen Sie Alarme für eine Reihe von Geräten, die durch eine Abfrage angegeben wurden.	Amazonas CloudWatch (CloudWatch)	<p>Fleet Hub-Dashboards enthalten CloudWatch Kennzahlen, die Sie in Kombination mit durchsuchbaren Feldern verwenden können, um alarmierende Schwellenwerte zu erstellen . Sie können beispielsweise einen CloudWatch Alarm erstellen, der eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung generiert, wenn die Anzahl der angeschlossenen Geräte eine bestimmte Anzahl unterschreitet.</p> <p>Informationen CloudWatch dazu finden Sie unter Was ist AmazonCloudWatch? Informationen zur AWS IoT Core Funktionsweise von CloudWatch zum Erstellen von Metriken und Alarmen finden Sie unter Überwachen von AWS IoT Alarmen und Metriken mithilfe von CloudWatch</p>

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.	<p>Stellen Sie sicher, dass Sie mindestens einen Benutzer zu Ihrer Anwendung hinzugefügt haben.</p> <p>Stellen Sie sicher, dass Ihre Rolle über die entsprechende Vertrauensbeziehung verfügt, z. B. die folgende:</p> <pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre>
Ich kann keine Webanwendung erstellen.	Stellen Sie sicher, dass Sie Ihr Limit für die Gesamtzahl der Webanwendungen nicht erreicht haben.
Ich sehe ein benutzerdefiniertes Feld nicht, das ich erwartet habe.	Stellen Sie sicher, dass die Flottenindexierung korrekt konfiguriert ist.

Symptom	Lösung
	Weitere Informationen zur Flottenindexierung finden Sie unter Flottenindexierung .

Fleet Hub für AWS IoT Gerätemanagement für Benutzer

Dieser Abschnitt enthält Informationen für Benutzer der Fleet Hub for AWS IoT Device Management-Webanwendungen. Informationen zum Erstellen von Fleet Hub-Anwendungen und zum Hinzufügen von Benutzern zu diesen finden Sie unter [Fleet Hub für AWS IoT Gerätemanagement für Administratoren](#).

Themen

- [Erste Schritte](#)
- [Abfragen und Filter](#)
- [Arbeiten mit Jobs und Job-Vorlagen in Fleet Hub für AWS IoT Gerätemanagement](#)
- [Alarme](#)
- [Fehlerbehebung](#)

Erste Schritte

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

Themen

- [Erstellen Ihrer ersten Anfrage](#)
- [Erstellen Ihres ersten Alarms](#)
- [Anzeigen von Gerätedetails Details Details anzeigen](#)

Erstellen Ihrer ersten Anfrage

Dieses Thema führt Sie durch die Schritte zum Erstellen einer einfachen Fleet Hub for AWS IoT Device Management-Abfrage. Die Abfragen werden mithilfe der Suchabfragesyntax spezifiziert.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die mit einem AWS IoT Core Konto verknüpft ist und Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das über Berechtigungen zur Nutzung der Fleet Hub-Anwendung verfügt.

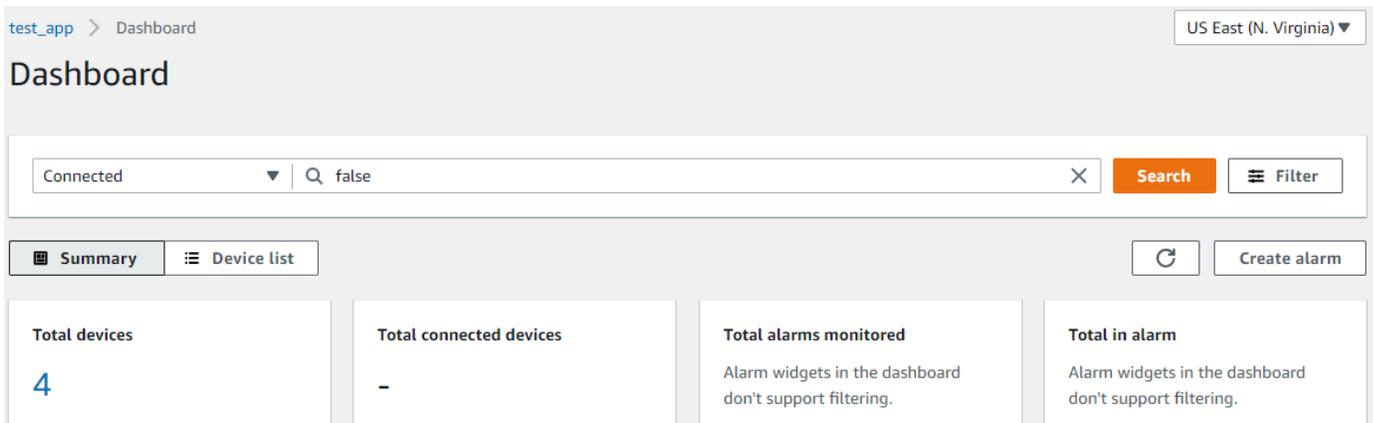
Erstellen Ihrer ersten Fleet Hub-Abfrage

Erstellen Ihrer ersten Fleet Hub-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 enthalten. Die Attribute, die das Attributpräfix enthalten, sind benutzerdefinierte Attribute.

2. Wählen Sie im Menü oben auf der Seite die Option Verbunden aus allen Feldern aus. Geben Sie **false** in das Textfeld neben dem Dropdown-Menü ein.



3. Um die Suche durchzuführen, wählen Sie Suchen. Eine Liste aller Geräte wird angezeigt, mit denen keine Verbindung bestehtAWS IoT Core.

Weitere Informationen zur Abfragesyntax und Beispielabfragen finden Sie unter [Abfragesyntax](#), [Beispieldingabfragen](#) und [Beispieldinggruppenabfragen](#).

Erstellen Ihres ersten Alarms

Dieses Thema führt Sie durch die Schritte zur Erstellung eines einfachen Fleet Hub for AWS IoT Device Management-Alarms.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die mit einem AWS IoT Core Konto verknüpft ist und Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das über Berechtigungen zur Nutzung der Fleet Hub-Anwendung verfügt.

Erstellen Ihres ersten Alarms

Erstellen Ihres ersten Fleet Hub-Alarms

1. Navigieren Sie zu Ihrer Fleet Hub-Anwendung.
2. Wenn Sie auf eine bestimmte Gruppe von Geräten abzielen möchten, erstellen Sie eine Abfrage. Anweisungen zum Erstellen einer einfachen Abfrage 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-Dashboardseite die Option Alarm erstellen aus.
4. Stellen Sie auf der Seite Aggregationsmetrik erstellen sicher, dass Ihre Abfrage unter Zielabfrage angezeigt wird. Wählen Sie im Abschnitt Aggregation von Flottenmetriken 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 AWS verwalteten Felder und die benutzerdefinierten Felder, die Ihr Administrator bei der AWS IoT Flottenindexierung erstellt hat.
5. Wählen Sie unter Wählen Aggregationstyp wählen Sie unter Wählen Sie eine der folgenden Optionen aus.
 - Maximum — Konfigurieren Sie einen maximalen Schwellenwert.
 - Anzahl — Konfigurieren Sie eine bestimmte Anzahl als Schwellenwert.
 - Summe -- Konfiguriert eine Summe als Schwellenwert.
 - Minimum — Konfigurieren Sie einen Mindestschwellenwert.
 - Durchschnitt — Konfigurieren Sie einen durchschnittlichen Schwellenwert.
6. Wählen Sie unter Zeitraum wählen die Dauer des Zustands aus, der in den vorherigen Menüs angegeben wurde und der den Alarm auslösen soll.

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

Configure fleet metric aggregation

Choose field

Choose a searchable field from your device's data.

Connected ▼

This field is a Boolean field. True will be converted to 1, and false to 0, to help aggregate data statistically.

Choose aggregation type

Choose how would you like your field to be aggregated. Different field types may trigger different aggregation options.

Count ▼

Choose period

Choose the frequency on which this alarm will be based.

1 minute ▼

Wählen Sie Weiter.

7. Auf der Seite Schwellenwert festlegen im Feld Alarm auslösen, wann immer... Abschnitt, wählen Sie eine der folgenden Optionen aus.
 - Größer — Meldet, wenn die Aggregationsmetrik und der Aggregationstyp den angegebenen Wert überschreiten.
 - Greater/Equal — Meldet, wenn die Aggregationsmetrik und der Aggregationstyp dem angegebenen Wert entsprechen oder diesen überschreiten.
 - Niedriger — Meldet, wenn die Aggregationsmetrik und der Aggregationstyp unter den angegebenen Wert fallen.
 - Niedriger/Gleichwertig — Alarmt, wenn die Aggregationsmetrik und der Aggregationstyp dem angegebenen Wert entsprechen oder diesen unterschreiten.
8. Geben Sie im Textfeld Als den Wert an, der als Schwellenwert für den Alarm verwendet werden soll.

Eine Beispielseinstellung für „Schwellenwert festlegen“ kann wie folgt aussehen:

Trigger the alarm whenever...

Metric is

Define alarm conditions

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

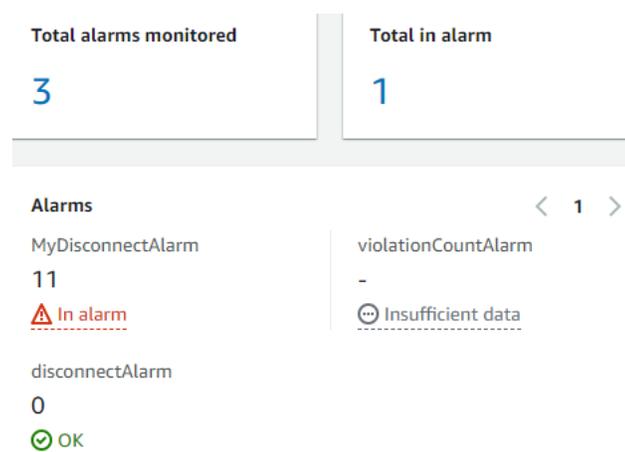
Than

Enter a threshold value.

1

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 Kommas getrennte Liste mit 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.
11. Überprüfen Sie auf der Überprüfungsseite die Informationen, die Sie auf den vorherigen Seiten eingegeben haben. Wählen Sie Submit (Absenden) aus. Sie kehren zum Standard-Dashboard zurück zum Standard-Dashboard zurück.
12. Im Standard-Dashboard zeigen die Alarm-Widgets Informationen zu allen von Ihnen erstellten Alarmen an.



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

Fleet Hub alarms			Delete	Edit	Create alarm
<input type="checkbox"/> Show triggered alarms			< 1 >		
Alarm name	Status	Latest update			
<input type="radio"/> MyDisconnectAlarm	Alarm	November 17, 2021 18:20 (UTC)			
<input type="radio"/> disconnectAlarm	OK	November 17, 2021 06:15 (UTC)			
<input type="radio"/> violationCountAlarm	Insufficient data	November 17, 2021 06:12 (UTC)			

Anzeigen von Gerätedetails Details Details anzeigen

Dieses Thema führt Sie Schritt für Schritt durch die einzelnen Schritte, um Details zu Ihren Gerätegruppen und Ihren Geräten einzusehen.

Voraussetzungen

- Eine Fleet Hub-Anwendung, die mit einem AWS IoT Core Konto verknüpft ist und Geräte (Dinge) enthält.
- Ein Konto in Ihrer Organisation, das über Berechtigungen zur Nutzung der Fleet Hub-Anwendung verfügt.

Gerätegruppen

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

test-0119		test-0119 > Device groups					US East (N. Virginia) ▼
Dashboards		Device groups					Run jobs
Jobs		Fleet Hub alarms					< 1 > ⚙
Group name	Parent group	Group type	Query	Group description	Created at		
<input type="radio"/> LightBulbs	-	Static group	-	-	March 11, 2022 18:59 (UTC)		
<input type="radio"/> MyDynamicThingGroup1	-	Dynamic group	attributes.wattage:75	-	October 17, 2021 22:15 (UTC)		
<input type="radio"/> MyStaticThingGroup	-	Static group	-	-	March 11, 2022 18:49 (UTC)		
<input type="radio"/> MyStaticThingGroup2	LightBulbs	Static group	-	-	March 11, 2022 19:01 (UTC)		

Details zur Gerätegruppe

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

The screenshot displays the 'MyDynamicThingGroup1' page in the AWS IoT Fleet Hub. At the top, there is a breadcrumb trail: 'test-0119 > Device groups > MyDynamicThingGroup1'. The main title 'MyDynamicThingGroup1' is on the left, with two buttons on the right: 'View on dashboard' and 'Run jobs'. Below this is a 'Group details' section with a table of attributes:

Name	MyDynamicThingGroup1	Group type	Dynamic group
Created on	October 17, 2021 22:15 (UTC)	Query terms	attributes.wattage:75

Below the group details is a 'Devices in MyDynamicThingGroup1 (2)' section. It features a search bar with the placeholder 'Find devices', a refresh button, and pagination controls showing '1' of 2 items. The device list contains two entries: 'MyLightBulb1' and 'MyLightBulb'. Below that is a 'Groups in MyDynamicThingGroup1' section, which also has a search bar with the placeholder 'Find device groups', a refresh button, and pagination controls showing '1' of 1 item. The group list is currently empty.

Angaben zum Gerät

Die Seite mit den Gerätedetails enthält Informationen zu Ihrem ausgewählten Gerät.

Note

Wenn Ihr Kunde beim Herstellen einer Verbindung eine andere Client-ID als Thing Name verwendet AWS IoT, wird der Konnektivitätsstatus Ihres „Dings“ von Fleet Indexing nicht indiziert.

Details

Der Abschnitt „Details“ enthält die folgenden Informationen zu Ihrem Gerät:

- **Gerätename** — Der Name der Dingressource, die Ihr Gerät repräsentiert. Weitere Informationen finden Sie unter [So verwalten Sie Dinge mit der Registrierung](#).
- **Ding-Typ** — Der Ding-Typ, der Ihrem Gerät zugeordnet ist. Sie können den Ding-Typ verwenden, um Informationen zu speichern, die allen Dingen mit demselben Ding-Typ gemeinsam sind. Weitere Informationen finden Sie unter [Dingtypen](#).
- **Zeitstempel der letzten Verbindung** — Der Zeitstempel, mit dem Ihr Gerät zuletzt verbunden wurde.
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 angeschlossen ist, ist der Wert *true*. Wenn es nicht verbunden ist, ist der Wert *false*.
- **Trennungsgrund** — Der Grund, warum Ihr Gerät getrennt wurde.

Gemeldete Daten

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

- **Gerätefelder** — Die indizierten Felder Ihres Geräts bei der AWS IoT Flottenindexierung. 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 Device Shadow unter [AWS IoT Device Shadow](#).

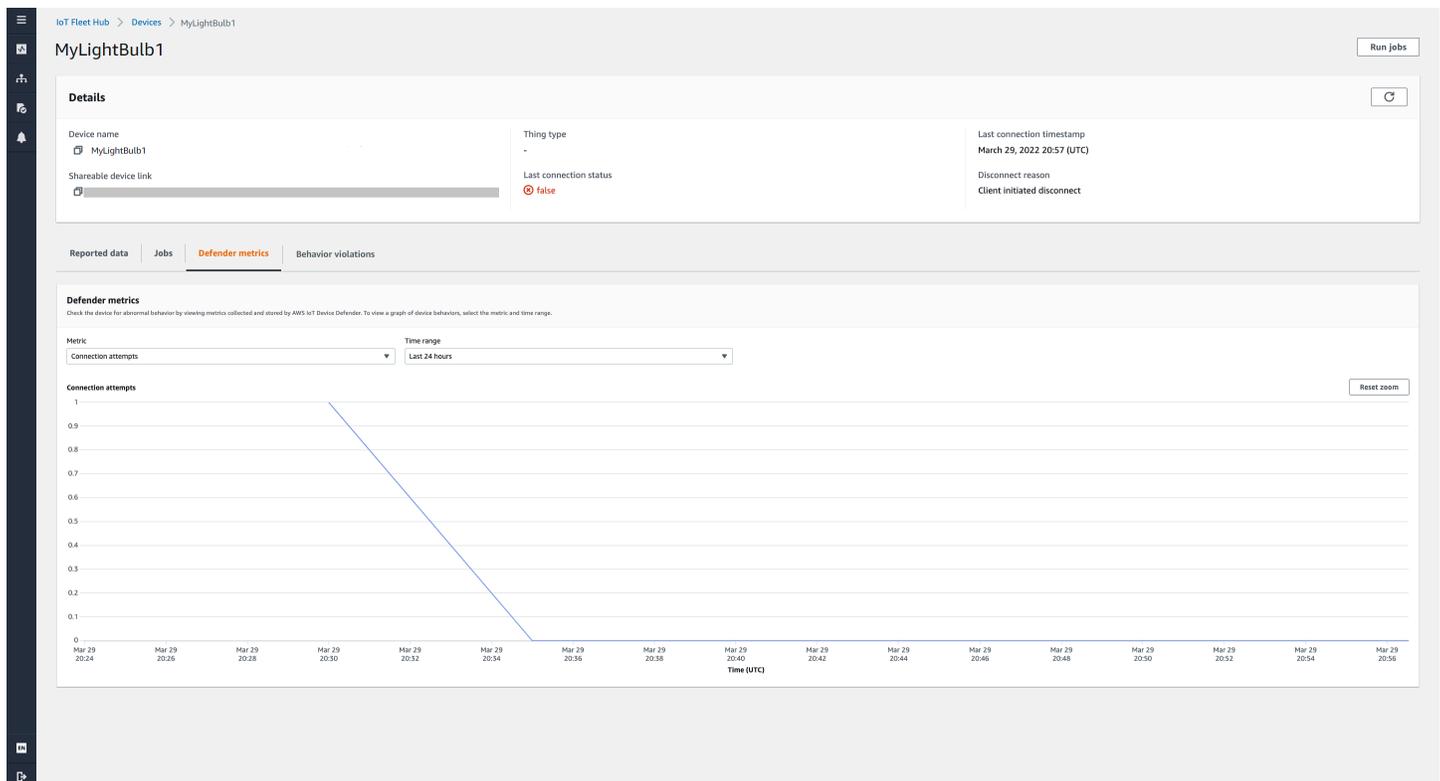
- **Gerätegruppen** — Die Gerätegruppen, die Ihrem Gerät zugeordnet sind. Die Gerätegruppen können sowohl statische Dinggruppen als auch dynamische Dinggruppen enthalten. Weitere Informationen finden Sie unter [Statische Dinggruppen](#) und [Dynamische Dinggruppen](#).

Aufträge

Im Abschnitt Jobs werden alle Jobs angezeigt, die auf dem Gerät ausgeführt werden. Jeder Job hat eine Detailseite, auf der zusammenfassende Informationen über den Job angezeigt werden, einschließlich Ziel- und Laufzeitinformationen. Weitere Informationen finden Sie unter [Arbeiten mit Aufträgen und Jobvorlagen in Fleet Hub for AWS IoT Device Management](#) und [Jobs](#).

Defender-Metriken

Im Abschnitt Defender-Metriken werden AWS IoT Device Defender Metriken angezeigt, die Ihrem aktuell ausgewählten Gerät zugeordnet sind. Sie können die angezeigten Metrikdaten verwenden, um den Betrieb Ihres Geräts über einen von Ihnen gewählten Zeitraum zu visualisieren. Um die Defender-Metrikdaten aus Ihrer Fleet Hub-Anwendung einsehen zu können, muss Ihr Fleet Hub-Administrator zunächst AWS IoT Device Defender Metriken 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, die Uhrzeit des letzten Verstößes und den Metrikwert des letzten Verstößes beinhalten. Um die Daten zu Verhaltensverstößen aus Ihrer Fleet Hub-Anwendung einzusehen, sollte Ihr Fleet Hub-Administrator AWS IoT Device Defender Verhaltensverstöße in einem Sicherheitsprofil einrichten und AWS IoT Device Defender Verstöße bei der [Flottenindexierung](#) konfigurieren. Weitere Informationen zum Einrichten von Verhaltensverstößen in einem Sicherheitsprofil finden Sie unter Erstellen von Verhaltensverstößen in einem AWS IoT Device Defender Sicherheitsprofil unter Erstellen von Verhaltensverletzungen in einem [AWS IoT Device Defender Sicherheitsprofil](#). Weitere Informationen zur Konfiguration von AWS IoT Device Defender Verstößen finden Sie unter [Flottenindizierung für Fleet Hub-Anwendungen verwalten und Objektindizierung verwalten](#).

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

Dashboard

The dashboard provides a summary of device and alarm status. It includes search and filter options, navigation tabs for Summary and Device list, and several key metrics.

Metric	Value
Total devices	40
Total connected devices	-
Total alarms monitored	2
Total in alarm	1

Disconnect reasons: There's something wrong with data loading. Contact your AWS IoT Fleet Hub admin for help.

Alarms: 1 alarm shown. **test-alarms-alarm** (40) is **In alarm**. **test-ok-alarm** (40) is **OK**.

Device types: There's something wrong with data loading. Contact your AWS IoT Fleet Hub admin for help.

Device groups: There's something wrong with data loading. Contact your AWS IoT Fleet Hub admin for help.

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 Gerätenamen
- 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

<input type="checkbox"/>	Name	Thing type	Thing groups	Connected	Last connection timestamp	Disconnect reason
<input type="checkbox"/>	waterSensor2	-	pennsylvania, surface-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor17	model-1	surface-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor11	model-1	surface-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor8	-	surface-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor31	-	surface-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor16	model-1	ground-sensors	⊗ false	-	-
<input type="checkbox"/>	waterSensor33	-	-	⊗ false	-	-

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 für 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 Jobs und Job-Vorlagen in Fleet Hub für AWS IoT Gerätemanagement

Note

Die Funktion „Auftragsvorlagen“ befindet sich in der Vorschau und kann Änderungen unterliegt.

Ein Auftrag ist eine Remote-Operation, die an ein oder mehrere mit 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 aus ausführen. Die Administratoren Ihrer Organisation erstellen Auftragsvorlagen in der Fleet Hub-Konsole und fügen Sie Richtlinien an, die die Vorlagen für Fleet Hub-Benutzer verfügbar machen. In Ihrer Fleet Hub-Anwendung geben Sie die Geräte oder eine Gerätegruppe an, auf der der Job ausgeführt wird.

Administratoren erstellen auch Gerätegruppen, die Sie in Ihrer Anwendung anzeigen können. Um diese Gruppen zu sehen, wählen Sie Geräte-Gruppen im Navigationsbereich. 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 läuft einmal.
- Fortlaufend: Nach dem ersten Lauf wird der Job auf jedem Gerät ausgeführt, das der Gruppe hinzugefügt wird.

Weitere Informationen zum Erstellen und Verwalten von Auftragsvorlagen finden Sie unter [Auftragsvorlagen](#) aus. Weitere Informationen zur Funktionsweise von Aufträgen finden Sie unter [Jobs](#) aus.

Ausführen von Aufgaben

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

1. Wählen Sie eine Gruppe oder ein oder mehrere Geräte als Ziel aus.
2. Wählen Sie Run job (Aufgabe ausführen) aus.
3. WÄHLEN SIE EIN ZIEL AUS, WÄHLEN SIE ENTWEDER KONTINUIERLICHE ODER SCHNAPPSCHUSS AUS.
4. Wählen Sie eine Auftragsvorlage aus. Stellen Sie sicher, dass der Text unter Auftragsübersicht beschreibt die Art des Auftrags, den Sie ausführen möchten.
5. Geben Sie optional einen Namen für die Aufgabe ein.
6. Wählen Sie Run (Ausführen) aus.

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

- Die Registerkarte Geräteliste im Dashboard.
- Die Detailseite eines bestimmten Geräts.
- Seite Gerätegruppen.
- Die Detailseite einer bestimmten Gerätegruppe.

Anzeigen und Verwalten von Aufträgen

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

- Die Job-Listenseite - Auf dieser Seite werden alle Jobs angezeigt, die in Ihrer Flotte ausgeführt werden. Um diese Seite zu sehen, wählen Sie Jobs im Navigationsbereich.
- Die Detailseite für ein bestimmtes Gerät - Auf dieser Seite werden alle auf dem Gerät ausgeführten Jobs angezeigt.

Jeder Job verfügt über 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. Es zeigt auch die folgenden Summen an.

- Anzahl der Durchläufe.
- Anzahl der abgebrochenen Läufe.
- Anzahl der erfolgreichen Läufe.
- Anzahl der fehlgeschlagenen Ausführungen.

- Anzahl der abgelehnten Läufe.
- Anzahl der in die Warteschlange gestellten Läufe
- Anzahl der laufenden Läufe.
- Anzahl der entfernten Läufe.
- Anzahl der Zeitüberschreitungen.

Um einen Auftrag zu stornieren, wählen Sie den Auftrag und anschließend **Abbrechen** aus.

Alarmer

In diesem Abschnitt wird erläutert, wie Fleet Hub AWS IoT Die Geräteverwaltungs-Alarmer funktionieren und führen Sie durch die erforderlichen Schritte zum Erstellen eines Alarms.

Wenn Sie einen Fleet Hub-Alarm erstellen, gilt er für alle Geräte, die derzeit in Ihrem Dashboard angezeigt werden. Wenn Sie keine Anfrage anwenden, gilt der Alarm für alle Geräte in Ihrer Flotte. Informationen zur Verwendung Ihres Dashboards und zum Erstellen von Abfragen finden Sie unter [the section called “Abfragen und Filter”](#) aus.

Alarmer verwenden Amazon CloudWatch (CloudWatch) -Metriken in Kombination mit durchsuchbaren Feldern aus dem AWS IoT Flottenindizierungsservice zum Erstellen von CloudWatch-Alarmen. Sie können beispielsweise einen Alarm erstellen, der eine Amazon-SNS-Nachricht (Amazon Simple Notification Service) generiert, sobald der durchschnittliche Akkuladestand der Geräte in Ihrer Flotte unter 50% liegt.

Fleet Hub-Alarmer verwenden die [GetStatistics](#) und [GetPercentiles](#) Funktionen des Flottenindizierungsdienstes zur Abfrage aggregierter Daten. Wenn Sie beispielsweise einen Alarm erstellen, der ein benutzerdefiniertes numerisches Feld verfolgt, können Sie alarmierende Schwellenwerte 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 zur Abfrage von Aggregatdaten im Flottenindizierungsservice finden Sie unter [Abfragen von Aggregatdaten](#) aus.

Die folgende Tabelle listet einige Beispiele für die Aggregationstypen auf, die für verfügbar sind AWS-verwaltete und benutzerdefinierte Felder.

Feld	Aggregationstyp
Objekttyp(AWS-verwaltetes String-Feld)	Anzahl
Objektgruppe(AWS-verwaltetes String-Feld)	Anzahl
Verbunden(AWS-verwaltetes boolesches Feld) Der Wert von <code>true</code> ist 1. Der Wert von <code>false</code> ist 0.	<ul style="list-style-type: none"> • Maximum • Anzahl • Summe • Minimum • Durchschnitt
<code>shadow.reported.batterylevel</code> (Numerisches Aggregationsfeld, das im Flottenindizierungsdienst erstellt wurde)	<ul style="list-style-type: none"> • Maximum • Anzahl • Summe • Minimum • Durchschnitt • p10 (10. Perzentil) • p50 (50. Perzentil) • p90 (90. Perzentil) • p95 (95. Perzentil) • p99 (99. Perzentil)

Neben der Angabe von Aggregationsfeldern und -typen geben Sie auch die folgenden Werte an.

- Die Dauer (1 Minute oder 5 Minuten), die für den angegebenen alarmierenden Schwellenwert erforderlich ist, um den Alarm auszulösen.
- Einer der folgenden Vergleichsoperatoren, der auf das angegebene Aggregationsfeld und den Typ angewendet werden soll.

- größer
- Größer/Gleich
- Senken
- Niedriger/gleich
- Der Wert, der mit Ihrem angegebenen Vergleichsoperator verwendet werden soll.
- Eine Liste der E-Mail-Adressen von Personen in Ihrer Organisation, die Amazon SNS 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”](#) aus.

Erstellen von Alarmen

In diesem Thema werden Sie durch die erforderlichen Schritte zum Erstellen eines Flottenhubs für AWS IoT Alarm zur Geräteverwaltung. Es geht davon aus, dass Ihr Administrator aus einem Geräteschattenfeld mit dem Namen ein Aggregationsfeld erstellt hat `shadow.reported.batterylevel` aus. Dieses benutzerdefinierte Feld gibt den Akkustand eines Geräts an. Sie müssen Ihren Administrator bitten, durchsuchbare benutzerdefinierte Felder im AWS IoT Flottenindizierungsservice

Der von Ihnen erstellte Alarm sendet eine Amazon Simple Notification Service (Amazon SNS) - Nachricht an eine Liste von Personen in Ihrem Unternehmen, wenn der durchschnittliche Akkustand der Geräte in Ihrer Flotte während eines Zeitraums von 1 Minute unter 50% fällt.

Erstellen einer Flottenhub-Abfrage

1. Navigieren Sie zu Ihrer Fleet Hub-Anwendung.
2. Wenn Sie eine bestimmte Gruppe von Geräten ansprechen möchten, erstellen Sie eine Abfrage. Eine Anleitung zum Erstellen einer einfachen Abfrage finden Sie unter [the section called “Erstellen Sie Abfragen mit Filtern”](#) aus. Wenn Sie keine Abfrage erstellen, gilt Ihr Alarm für alle Geräte in Ihrer Flotte.
3. Wählen Sie auf der Standard-Dashboard-Seite Alarm erstellen aus.
4. Auf der Build-Aggregationsmetrik Überprüfen Sie, ob Ihre Abfrage unter Ziel-Abfrage aus. In der Konfigurieren der Flottenmetrik AggregAbschnitts-Feld wählen, wähle `shadow.reported.batterylevel` aus. Dieses Menü enthält die AWS-verwaltete Felder und die benutzerdefinierten Felder, die Ihr Administrator im AWS IoT Flottenindizierungsservice

5. Für Wählen Sie Aggregationstyp, wählen Average (Durchschnitt) aus. Diese Wahl basiert den Alarm auf den durchschnittlichen Akkustandwert in Ihrer Geräteflotte.
6. Für Zeitraum wählen, wählen 1 Minute aus. Dies löst den Alarm aus, wenn Ihre Geräteflotte eine Minute lang im angegebenen alarmierenden Zustand bleibt.

Wählen Sie Next (Weiter).

7. Auf der Setzen des Schwellwerts Seite, im Löse den Alarm aus, wenn...-Bereich wählen Niedriger/gleichaus. Dies löst den Alarm aus, wenn der durchschnittliche Akkustandwert unter einen von Ihnen angegebenen Wert fällt.
8. In der THANGeben Sie 50 ein.

Wählen Sie Next (Weiter).

9. Auf der Benachrichtigen des Benutzers Seite, im Benachrichtigen - optionale 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 Kommas getrennte Liste mit E-Mail-Adressen ein, um diese Liste aufzufüllen.
10. In der Alarm details Geben Sie einen Namen für Ihren Alarm ein und geben Sie optional eine Beschreibung für Ihren Alarm ein. Wählen Sie Next (Weiter).
11. Auf der Prüfen Überprüfen Sie die Informationen, die Sie auf den vorherigen Seiten eingegeben haben. Wählen Sie Submit (Absenden) aus. Sie kehren zum Standard-Dashboard zurück.
12. Wählen Sie im Standard-Dashboard im linken Navigationsbereich Flottenhub-Alarme aus. Stellen Sie sicher, dass der von Ihnen erstellte Alarm angezeigt wird.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Fehlerbehebung und mögliche Lösungen, mit denen Sie Probleme als Benutzer von Fleet Hub lösen können.

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.

Symptom	Lösung
Ich kann keine benutzerdefinierte Metrik finden.	Bitte Sie Ihren Administrator, die Metrik im Fleet Indexing Service zu erstellen.
Mein Alarm zeigt keine Daten an.	Das Laden von Alarmdaten nimmt einige Minuten in Anspruch.
Ich muss die Geräte ändern, auf die mein Alarm abzielt.	Gehen Sie zu Ihrem Dashboard und ändern Sie die Abfrage.
Ich sehe eine Fehlermeldung, wenn ich die Region in meinem Dashboard ändere.	Bitte Sie Ihren Administrator, sicherzustellen, dass die Flottenindexierung in der von Ihnen ausgewählten Region aktiviert ist.
Der Konnektivitätsstatus meines „Dings“ wird von Fleet Indexing nicht indexiert.	Stellen Sie sicher, dass Ihr Client dieselbe Client-ID wie Thing Name verwendet, wenn er eine Verbindung herstellt AWS IoT. Wenn Ihr Client beim Herstellen einer Verbindung eine andere ID als Thing Name verwendet AWS IoT, wird der Konnektivitätsstatus Ihres „Dings“ von Fleet Indexing nicht indexiert.

Fuhrpark für AWS IoT Gerätemanagement

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Fuhrpark und Ihren anderen AWS -Lösungen aufrechtzuerhalten. AWS stellt die folgenden Überwachungstools bereit, um Fuhrpark zu überwachen, Sie zu informieren, wenn etwas nicht stimmt, und um gegebenenfalls automatische Aktionen durchzuführen.

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im [AWS CloudTrail-Benutzerhandbuch](#).

Themen

- [Protokollierung von Fleet Hub für AWS IoT Gerätemanagement-API-Aufrufe mit AWS CloudTrail](#)

Protokollierung von Fleet Hub für AWS IoT Gerätemanagement-API-Aufrufe mit AWS CloudTrail

Fleet Hub für 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 -Service in Fuhrpark durchführt. CloudTrail erfasst alle API-Aufrufe für Fuhrpark als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe über die Fuhrpark und Codeaufrufe der Fuhrpark.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen in einem Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Fuhrpark. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Event history (Ereignisverlauf) anzeigen.

Mit den von CloudTrail gesammelten Informationen können Sie die an Fuhrpark gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage und weitere Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Fleet Hub-Informationen in CloudTrail

AWS CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Die in Fuhrpark auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderen AWS -Serviceereignissen in Event history (Ereignisverlauf) aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf](#).

Um die Ereignisse in Ihrem AWS Konto einschließlich Ereignissen für Fuhrpark kontinuierlich aufzuzeichnen, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien in einem 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 in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit.

Sie können auch andere AWS -Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#)
- [Empfangen von CloudTrail -Protokolldateien von mehreren Konten](#)

CloudTrail protokolliert alle Fleet Hub-Aktionen. Sie sind in der [AWS IoTAPI-Referenz](#) dokumentiert. Zum Beispiel generieren Aufrufe der `UpdateApplication` Aktionen `CreateApplication` und 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-Benutzeranmeldeinformationen ausgeführt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Grundlegendes zu den Protokolldateieinträgen von Fleet Hub forAWS 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 können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter.

CloudTrail Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

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 Geräteverwaltung AWS IoT

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 Device Management AWS IoT](#)
- [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 [Modell der AWS gemeinsamen Verantwortung](#) und geteilter Verantwortung 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 im [Abschnitt Datenschutz FAQ](#). Informationen zum Datenschutz in Europa finden Sie im [AWS Shared Responsibility Model und](#) im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit 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 FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigen API, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter [Federal Information Processing Standard](#) () 140-3. FIPS

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 arbeiten, API, AWS CLI oder 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 einem externen Server eine

URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

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

Bei Cloud-Implementierungen von Datenströmen schützt Fleet Hub 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. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Fleet Hub-Ressourcen zu nutzen. IAM ist eine AWS-Service , die 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

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 Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Fleet Hub nutzen IAM kann, finden Sie unter[Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM](#).

IAM Administrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Fleet Hub verfassen können. Beispiele für identitätsbasierte Fleet Hub-Richtlinien, die Sie in verwenden könnenIAM, 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 übernehmen. Root-Benutzer des AWS-Kontos

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

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

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

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

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

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 [IAMBenutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind](#).

Eine [IAMGruppe](#) ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Wann sollte ein IAM Benutzer \(statt einer Rolle\) erstellt werden?](#) im IAMBenutzerhandbuch.

IAMRollen

Eine [IAMRolle](#) ist eine Identität innerhalb von Ihnen AWS-Konto, für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die [Rollen wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter [Methoden zur Übernahme einer Rolle](#) im IAMBenutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer Rolle für einen externen Identitätsanbieter](#). Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM-Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** — Ein IAM-Benutzer oder eine Rolle kann eine IAM-Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- **Kontoübergreifender Zugriff** — Sie können eine IAM-Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM
- **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.
- **Zugriffssitzungen weiterleiten (FAS)** — Wenn Sie einen IAM-Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an 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 beim Stellen von FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

- **Service-Rolle** — Eine Service-Rolle ist eine [IAM-Rolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Service-Rolle von innen heraus erstellen, ändern und löschen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).
- **Dienstbezogene Rolle** — Eine dienstverknüpfte Rolle ist eine Art von Service-Rolle, die mit einer Dienst-EC2-Instanz verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- **Auf Amazon ausgeführte Anwendungen EC2** — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden](#).

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden [Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle \(anstelle eines IAM Benutzers\) erstellt werden](#).

Verwalten des Zugriffs mit Richtlinien

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

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAM Richtlinien erstellen im Benutzerhandbuch](#). IAM

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

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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 nicht IAM 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 AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bieten ACLs. 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 eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAM Benutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAM Benutzerhandbuch unter [Berechtigungsgrenzen für IAM Entitäten](#).
- **Dienststeuerungsrichtlinien (SCPs)** — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.

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

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

Wie Fleet Hub for AWS IoT Device Management funktioniert mit IAM

Bevor Sie IAM den Zugriff auf Fleet Hub verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für Fleet Hub verfügbar sind.

IAMFunktionen, die Sie mit verwenden können Fleet Hub for AWS IoT Device Management

IAMMerkmal	Fleet-Hub-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja

IAMMerkmal	Fleet-Hub-Unterstützung
Hauptberechtigungen	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 IAM im IAMBenutzerhandbuch unter [AWS Dienste, die mit funktionieren](#).

Identitätsbasierte Fleet-Hub-Richtlinien

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter [IAMRichtlinien erstellen im Benutzerhandbuch](#). IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der [Referenz zu den IAM JSON Richtlinienelementen](#) im IAMBenutzerhandbuch.

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 anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und

Amazon S3 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 den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal 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 Prinzipalentsität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. 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 [IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff](#).

Politische Maßnahmen für Fleet Hub

Note

Fleet-Hub-Anwendungen verwenden die `AWSIoT FleetHubFederationAccess`-verwaltete Richtlinie. Weitere Informationen finden Sie unter [???](#).

Unterstützt Richtlinienaktionen: Ja

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

Das `Action` Element 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, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API 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 Aktionen](#) in 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 bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem [Amazon-Ressourcennamen \(ARN\)](#) anzugeben. 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 darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren 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](#).

Richtlinien-Bedingungsschlüssel für Fleet Hub

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMRichtlinienelemente: Variablen und Tags](#).

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontext-Schlüssel für AWS globale Bedingungen](#) im IAMBenutzerhandbuch.

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 (ABAC) mit Fleet Hub

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In werden AWS 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, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABAC ist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 finden Sie ABAC unter [Was ist? ABAC](#) im IAM Benutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter [Verwenden der attributbasierten Zugriffskontrolle \(ABAC\)](#). IAM

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 darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen [arbeiten können AWS-Services](#), finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort 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 Rollenwechsel finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. 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 unter IAM](#).

Serviceübergreifende Prinzipal-Berechtigungen für Fleet Hub

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASANfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Fleet Hub

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine [IAMRolle](#), die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschen IAM. Weitere Informationen finden Sie im IAM Benutzerhandbuch unter [Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine](#).

 Warning

Das Ändern der Berechtigungen für eine Servicerolle könnte die Fleet-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 serviceverknüpfte 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 dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter [AWS Dienste, die mit funktionieren](#). IAM 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 von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. AWS API Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter [IAM Richtlinien erstellen](#) 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 AWS im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen](#).
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie [IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen](#). IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten

Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter [IAMJSONRichtlinienelemente: Bedingung](#).

- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtlinienprache (JSON) und den IAM bewährten Methoden entsprechen. IAM Access Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter [IAM Access Analyzer-Richtlinienvvalidierung](#) im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter [Konfiguration des MFA -geschützten API Zugriffs](#) im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter [Bewährte Sicherheitsmethoden IAM im IAM](#) Benutzerhandbuch. IAM

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 einzusehen 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 Anrufe an den AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

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 im [Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM](#) Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die internen und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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 häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Fleet Hub und auftreten können IAM.

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 durchzuführen, 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 `AWSIoT FleetHub Federation Access`-verwaltete Richtlinie. Weitere Informationen finden Sie unter [???](#).

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven `my-example-widget` Ressource anzuzeigen, aber nicht über die fiktiven `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 für 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 Benutzerhandbuch unter [Gewähren des Zugriffs IAM für einen Benutzer in einem anderen AWS-Konto, dem IAM Sie gehören](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund [gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie [IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff](#). IAM

Konformitätsprüfung für Fleet Hub for Device Management AWS IoT

Externe Prüfer bewerten die Sicherheit und Konformität von Fleet Hub im Rahmen mehrerer AWS Compliance-Programme. Dazu gehören SOC PCI RAMPHIPAA, Fed und andere.

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

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

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

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

Note

Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der [Referenz für HIPAA qualifizierte Dienste](#).

- [AWS Ressourcen zur AWS](#) von Vorschriften — Diese Sammlung von Arbeitsmapen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

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 vom [IAMKunden verwaltete Richtlinien zu erstellen](#), die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. 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 im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

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 eine Beschreibung der Richtlinien für Jobfunktionen finden Sie im IAMBenutzerhandbuch unter [AWS Verwaltete Richtlinien für Jobfunktionen](#).

AWS verwaltete Richtlinie: AWSIoT FleetHubFederationAccess

Sie können die `AWSIoT FleetHubFederationAccess` Richtlinie an Ihre IAM Identitäten anhängen.

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-Alarmer beschränkt sind.
- `sns` - Führen Sie Vorgänge zum Erstellen, Lesen, Löschen, Abonnieren und Abbestellen durch. Diese Operationen beziehen sich auf Fleet SNS Hub-Themen.

```
{
  "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-Aktualisierungen der verwalteten Richtlinien AWS

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
AWSIoT FleetHub FederationAccess – 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
AWSIoT FleetHub FederationAccess – 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 hinzugefügt, die es App-Benutzern ermöglicht, die Ausführung eines AWS	15. November 2021

Änderung	Beschreibung	Datum
	IoT Jobs innerhalb der App abzurechnen.	
AWSIoT Fleet Hub Federation Access – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat neue Berechtigungen für App-Benutzer hinzugefügt, um Thing Group-Daten abzurufen und CRUD Operationen an AWS IoT Jobs auszuführen.	24. Mai 2021
AWSIoT Fleet Hub Federation Access – Aktualisierung auf eine bestehende Richtlinie	Fleet Hub hat die Berechtigungen für das Fleet Hub-Dashboard APIs entfernt, das nicht unterstützt wird.	12. April 2021
AWSIoT Fleet Hub Federation Access – 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 Anrufe, 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. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie Ephemeral Diffie-Hellman (E) oder Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) unterstützen. Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. 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. Bei AWS dienstübergreifendem Identitätswechsel kann es zu einem Problem mit dem verwirrten Stellvertreter kommen. 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, sich vor dem Problem des verwirrten Stellvertreters zu schützen, besteht darin, den `aws:SourceArn` globalen Bedingungskontextschlüssel mit dem vollständigen Amazon-Ressourcennamen (ARN) der Ressource zu verwenden. Für Fleet Hub `aws:SourceArn` müssen Sie das folgende Format einhalten: `arn:aws:iot:region:account-id:*`. Stellen Sie sicher, dass `region` entspricht Ihrer Fleet Hub-Region und der `account-id` entspricht Ihrer Kundenkonto-ID.

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 Ihre Fleet Hub-Rolle zu findenARN, 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.

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

Dokumentationsverlauf

In der folgenden Tabelle werden die Aktualisierungen der Dokumentation für Fuhrpark beschrieben. Für Änderungen bei AWS verwaltete Richtlinien für Fleet Hub finden Sie unter [AWS verwaltete Richtlinien für Fuhrpark AWS IoT Gerätemanagement](#) aus.

Änderung	Description	Datum
Fuhrpark für AWS IoT Allgem eine Einführung von Gerätemanagement	Fuhrpark entsprechend den Verbesserungen an Fuhrpark für AWS IoT Geräte management während der Dauer der Vorversion.	25. Mai 2021.
Vorversion von Fuhrpark für AWS IoT Geräte management	Die Vorversion von Fuhrpark für AWS IoT Geräte management aus.	16. Dezember 2020.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.