



Fleet Hub for AWS IoT Device Management ガイド

AWS IoT デバイス管理用の Fleet Hub



AWS IoT デバイス管理用の Fleet Hub: Fleet Hub for AWS IoT Device Management ガイド

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Fleet Hub for AWS IoT Device Management とは?	1
Fleet Hub for AWS IoT Device Management の仕組み	1
Fleet Hub のデータインデックス作成の仕組み	2
Fleet Hub アラームの仕組み	2
Fleet Hub ジョブの仕組み	2
AWS IoT 管理者向けデバイス管理用フリートハブ	3
開始	3
最初の Fleet Hub アプリケーションを作成する	3
Fleet Hub アプリケーション用フリートインデックス作成を管理する	6
Fleet Hub アプリケーションにユーザーをい追加する	7
Fleet Hub for AWS IoT Device Management とインタラクションする AWS のサービスおよび AWS IoT Core サービス	7
トラブルシューティング	9
Fleet Hub for AWS IoT Device Management (ユーザー向け)	11
開始方法	11
最初のクエリを作成する	11
最初のアラームを作成する	12
デバイスの詳細を表示	15
クエリとフィルター	20
ダッシュボードを表示する	20
フィルターを使用してクエリを作成する	22
Fleet Hub for AWS IoT Device Management でのジョブとジョブテンプレートの使用	23
ジョブの実行	24
ジョブの表示と管理	25
Alarms	26
アラームの作成	28
トラブルシューティング	29
Fleet Hub for AWS IoT Device Management のモニタリング	31
AWS CloudTrail を使用した Fleet Hub for AWS IoT Device Management API コールのログ記 録	31
CloudTrail での Fleet Hub 情報	31
Fleet Hub for AWS IoT Device Management ログファイルのエントリについて	33
セキュリティ	35
データ保護	36

保管時の暗号化	37
転送中の暗号化	37
Identity and Access Management	37
対象者	37
アイデンティティを使用した認証	38
ポリシーを使用したアクセスの管理	42
での Fleet Hub for AWS IoT Device Management の仕組み IAM	44
アイデンティティベースポリシーの例	51
トラブルシューティング	54
コンプライアンス検証	56
耐障害性	58
AWS マネージドポリシー	58
AWSIoT FleetHubFederationAccess	59
ポリシーの更新	61
インフラストラクチャセキュリティ	63
サービス間の混乱した代理の防止	63
ドキュメント履歴	65
.....	lxvi

Fleet Hub for AWS IoT Device Management とは？

Fleet Hub for AWS IoT Device Management (Fleet Hub) を使用すると、デバイスフリートの状態をモニタリングするためのスタンドアロンのウェブアプリケーションを構築できます。AWS アカウントを持っていない組織内のユーザーにも、これらのアプリケーションを使用可能な状態にすることができます。Fleet Hub を使用して、運用上の問題やセキュリティ上の問題の調査や是正など、フリート全体の一般的なタスクを管理します。

Fleet Hub には以下の機能があります。

- ほぼリアルタイムでデバイスフリートを監視します。
- 異常な動作について技術者に通知するアラートを設定します。
- ジョブを実行します。

Note

Fleet Hub が接続状況データをインデックスするためには、モノの名前と同じクライアント ID を持つ AWS IoT Core に接続する必要があります。

Fleet Hub for AWS IoT Device Management の仕組み

管理者は Fleet Hub for AWS IoT Device Management を使用して、リソースをプロビジョニングしたり、コードを記述したりすることなく、安全なウェブアプリケーションを数分で作成できます。Fleet Hub を使用して作成したウェブアプリケーションは、Active Directory などの既存の ID システムと統合されます。これにより、管理者は独自の認証および承認モデルを適用できます。

Fleet Hub ウェブアプリケーションは、AWS IoT Core フリートインデックス作成およびデバイスモニタリングと統合されています。これらの統合により、デバイスの状態データを監視し、フリート内のデバイスが指定された状態に達したときにアラームを作成できます。

Fleet Hub のアプリケーションは `AWSIoT FleetHubFederationAccess` 管理ポリシーを使用します。詳細については、「」を参照してください[???](#)

ユースケースの例:

- デバイス接続の問題を視覚化する - フリート内の切断されたデバイスの数、デバイスの最後の接続ステータス、およびデバイスが切断された理由 (1 つまたは複数) を確認できます。

- アラームを設定する - 特定の数のデバイスが切断されたときにアラームをトリガーするしきい値を設定できます。アラームは、特定の理由でデバイス (1 つまたは複数) が切断されたときに通知を発することもできます。その後、詳細なデバイスデータを調べて、調査とトラブルシューティングを行うことができます。
- ジョブを実行する - 1 つ以上のデバイスのリモート操作 (ファームウェアアップデートなど) を実行できます。

Fleet Hub のデータインデックス作成の仕組み

Fleet Hub コンソールを使用して、デバイスフリートのフリートインデックス作成を有効化できます。Fleet Hub でフリートインデックス作成を有効化すると、フリート全体で有効化され、すべての Fleet Hub アプリケーションで使用できるようになります。

有効にすると、フリートインデックス作成により、AWS IoT Core で管理されるすべてのフィールドに自動的にインデックスが付されます。フリートインデックス作成を使用して、Fleet Hub アプリケーションのデータのクエリと集計に使用できるカスタムデータを追加することもできます。

Fleet Hub アラームの仕組み

Fleet Hub ウェブアプリケーションは、ユーザーがアラームを作成できるインターフェイスを提供します。次の手順では、Fleet Hub でアラームを作成する方法を示します。

1. データを集計するクエリを作成する - 検索可能なフィールドを使用して、ユーザーが対象とするデバイスを集計するクエリを指定します。
2. しきい値を設定する - インデックス付きデータの条件 (指定された間隔での接続ステータスなど) に達したときにアラームをトリガーするしきい値を設定します。
3. 通知を設定する - 指定されたデバイスがアラーム状態になったときに Fleet Hub が通知する受信者のグループを指定します。

Fleet Hub ジョブの仕組み

Fleet Hub コンソールを使用して、デバイスのリモート操作を実行できます。

ジョブテンプレートを有効にすると、Fleet Hub アプリケーションのテンプレートから特定のジョブを作成できます。

AWS IoT 管理者向けデバイス管理用フリートハブ

このセクションには、AWS IoT デバイス管理用の Fleet Hub Web アプリケーションを作成および管理する方法に関する管理者向けのガイダンスが含まれています。

トピック

- [開始](#)
- [Fleet Hub for AWS IoT Device Management とインタラクションする AWS のサービスおよび AWS IoT Core サービス](#)
- [トラブルシューティング](#)

開始

このセクションでは、デバイス管理用 Fleet Hub for AWS IoT Device Management Web アプリケーションを作成して設定する方法について説明します。

トピック

- [最初の Fleet Hub アプリケーションを作成する](#)
- [Fleet Hub アプリケーション用フリートインデックス作成を管理する](#)
- [Fleet Hub アプリケーションにユーザーをい追加する](#)

最初の Fleet Hub アプリケーションを作成する

前提条件


次のリストは、Fleet Hub ウェブアプリケーションを作成するために必要なリソースを記載しています。

- [AWS アカウント](#)。
- アカウントで有効になっている [AWS IAM Identity Center](#)。(このサービスを有効化していない場合、AWS IoT Core コンソール (<https://console.aws.amazon.com/iot/>) で有効にするように求められます。)

最初の Fleet Hub ウェブアプリケーションを作成する

以下の手順では、AWS IoT デバイス管理 Web アプリケーション用フリートハブを作成する方法について説明します。

1. AWS IoT Core コンソール (<https://console.aws.amazon.com/iot/>) に移動し、左側のパネルで [Fleet Hub] を選択し、[アプリケーション] を選択します。
2. アプリケーションのページで、[Create application] (アプリケーションの作成) を選択します。
3. 「IAM ID センターのセットアップ」ページ AWS IAM Identity Center (IAM ID センター) をまだ有効化していない場合は、手順に従って有効化します。AWS Organizations から E メールが送信されます。Eメールのリンクを選択して、IAM Identity Center の有効化を完了します。

 Note

独自の ID プロバイダーを IAM Identity Center に接続できます。詳細については、「[What Is AWS IAM Identity Center?](#)」を参照してください。[外部 ID プロバイダー Connect](#)。

Fleet Hub アプリケーションを作成するときに、IAM Identity Center の組織インスタンスをまだ作成していない場合は、作成する必要があります。作成する Fleet Hub アプリケーションも IAM Identity Center AWS リージョンの組織インスタンスと同じである必要があります。詳細については、「[IAM ID センターと IAM ID センターの組織インスタンスの有効化](#)」を参照してください。

このページには、IAM Identity Center を既に有効化しているかどうかが表示されます。

[次へ] を選択します。

4. AWS IoT インデックスデータページで、「Fleet Hub AWS IoT へのデータフローの仕組み」セクションの情報を確認してください。このページは、AWS IoT Core AWS IoT Core フリートインデックスを有効化および管理できるコンソールのページにリンクしています。このサービスを使用して、レジストリデータ、シャドウデータ、デバイス接続データ (デバイスライフサイクルイベント)、およびデバイス違反データのインデックス作成、検索、集計ができます。AWS IoT Core デフォルトでフリートインデックスが作成する管理フィールドに加えて、カスタムフィールドを作成することもできます。
- フリートインデックス作成を既に有効化している場合、このページには、フリートインデックス作成設定とカスタムフィールドが表示されます。

- Fleet Hub を使用するには、モノのインデックス作成とモノの接続を有効にする必要があります。

フリートインデックス作成設定の管理と確認が完了したら、[Next] (次へ) を選択します。

Fleet Hub アプリケーションのフリートインデックス作成を有効にする方法の詳細については、「[フリートハブアプリケーションのフリートインデックス作成の管理](#)」を参照してください。

5. [Configure application] (アプリケーションの設定) ページの [Application role] (アプリケーションロール) セクションで、新しいサービスロールを作成するか、既存のサービスロールを選択します。Fleet Hub ウェブアプリケーションは、Fleet Hub リソースを使用する場合にこのロールを引き受けます。フェデレーティッドユーザーは、ウェブアプリケーションを使用するときに、ロールと同じアクセス許可を持ちます。
 - 新しいロールを作成する場合、ロール名は次の文字列で始める必要があります。AWSIoT FleetHub_*random_string*。
 - 既存のロールを選択する場合は、そのロールにこのポリシードキュメント内のアクセス許可があることを確認してください。Fleet Hub ウェブアプリケーションに必要なアクセス許可を表示するには、[View role details] (ロールの詳細を表示) を選択します。このページから作成した新しいロールにサービスが適用するポリシードキュメントを表示するウィンドウが開きます。
6. [Configure application] (アプリケーションの設定) ページの [Application properties] (アプリケーションプロパティ) セクションで、アプリケーションの名前を入力します。オプションで、アプリケーションの説明を入力することもできます。

[Create application] を選択します。

7. [Applications] (アプリケーション) ページで、作成したアプリケーションを選択し、[View details] (詳細の表示) を選択します。アプリケーションの詳細を確認します。

Note

Fleet Hub の管理者として問題を解決するための方法の詳細については、「[トラブルシューティング](#)」を参照してください。

Fleet Hub アプリケーション用フリートインデックス作成を管理する

AWS IoT Core コンソールまたはを使用してフリートインデックスを有効にし、[AWS IoT レジストリデータ](#)、AWS IoT [Device Shadow](#) データ、[AWS IoT 接続データ](#)、[AWS IoT Device Defender 違反データのインデックスを作成するデータソースを設定できます](#)。AWS CLI 以下の手順では、コンソールで Fleet Hub for AWS IoT Device Management アプリケーションのフリートインデックス作成を有効化する方法について説明します。AWS IoT Core を使用した手順については AWS CLI、「[Thing のインデックスの管理](#)」を参照してください。

Important

2022 年 7 月 20 日は、AWS IoT Core AWS IoT Device Defender デバイス管理フリートインデックス作成と名前付きシャドウの統合および違反検出の一般提供リリースです。この一般提供版 (GA) リリースにより、ユーザーはシャドウ名を指定して、特定の名前付きシャドウにインデックスを付けることができます。2021 年 11 月 30 日から 2022 年 7 月 19 日までのこの機能のパブリックプレビュー期間中に、インデックス作成のために名前付きシャドウを追加した場合は、フリートのインデックス作成設定を再構成して特定のシャドウ名を選択することにより、インデックス作成コストを削減してパフォーマンスを最適化するようお勧めします。フリートインデックス設定を再構成する方法の詳細については、「[Managing fleet indexing](#)」(フリートインデックス作成の管理) を参照してください。

1. AWS IoT Core コンソール (<https://console.aws.amazon.com/iot/>) に移動し、左側のパネルで [設定] を選択します。
2. [Settings] (設定) ページで、[Fleet indexing] (フリートインデックス作成) セクションに移動し、[Manage indexing] (インデックス作成の管理) をクリックします。
3. 「フリートインデックスの管理」ページの「設定」セクションで、「Thing のインデックス作成」と、インデックスを作成するデータソースを選択します。AWS IoT Fleet Hub を使用するには、モノのインデックス作成とモノの接続をアクティブ化する必要があります。
4. (オプション) [Manage fleet indexing] (フリートインデックス作成の管理) ページの [Custom fields for aggregation-optional] (集計のカスタムフィールド-オプション) セクションで、フリートインデックスがデフォルトでインデックスを作成する管理フィールドに加えてカスタムフィールドを作成します。

フリートインデックス作成設定の管理と確認が完了したら、[Next] (次へ) を選択します。

フリートのインデックス作成をして設定を更新するには、しばらく時間がかかる場合があります。フリートインデックス作成を管理する方法の詳細については、「[Managing fleet indexing](#)」を参照してください。

Fleet Hub アプリケーションにユーザーを追加する

Fleet Hub for AWS IoT Device Management Web アプリケーションを新しく作成したときには、ユーザーが含まれていません。自分と組織のメンバーがアプリケーションを使用する前に、ユーザーを追加する必要があります。このトピックの手順では、アプリケーションにユーザーを追加する方法について説明します。

アカウントに AWS IAM Identity Center (IAM Identity Center) を設定して、既存の ID システムからユーザーを追加します。独自の ID プロバイダーを IAM Identity Center に接続できます。詳細については、「[IAM Identity Center とは](#)」を参照してください。

1. [Applications] (アプリケーション) ページで、Fleet Hub アプリケーションリストからウェブアプリケーションを選択します。[View details] を選択します。
2. アプリケーションの詳細ページで、[Add user] (ユーザーの追加) を選択します。
3. [Add Fleet Hub users] (Fleet Hub ユーザーの追加) ウィンドウで、アプリケーションへのアクセスを許可する組織のユーザーを選択します。[Add selected users] (選択したユーザーの追加) を選択します。
4. アプリケーションの詳細ページで、Fleet Hub のユーザーリストで選択したユーザーが表示されていることを確認します。

Fleet Hub for AWS IoT Device Management とインタラクションする AWS のサービスおよび AWS IoT Core サービス

このトピックでは、Fleet Hub for AWS IoT Device Management の機能が、他の AWS のサービスとインタラクションして、Fleet Hub ウェブアプリケーションに機能を提供する方法について説明します。

次の表は、AWS のサービスの Fleet Hub for AWS IoT Device Management が各機能を実装するために何を使用するのかを示しています。

機能	AWS のサービス	説明
Active Directory などの既存の ID システムを統合します。	AWS IAM Identity Center (IAM Identity Center)	<p>既存の ID システムからユーザーを追加するには、アカウントの AWS IAM Identity Center (IAM Identity Center) を設定します。独自の ID プロバイダーを IAM Identity Center に接続できます。</p> <p>詳細については、「AWS IAM Identity Center とは」と「ワークフォースアイデンティティ」を参照してください。</p>
インデックス化されたデータソース内の AWS 管理対象フィールド、カスタムフィールド、および任意の属性を使用してクエリを作成します。	AWS IoT フリートのインデックス作成	<p>フリートインデックス作成は、クラウド上でレジストリデータ、シャドウデータ、およびデバイス接続データ (デバイスライフサイクルイベント) のインデックス作成、検索や集計に使用できるマネージド型サービスです。AWS IoT フリートインデックス作成がデフォルトでインデックス作成する管理フィールドに加えて、集計用のカスタムフィールドを作成することもできます。</p> <p>フリートインデックス作成の詳細については、「フリートインデックス作成サービス」を参照してください。</p>

機能	AWS のサービス	説明
クエリで指定されたデバイスのセット用にアラームを作成します。	Amazon CloudWatch (CloudWatch)	<p>Fleet Hub のダッシュボードには、CloudWatch メトリクスが表示されます。このメトリクスは、検索可能なフィールドと組み合わせて使用して、アラームしきい値を作成できます。例えば、コネクテッドデバイス数が指定した数量を下回るたびに Amazon Simple Notification Service (Amazon SNS) 通知を生成する CloudWatch アラームを作成できます。</p> <p>CloudWatch の詳細については、Amazon CloudWatch とはを参照してください。AWS IoT Core が CloudWatch と連携してメトリクスとアラームを作成する方法の詳細については、CloudWatch を使用して AWS IoT アラームとメトリクスをモニタリングするを参照してください。</p>

トラブルシューティング

このセクションでは、Fleet Hub の管理者として問題を解決するのに役立つトラブルシューティング情報と、考え得る解決策を示しています。

症状	ソリューション
ウェブアプリケーションのリンクが機能しません。	アプリケーションを作成してからリンクが機能するまでには、数時間かかる場合があります。

症状	ソリューション
ウェブアプリケーションにログインできません。	<p>アプリケーションに少なくとも 1 人のユーザーを追加していることを確認します。</p> <p>ロールに次のような適切な信頼関係があることを確認します。</p> <pre data-bbox="829 474 1507 989">{"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazons.com" }, "Action": "sts:AssumeRole" }] }</pre> <p>IAM の信頼関係を編集する方法の詳細については、「Editing the trust relationship for an existing role」を参照してください。</p>
ウェブアプリケーションを作成できません。	ウェブアプリケーションの合計数の制限に達していないことを確認します。
想定されるカスタムフィールドが表示されません。	<p>フリートインデックス作成が正しく設定されていることを確認してください。</p> <p>フリートインデックス作成の詳細については、「フリートインデックス作成サービス」を参照してください。</p>

Fleet Hub for AWS IoT Device Management (ユーザー向け)

このセクションには、Fleet Hub for AWS IoT Device Management ウェブアプリケーションのユーザー向けの情報が含まれています。Fleet Hub アプリケーションの作成およびアプリケーションへのユーザーの追加の詳細については、[AWS IoT 管理者向けデバイス管理用フリートハブ](#) を参照してください。

トピック

- [開始方法](#)
- [クエリとフィルター](#)
- [Fleet Hub for AWS IoT Device Management でのジョブとジョブテンプレートの使用](#)
- [Alarms](#)
- [トラブルシューティング](#)

開始方法

このセクションでは、Fleet Hub for AWS IoT Device Management ウェブアプリケーションの機能の使用を開始する方法について説明します。

トピック

- [最初のクエリを作成する](#)
- [最初のアラームを作成する](#)
- [デバイスの詳細を表示](#)

最初のクエリを作成する

このトピックでは、シンプルな Fleet Hub for AWS IoT Device Management クエリを作成する手順を説明します。クエリは検索クエリシンタックスを使用して指定されています。

前提条件

- デバイス (モノ) を含む AWS IoT Core アカウントに関連付けられた Fleet Hub アプリケーション。
- Fleet Hub アプリケーションを使用する権限を持つ組織内のアカウント。

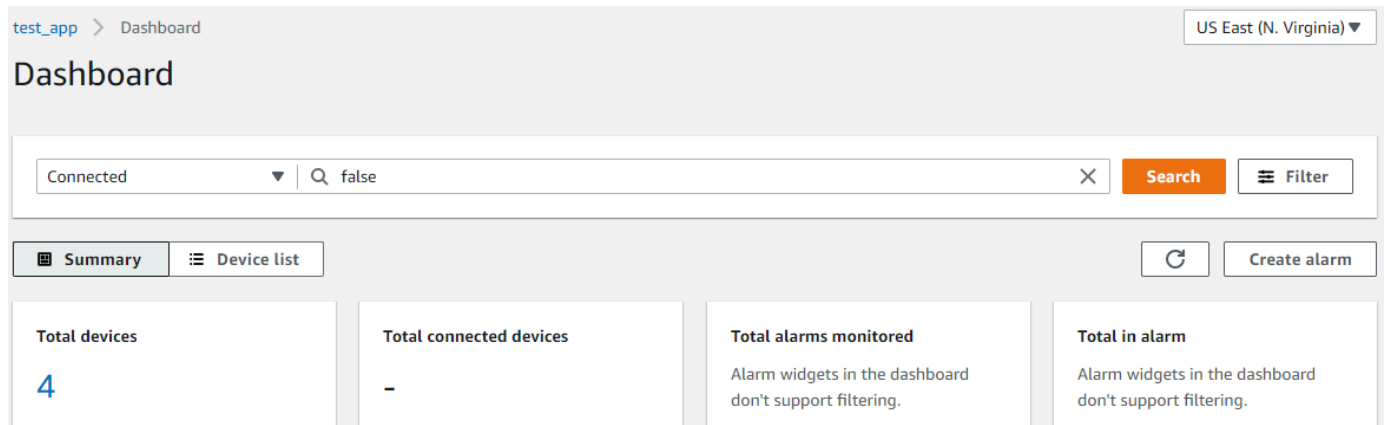
最初の Fleet Hub クエリを作成する

最初の Fleet Hub クエリを作成する

1. Fleet Hub アプリケーションに移動します。

デフォルトのダッシュボードビューには、管理対象の属性とカスタム属性を含むすべてのデバイスのリストが表示されます。属性プレフィックスを含む属性は、カスタム属性です。

2. ページの上部にあるメニューで、[All fields] (すべてのフィールド) から [Connected] (接続済) を選択します。ドロップダウンメニューの隣にあるテキストボックスに **false** と入力します。



3. 検索を実行するには、[Search] (検索) を選択します。AWS IoT Core に接続されていないすべてのデバイスのリストが表示されます。

クエリ構文とクエリの例の詳細については、「[クエリ構文](#)」、「[モノのクエリの例](#)」、および「[モノのグループのクエリの例](#)」を参照してください。

最初のアラームを作成する

このトピックでは、シンプルな Fleet Hub for AWS IoT Device Management アラームを作成する手順を説明します。

前提条件

- デバイス (モノ) を含む AWS IoT Core アカウントに関連付けられた Fleet Hub アプリケーション。
- Fleet Hub アプリケーションを使用する権限を持つ組織内のアカウント。

最初のアラームの作成

最初の Fleet Hub アラームを作成する

1. Fleet Hub アプリケーションに移動します。
2. 特定のデバイスのセットをターゲットにする場合は、クエリを作成します。シンプルなクエリを作成する手順については、「[the section called “最初のクエリを作成する”](#)」を参照してください。クエリを作成しない場合、アラームはフリート内のすべてのデバイスに適用されます。
3. デフォルトのダッシュボードページで、[Create alarm] (アラームの作成) を選択します。
4. [Build aggregation metric] (集計メトリクスの構築) ページで、クエリが [Target query] (ターゲットクエリ) の下に表示されていることを確認します。[Configure fleet metric aggregation] (フリートメトリクス集計を設定) セクションの [Choose field] (フィールドを選択) メニューで、[Connected] (接続済み) を選択します。この AWS 管理フィールドは、デバイスが AWS IoT Core に接続されているかどうかを示します。[Choose field] (フィールドを選択) メニューには、AWS 管理フィールドと、管理者が AWS IoT フリートインデックス作成サービスで作成したカスタムフィールドが含まれています。
5. [Choose aggregation type] (集計タイプを選択) で、次のオプションのいずれかを選択します。
 - Maximum (最大) — 最大しきい値を設定します。
 - Count (カウント) — しきい値として特定のカウントを設定します。
 - Sum (合計) — 合計をしきい値として設定します。
 - Minimum (最小) — 最小しきい値を設定します。
 - Average (平均) — 平均しきい値を設定します。
6. [Choose period] (期間の選択) で、アラームをトリガーする前のメニューで指定された状態の期間を選択します。

[Configure fleet metric aggregation] (フリートメトリクス集計を設定) の設定例は次のようになります。

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 ▼

[Next] (次へ) をクリックします。

7. [Set threshold] (しきい値を設定) ページの [Trigger the alarm whenever...] (次の場合はいつでもアラームをトリガー...) セクションで、次のオプションのいずれかを選択します。

- Greater (より大きい) -- 集計メトリクスとタイプが指定値を超えたときにアラームを発生します。
- Greater/Equal (より大きい/等しい) -- 集計メトリクスとタイプが指定値以上になった場合にアラームを発生します。
- Lower (より小さい) -- 集計メトリクスとタイプが指定値を下回ったときにアラームを発生します。
- Lower/Equal (より小さい/等しい) -- 集計メトリクスとタイプが指定値以下になったときにアラームを発生します。

8. [Than] (よりも) テキストボックスに、アラームのしきい値として使用する値を指定します。

[Set threshold] (しきい値を設定) の設定例は次のようになります。

Trigger the alarm whenever...

Metric is
Define alarm conditions

Greater > threshold

Greater/Equal >= threshold

Lower/Equal <= threshold

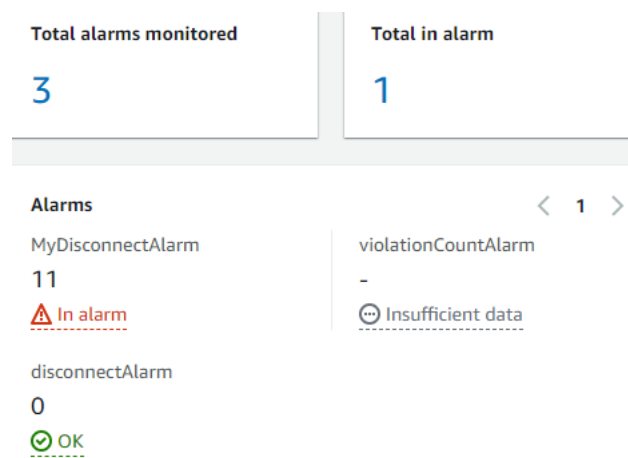
Lower < threshold

Than
Enter a threshold value.

1

[Next] (次へ) をクリックします。

- [Notify user] (ユーザーに通知) ページの [Notify -- optional] (通知 -- オプション) セクションで、アラームがアクティブなときに通知を受信する組織内のユーザーを含むメーリングリストの名前を入力します。E メールアドレスのカンマ区切りリストを入力して、このリストを作成します。
- [Alarm details] (アラームの詳細) セクションで、アラームの名前を入力し、必要に応じてアラームの説明を入力します。[Next] を選択します。
- [Review] (確認) ページで、前のページで入力した情報を確認します。[Submit] (送信) をクリックします。デフォルトのダッシュボードに戻ります。
- デフォルトのダッシュボードでは、アラームウィジェットには、作成したすべてのアラームの情報が表示されます。



作成したアラームの詳細を表示するには、左側のナビゲーションパネルで、[Fleet Hub alarms] (Fleet Hub アラーム) を選択します。

The screenshot shows the 'Fleet Hub alarms' management page with the following table:

Alarm name	Status	Latest update
MyDisconnectAlarm	⚠ Alarm	November 17, 2021 18:20 (UTC)
disconnectAlarm	✅ OK	November 17, 2021 06:15 (UTC)
violationCountAlarm	⚪ Insufficient data	November 17, 2021 06:12 (UTC)

デバイスの詳細を表示

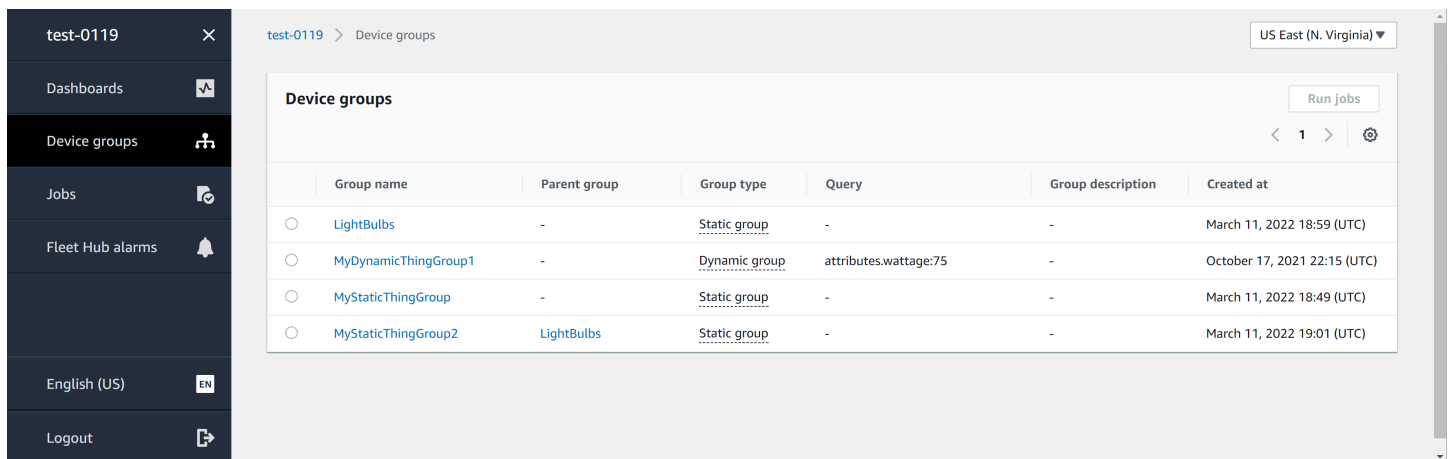
このトピックでは、デバイスグループおよびデバイスに関する詳細を表示する手順を説明します。

前提条件

- デバイス (モノ) を含む AWS IoT Core アカウントに関連付けられた Fleet Hub アプリケーション。
- Fleet Hub アプリケーションを使用する権限を持つ組織内のアカウント。

デバイスグループ

Fleet Hub ウェブアプリケーションにログインすると、左側のナビゲーションパネルに [Device groups] (デバイスグループ) が表示されます。[Device groups] (デバイスグループ) ページには、Fleet Hub ウェブアプリケーション内のすべてのデバイスグループが一覧表示されます。デバイスグループの詳細を表示するには、[Group name] (グループ名) 列で特定のデバイスグループを選択します。



	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)

デバイスグループの詳細

[Device group details] (デバイスグループの詳細) ページには、選択したデバイスグループに関する情報が含まれています。デバイスの詳細を表示するには、[Devices in **XXX**] (XXX のデバイス) セクションの [Device name] (デバイス名) 列から特定のデバイスを選択します。

test-0119 > Device groups > MyDynamicThingGroup1

MyDynamicThingGroup1

[View on dashboard](#) [Run jobs](#)

Group details

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

Devices in MyDynamicThingGroup1 (2)

Find devices

< 1 > ⚙️

Device name
MyLightBulb1
MyLightBulb

Groups in MyDynamicThingGroup1

Find device groups

< 1 > ⚙️

Group name

デバイスの詳細

[Device details] (デバイスの詳細) ページには、選択したデバイスに関する情報が含まれています。

Note

クライアントが AWS IoT へ接続する際に Thing Name とは異なるクライアント ID を使用している場合、「モノ」の接続ステータスはフリートのインデックス作成によってインデックス化されません。

詳細

[Details] (詳細) セクションには、デバイスに関する以下の情報が含まれます。

- デバイス名 — デバイスを表すモノのリソースの名前。詳細については、「[レジストリを使用したモノの管理方法](#)」を参照してください。
- モノのタイプ — デバイスに関連付けられているモノのタイプ。モノのタイプを使用すると、同じモノのタイプを持つすべてのモノに共通する情報を保存できます。詳細については、「[モノのタイプ](#)」を参照してください。
- 最終接続のタイムスタンプ — デバイスが最後に AWS IoT に接続したときのタイムスタンプ。
- 共有可能なデバイスリンク — 選択したデバイスの [Device details] (デバイスの詳細) ページを指す、共有可能なリンク。
- 前回の接続ステータス — AWS IoT へのデバイスの接続ステータス。デバイスが接続されている場合、値は *true*。接続されていない場合、値は *false*。
- 切断の理由 — デバイスの接続が切断された理由。

報告されたデータ

[Reported data] (報告されたデータ) セクションには、デバイスのレジストリデータ、デバイスシャドウデータ、モノのグループに関する情報が含まれています。

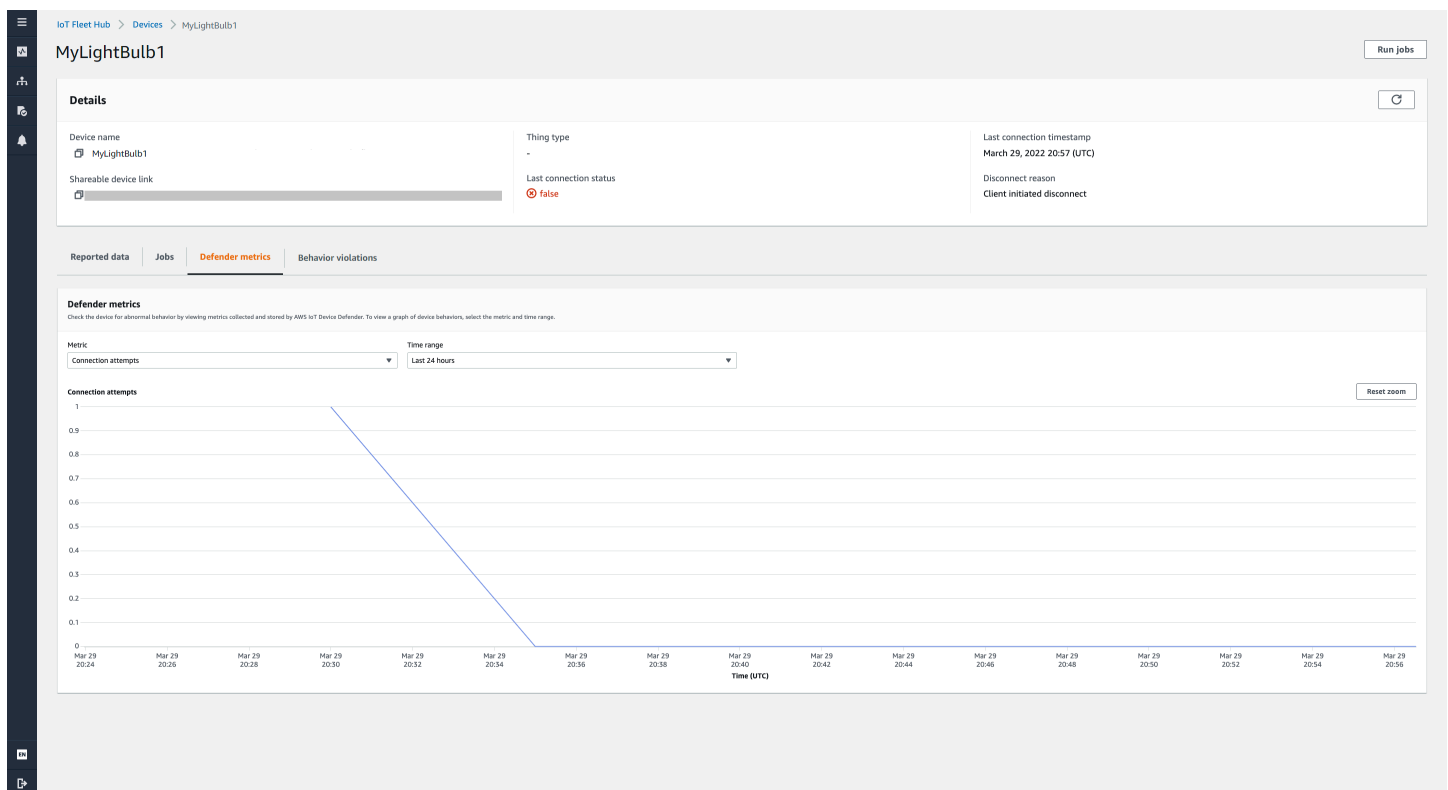
- デバイスフィールド — AWS IoT フリートのインデックス作成におけるデバイスのインデックス付きフィールド。詳細については、「[Managing fleet indexing](#)」を参照してください。
- デバイスシャドウ — デバイスに関連付けられているシャドウ。デバイスシャドウには、名前のないクラシックシャドウと名前付きシャドウの両方を含めることができます。詳細については、「[AWS IoT デバイスシャドウ](#)」を参照してください。
- デバイスグループ — デバイスに関連付けられているデバイスグループ。デバイスグループには、モノの静的グループと動的グループの両方を含めることができます。詳細については、「[モノの静的グループ](#)」および「[モノの動的グループ](#)」を参照してください。

ジョブ

[Jobs] (ジョブ) セクションには、デバイスで実行されているすべてのジョブが表示されます。各ジョブには、ターゲットおよびランタイム情報など、ジョブに関する概要情報が表示される詳細ページがあります。詳細については、「[Fleet Hub for AWS IoT Device Management でのジョブとジョブテンプレートの使用](#)」、および「[ジョブ](#)」を参照してください。

Defender メトリクス

[Defender metrics] (Defender メトリクス) セクションには、現在選択されているデバイスに関連する AWS IoT Device Defender メトリクスが表示されます。表示されたメトリクスデータを使用して、選択した時間枠のデバイスのオペレーションを視覚化できます。Fleet Hub アプリケーションから Defender メトリクスのデータを表示するには、まず、Fleet Hub 管理者が、選択したデバイスに関連する AWS IoT Device Defender メトリクスを設定する必要があります。デバイスの AWS IoT Device Defender メトリクスの作成と設定方法の詳細については、「[カスタムメトリクス](#)」、「[デバイス側のメトリクス](#)」、および「[クラウド側のメトリクス](#)」を参照してください。



動作違反

[Behavior violations] (動作違反) セクションには、現在選択されているデバイスに関連するインデックス付き AWS IoT Device Defender の検出違反データを表示されます。動作違反データには、違反回数、最終違反時間、および最終違反メトリクス値を含めることができます。Fleet Hub アプリ

セッションから動作違反データを表示するには、Fleet Hub 管理者がセキュリティプロファイルに AWS IoT Device Defender の動作違反を設定し、[フリートのインデックス作成](#)に AWS IoT Device Defender の違反を設定する必要があります。AWS IoT Device Defender のセキュリティプロファイルで動作違反を設定する方法の詳細については、「[AWS IoT Device Defender 検出](#)」を参照してください。AWS IoT Device Defender の違反の設定方法の詳細については、「[Fleet Hub アプリケーションのフリートのインデックス作成の管理](#)」および「[モノのインデックス作成の管理](#)」を参照してください。

クエリとフィルター

Fleet Hub for AWS IoT Device Management クエリを使用して、デバイスフリート内のモノのリストを作成および表示できます。インデックス付きデータソース内のすべての AWS マネージドフィールド、カスタムフィールド、および属性は、クエリフィルターとして使用できます。AWS IoT フリートインデックス作成 [the section called “Alarms”](#) を使用して、の集計を有効にするカスタムフィールドを作成することもできます。フリートインデックス作成の詳細については、「[フリートインデックス作成サービス](#)」を参照してください。

トピック

- [ダッシュボードを表示する](#)
- [フィルターを使用してクエリを作成する](#)

ダッシュボードを表示する

Fleet Hub for AWS IoT Device Management ウェブアプリケーションにログインすると、フリート内のデバイスに関する 2 つのデータビューを表示するダッシュボードが表示されます。

[概要]

概要ビューには、フリート内のすべてのデバイスに関するデータのロールアップビューが表示されます。以下の情報を提供します。

- デバイスの総数
- コネクテッドデバイスの数
- デバイスが切断された理由のリスト
- フリート用に作成したモノのタイプと各タイプのデバイスの数
- フリート用に作成したモノのグループと各グループ内のデバイスの数

Dashboard

All fields ▼ | 🔍 Search by values | Search | Filter

Summary | Device list | Refresh | Create alarm

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 >

test-alarming-alarm 40 ▲ In alarm	test-ok-alarm 40 ● OK
--	--

Device types

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

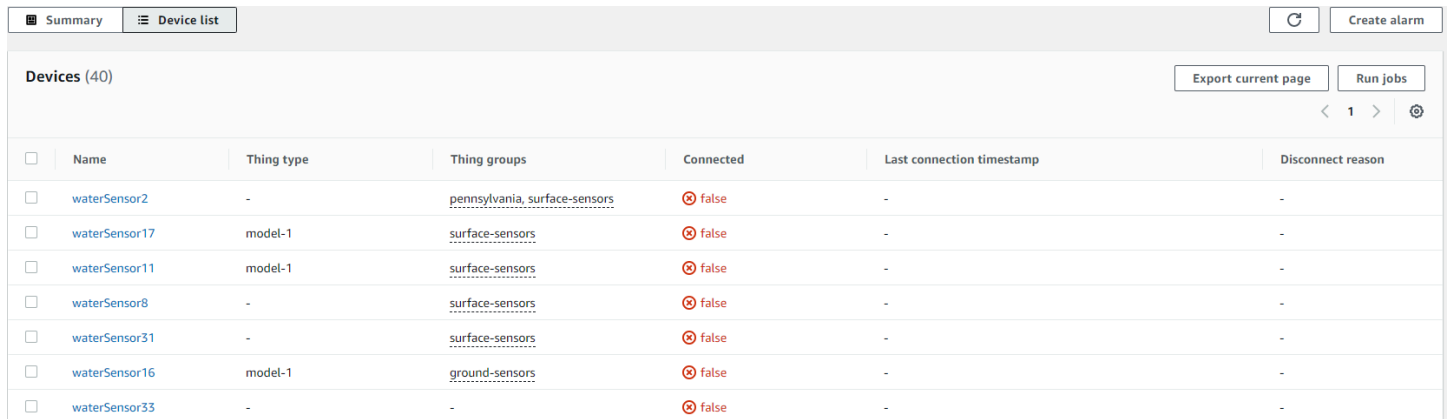
Device groups

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

デバイスリスト

デバイスリストビューには、フリート内のデバイスを一覧表示するテーブルが表示されます。このテーブルには、リストの各デバイスに関する次の情報が表示されます。

- デバイス名
- デバイスの接続ステータス
- デバイスの最後の接続のタイムスタンプ
- 接続されていないデバイスの場合、切断された理由
- デバイスのモノのタイプ
- デバイスのモノのグループ
- フリートインデックス作成サービスで作成したカスタムフィールド



<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	-	-

ページに表示されるデバイスを含むCSVファイルをダウンロードするには、デバイスリストで現在のページをエクスポートを選択します。リストがページ分割されている場合、現在のページで表示されているデータのみがダウンロードされ、後続のページではダウンロードされないことに注意してください。

クエリとフィルターを使用して、最初のビューで概要データを生成し、デバイスリストに表示されるデバイスの数を絞り込むことができます。フリート内のデバイスに関するより具体的な情報を取得するためのクエリとフィルターの使用の詳細については、[the section called “クエリの作成”](#) を参照してください。

フィルターを使用してクエリを作成する

このトピックでは、Fleet Hub for AWS IoT Device Management クエリがどのように機能するかを説明し、フィルターを使用してクエリを作成するために必要な手順について説明します。

クエリを使用して、ダッシュボードの概要とリストビューに表示されるデバイスの数と種類を制御できます。AWSマネージドフィールド、カスタムフィールド、およびフリー AWS IoT トインデックス作成からのインデックス付きデータソースからの属性を使用してクエリをフィルタリングします。フリートインデックス作成の詳細については、「[フリートインデックス作成サービス](#)」を参照してください。

クエリにキーワードを追加することもできます。キーワードは、すべての検索可能なフィールドに適用されます。これらは、1つのクエリで適用できる3つのフィルターの制限にカウントされます。

以下のセクションでは、一般的なクエリの作成に必要な手順について説明します。

クエリの作成

以下の手順では、一般的なクエリを作成する方法について説明します。

前提条件

- 複数のデバイス (モノ) を含む AWS IoT Core アカウントに関連付けられた Fleet Hub アプリケーション
- Fleet Hub アプリケーションを使用するためのアクセス許可を持つアカウント

コンソールでフィルターを使用して最初の Fleet Hub クエリを作成する

1. Fleet Hub アプリケーションに移動します。
2. デフォルトのダッシュボードで、デバイスリストタブと、関連付け AWS IoT Core アカウント内のデバイス (モノ) の総数が表示されていることを確認します。
3. デフォルトのダッシュボードで、[Device list] (デバイスリスト) タブを選択します。管理属性とカスタム属性を含むすべてのデバイスのリストが表示されていることを確認します。カスタム属性には属性プレフィックスが含まれます。
4. ページの上部で、クエリに含めるキーワードを入力します。キーワードクエリはすべてのフィールドに適用されます。
5. ページの上部で、[Filter] (フィルター) を選択します。
6. [Filter] (フィルター) モーダルの [Field] (フィールド) で、フィルターとして使用するフィールドを選択します。[Operator] (演算子) で、オプションを選択します。最後に、[Value] (値) で、フィルターで使用するフィールド値を選択します。

フィルターは 3 つまで追加できます。キーワードクエリは、この数に対してカウントされません。

7. クエリを実行するには、[Apply filters] (フィルターの適用) を選択します。結果には、クエリに一致するすべてのデバイスが表示されます。

Fleet Hub for AWS IoT Device Management でのジョブとジョブテンプレートの使用

Note

ジョブテンプレート機能はプレビュー版のため、変更される可能性があります。

ジョブは、AWS IoT に接続された 1 つ以上のデバイスに送信され実行されるリモート操作です。たとえば、一連のデバイスに対して、アプリケーションやファームウェア更新のダウンロードとインストール、再起動、証明書のローテーション、またはリモートトラブルシューティングオペレーションの実行を指示するジョブを定義できます。Fleet Hub for AWS IoT Device Management ウェブアプリケーションから、事前設定済みのジョブを実行できます。組織の管理者は、ジョブテンプレートを AWS IoT コンソールで作成し、Fleet Hub ユーザーがそのテンプレートを使用できるようにするポリシーをアタッチします。Fleet Hub アプリケーションで、ジョブを実行するデバイスまたはデバイスグループを指定します。

また、管理者は、アプリケーションで表示できるデバイスグループも作成します。これらのグループを表示するには、ナビゲーションペインで [Device groups] (デバイスグループ) を選択します。ターゲットとしてデバイスグループを指定する場合、ジョブの実行方法について、次の 2 種類のオプションのいずれかを指定できます。

- snapshot (スナップショット): ジョブは一度実行されます。
- continuous (継続的): 初回実行後、ジョブはグループに追加されるすべてのデバイスで実行されます。

ジョブテンプレートの作成および管理の詳細については、[ジョブテンプレート](#)を参照してください。ジョブの仕組みについては、[ジョブ](#)を参照してください。

ジョブの実行

Fleet Hub アプリケーションの複数の場所からジョブを実行できますが、以下のステップは常に同じです。

1. ターゲットとしてグループまたは 1 つ以上のデバイスを選択します。
2. [Run job] (ジョブの実行) を選択します。
3. [Job target selection] (ジョブターゲットの選択) で、[continuous] (継続的) または [snapshot] (スナップショット) のいずれかを選択します。
4. ジョブテンプレートを選択します。[Job summary] (ジョブサマリー) に表示されているテキストが、実行するジョブの種類を表していることを確認します。
5. 必要に応じて、ジョブの名前を入力します。
6. [Run] (実行) を選択します。

Fleet Hub アプリケーションの次の場所からターゲットを選択し、これらのステップを実行できます。

- ダッシュボードのデバイスリストタブ。
- 特定のデバイスの詳細ページ。
- デバイスグループページ。
- 特定のデバイスグループの詳細ページ。

ジョブの表示と管理

フリートで実行されているジョブは、次の場所に表示されます。

- ジョブリストページ -- このページには、フリートで実行されているすべてのジョブが表示されます。このページを表示するには、ナビゲーションペインで [Jobs] (ジョブ) を選択します。
- 特定のデバイスの詳細ページ -- このページには、デバイスで実行されているすべてのジョブが表示されます。

各ジョブには、ターゲットおよびランタイム情報など、ジョブに関する概要情報が表示される詳細ページがあります。このページには、各デバイスのジョブのランタイムステータスが表示されます。また、次の総計も表示されます。

- 実行の数。
- キャンセルされた実行の数。
- 成功した実行の数。
- 失敗した実行の数。
- 拒否された実行の数。
- キューに入れられた実行の数。
- 進行中の実行の数。
- 削除された実行の数。
- タイムアウトした実行の数。

ジョブをキャンセルするには、そのジョブを選択し、[Cancel] (キャンセル) を選択します。

Alarms

このセクションでは、Fleet Hub for AWS IoT Device Management アラームの仕組みについて説明し、アラームの作成に必要な手順を順を追って説明します。

Fleet Hub アラームを作成すると、ダッシュボードに現在表示されているすべてのデバイスに適用されます。クエリを適用しない場合、アラームはフリート内のすべてのデバイスに適用されます。ダッシュボードの使用とクエリの作成については、[the section called “クエリとフィルター”](#) を参照してください。

アラームは、Amazon CloudWatch (CloudWatch) メトリクスを AWS IoT フリートインデックス作成サービスの検索可能なフィールドと組み合わせて使用し、CloudWatch アラームを作成します。例えば、フリート内のデバイスの平均バッテリーレベルが 50% を下回るたびに、Amazon Simple Notification Service (Amazon SNS) メッセージを生成するアラームを作成できます。

Fleet Hub のアラームは、フリートインデックス作成サービスの [GetStatistics](#) および [GetPercentiles](#) 機能を使用して、集計データをクエリします。例えば、カスタム数値フィールドを追跡するアラームを作成する場合、指定した属性の次の値に適用されるアラームしきい値を作成できます。

- 最大
- Count (カウント)
- 合計
- Minimum
- 平均
- 10、50、90、95、または 99 パーセンタイルの値

フリートインデックス作成サービスでの集計データのクエリの詳細については、[集計データのクエリ](#) を参照してください。

次の表に、AWS 管理フィールドとカスタムフィールドで使用できる集計タイプの例をいくつか示します。

フィールド	集計タイプ
モノのタイプ (AWS 管理の文字列フィールド)	Count (カウント)

フィールド	集計タイプ
モノのグループ (AWS 管理の文字列フィールド)	Count (カウント)
Connected (AWS 管理のブール型フィールド) true の値は 1 です。false の値は 0 です。	<ul style="list-style-type: none"> • 最大 • Count (カウント) • 合計 • Minimum • 平均
shadow.reported.batterylevel (フリートインデックス作成サービスで作成される数値集計フィールド)	<ul style="list-style-type: none"> • 最大 • Count (カウント) • 合計 • Minimum • 平均 • 10 パーセンタイル値 (t10) • 50 パーセンタイル値 (t50) • 90 パーセンタイル値 (t90) • 95 パーセンタイル値 (t95) • 99 パーセンタイル値 (t99)

集計フィールドと集計タイプの指定に加えて、次の値も指定します。

- 指定したアラームしきい値がアラームをトリガーするのに必要な時間 (1 分または 5 分)。
- 指定した集計フィールドとタイプに適用する次の比較演算子のいずれか。
 - 次よりも大きい
 - 以上
 - Lower
 - 以下
- 指定した比較演算子で使用する値。
- アラームがトリガーされるたびに Amazon SNS メッセージを受信する組織内のユーザーの E メールアドレスのリスト。

- アラーム名。

Fleet Hub アラームを作成するには、「[the section called “アラームの作成”](#)」を参照してください。

アラームの作成

このトピックでは、Fleet Hub for AWS IoT Device Management アラームを作成するために必要なステップについて順を追って説明します。管理者が、shadow.reported.batterylevel という名前のデバイスシャドウフィールドから集計フィールドを作成したことを前提としています。このカスタムフィールドは、デバイスのバッテリーレベルを示します。AWS IoT フリートインデックス作成サービスで検索可能なカスタムフィールドを作成するよう管理者に依頼する必要があります。

作成したアラームは、1 分間にフリート内のデバイスの平均バッテリーレベルが 50% を下回ったときに、組織内のユーザーのリストに Amazon Simple Notification Service (Amazon SNS) メッセージを送信します。

Fleet Hub クエリを作成する

1. Fleet Hub アプリケーションに移動します。
2. 特定のデバイスのセットをターゲットにする場合は、クエリを作成します。シンプルなクエリを作成する手順については、「[the section called “フィルターを使用してクエリを作成する”](#)」を参照してください。クエリを作成しない場合、アラームはフリート内のすべてのデバイスに適用されます。
3. デフォルトのダッシュボードページで、[Create alarm] (アラームの作成) を選択します。
4. [Build aggregation metric] (集計メトリクスの構築) ページで、クエリが [Target query] (ターゲットクエリ) の下に表示されていることを確認します。[Configure fleet metric aggregation] (フリートメトリクス集計の設定) セクションの [Choose field] (フィールドの選択) で、shadow.reported.batterylevel を選択します。このメニューには、AWS 管理フィールドと、管理者が AWS IoT フリートインデックス作成サービスで作成したカスタムフィールドが含まれます。
5. [Choose aggregation type] (集計タイプの選択) で、[Average] (平均) を選択します。この選択肢は、デバイスフリートの平均バッテリーレベル値に基づいてアラームを設定します。
6. [期間の選択] で、[1 分] を選択します。これにより、デバイスフリートが 1 分間指定されたアラーム状態のままとなったときにアラームがトリガーされます。

[Next] を選択します。

7. [しきい値を設定] ページの [次の場合にアラームをトリガー...] セクションで、[以下] を選択します。これにより、平均バッテリーレベル値が指定した値を下回ったときにアラームがトリガーされます。
8. [次よりも:] のテキストボックスで、50 と入力します。

[Next] を選択します。
9. [Notify user] (ユーザーに通知) ページの [Notify -- optional] (通知 -- オプション) セクションで、アラームがアクティブなときに通知を受信する組織内のユーザーを含むメーリングリストの名前を入力します。E メールアドレスのカンマ区切りリストを入力して、このリストを作成します。
10. [Alarm details] (アラームの詳細) セクションで、アラームの名前を入力し、必要に応じてアラームの説明を入力します。[Next] を選択します。
11. [Review] (確認) ページで、前のページで入力した情報を確認します。[Submit] (送信) をクリックします。デフォルトのダッシュボードに戻ります。
12. デフォルトのダッシュボードの左のナビゲーションペインで、[Fleet Hub アラーム] を選択します。作成したアラームが表示されていることを確認します。

トラブルシューティング

このセクションでは、Fleet Hub のユーザーとして問題を解決するのに役立つトラブルシューティング情報と、考え得る解決策を示しています。

症状	ソリューション
クエリにフィルターや用語を追加することができません。	クエリ条件とフィルターが 4 個までという制限に達していないことを確認します。
カスタムメトリクスが見つかりません。	フリートインデックス作成サービスでメトリクスを作成するように管理者に依頼します。
アラームにデータが表示されません。	アラームデータのロードには数分かかります。
アラームがターゲットとするデバイスを変更する必要があります。	ダッシュボードに移動して、クエリを変更します。

症状	ソリューション
ダッシュボードでリージョンを変更すると、エラーが表示されます。	管理者に依頼して、選択したリージョンでフリートインデックス作成が有効になっていることを確認します。
「モノ」の接続状態が、フリートのインデックス作成でインデックス化されていません。	AWS IoT に接続するときは、クライアントが Thing Name と同じクライアント ID を使用していることを確認してください。クライアントが AWS IoT へ接続する際に Thing Name とは異なる ID を使用している場合、「モノ」の接続ステータスはフリートのインデックス作成によってインデックス化されません。

Fleet Hub for AWS IoT Device Management のモニタリング

モニタリングは、Fleet Hub およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。AWS には、Fleet Hub を監視したり、問題が発生したときに報告したり、必要に応じて自動アクションを実行したりするために以下のモニタリングツールが用意されています。

- AWS CloudTrail は、AWS アカウントにより、またはそのアカウントに代わって行われた、API コールおよび関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、[AWS CloudTrail ユーザーガイド](#)を参照してください。

トピック

- [AWS CloudTrail を使用した Fleet Hub for AWS IoT Device Management API コールのログ記録](#)

AWS CloudTrail を使用した Fleet Hub for AWS IoT Device Management API コールのログ記録

Fleet Hub for AWS IoT Device Management は AWS CloudTrail と統合されています。CloudTrail サービスは、ユーザー、ロール、または AWS のサービスが Fleet Hub で実行するアクションの記録を提供します。CloudTrail は、Fleet Hub のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされた呼び出しには、Fleet Hub コンソールからの呼び出しと、Fleet Hub API オペレーションへのコード呼び出しが含まれます。

証跡を作成する場合は、Fleet Hub のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。

CloudTrail が収集する情報を使用して、Fleet Hub に対して行われたリクエスト、リクエスト元の IP アドレス、リクエストを行ったユーザーと時期、および詳細を判別できます。

CloudTrail の詳細については、[AWS CloudTrail ユーザーガイド](#)を参照してください。

CloudTrail での Fleet Hub 情報

AWS CloudTrail は、アカウント作成時に AWS アカウントで有効になります。Fleet Hub でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) 内の他の AWS のサービ

スのイベントとともに CloudTrail イベントに記録されます。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、[CloudTrail イベント履歴でのイベントの表示](#)を参照してください。

Fleet Hub のイベントなど、AWS アカウントのイベントを継続的に記録する場合は、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon Simple Storage Service (Amazon S3) バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。

その他の AWS のサービスを設定して、CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うこともできます。詳細については、以下を参照してください。

- [「追跡を作成するための概要」](#)
- [CloudTrail がサポートされているサービスと統合](#)
- [CloudTrail の Amazon SNS 通知の設定](#)
- [複数のリージョンからの CloudTrail ログファイルの受信](#)
- [複数のアカウントからの CloudTrail ログファイルの受信](#)

CloudTrail は、すべての Fleet Hub アクションを記録します。これらは、[AWS IoT API リファレンス](#)で説明されています。例えば、CreateApplication および UpdateApplication の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと AWS Identity and Access Management ユーザー認証情報のどちらを使用して送信されたか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが、別の AWS のサービスによって送信されたかどうか

詳細については、[CloudTrail userIdentity エlement](#)を参照してください。

Fleet Hub for AWS IoT Device Management ログファイルのエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。

CloudTrail のログファイルには、単一か複数のログエントリがあります。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。

CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Example

次の CloudTrail ログエントリは、CreateApplication アクションに関する情報を示します。

```
{
  "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": "9fffb5d72-9267-4f4e-88e6-d26051133c8c",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
```

Fleet Hub for AWS IoT Device Management のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

セキュリティは、AWS とユーザーの間で共有される責任です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。は、安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#)コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。Fleet Hub に適用されるコンプライアンスプログラムの詳細については、[AWS 「コンプライアンスプログラムによる対象範囲内のサービスコンプライアンス」](#)を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、Fleet Hub for AWS IoT Device Management を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Fleet Hub を設定する方法を示します。また、Fleet Hub リソースのモニタリングと保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- [Fleet Hub でのデータ保護](#)
- [の ID とアクセスの管理 Fleet Hub for AWS IoT Device Management](#)
- [Fleet Hub for AWS IoT Device Management のコンプライアンス検証](#)
- [AWS IoT デバイス管理用の Fleet Hub の耐障害性](#)
- [AWS Fleet Hub for AWS IoT Device Management の 管理ポリシー](#)
- [Fleet Hub for AWS IoT Device Management のインフラストラクチャセキュリティ](#)
- [サービス間の混乱した代理の防止](#)

Fleet Hub でのデータ保護

責任 AWS [共有モデル](#)、Fleet Hub for AWS IoT Device Management のデータ保護に適用されます。このモデルで説明されているように、AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「[データプライバシーFAQ](#)」を参照してください。欧州でのデータ保護の詳細については、[AWS 「責任共有モデル」とGDPR](#) AWS 「セキュリティブログ」のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント、AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1.2 が必要でTLS、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定します AWS CloudTrail。証 CloudTrail 跡を使用して AWS アクティビティをキャプチャする方法については、AWS CloudTrail 「ユーザーガイド」の [CloudTrail 「証跡の操作」](#) を参照してください。
- AWS 暗号化ソリューションと、内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPS エンドポイントの詳細については、「[連邦情報処理標準 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、コンソール、または を使用して Fleet Hub または他の AWS のサービス API AWS CLIを操作する場合も含まれます AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

保管時の暗号化

Fleet Hub は、サーバー側の暗号化により保管中のデータを保護します。詳細については、AWS IoT デベロッパーガイドの [AWS IoTでのデータ暗号化](#) を参照してください。

転送中の暗号化

フローのクラウドデプロイでは、Fleet Hub は Transport Layer Security (TLS) プロトコルを使用して転送中のデータを保護します。詳細については、AWS IoT 開発者ガイドの [AWS IoTのトランスポートセキュリティ](#) を参照してください。

の ID とアクセスの管理 Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つです。IAM 管理者は、Fleet Hub リソースの使用を認証 (サインイン) および承認 (アクセス許可を持つ) できるユーザーを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [での Fleet Hub for AWS IoT Device Management の仕組み IAM](#)
- [のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#)
- [Fleet Hub for AWS IoT Device Management ID とアクセスのトラブルシューティング](#)

対象者

AWS Identity and Access Management (IAM) の使用方法は、Fleet Hub で行う作業によって異なります。

サービスユーザー - ジョブを実行するために Fleet Hub サービスを使用する場合は、管理者が必要なアクセス許可と認証情報を用意します。さらに多くの Fleet Hub 機能を使用して作業を行う場合は、

追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切なアクセス許可をリクエストするのに役に立ちます。Fleet Hub の機能にアクセスできない場合は、[Fleet Hub for AWS IoT Device Management ID とアクセスのトラブルシューティング](#) を参照してください。

サービス管理者 - 社内の Fleet Hub リソースを担当している場合は、通常、Fleet Hub へのフルアクセスがあります。サービスユーザーがどの Fleet Hub 機能およびリソースにアクセスする必要があるかを決定するのは管理者の仕事です。その後、IAM管理者にリクエストを送信して、サービスユーザーのアクセス許可を変更する必要があります。このページの情報を確認して、の基本概念を理解しますIAM。Fleet Hub IAMで を使用する方法の詳細については、「」を参照してください [Fleet Hub for AWS IoT Device Management の仕組み IAM](#)。

IAM 管理者 – IAM管理者の場合は、Fleet Hub へのアクセスを管理するポリシーの作成方法の詳細を知りたい場合があります。で使用できる Fleet Hub アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してください [のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#)。

アイデンティティを使用した認証

認証は、アイデンティティ認証情報 AWS を使用して にサインインする方法です。として、IAMユーザーとして AWS アカウントのルートユーザー、またはIAMロールを引き受けることで、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーテッド ID AWS として にサインインできます。AWS IAM Identity Center (IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーテッド ID の例です。フェデレーテッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることとなります。

ユーザーのタイプに応じて、AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、AWS サインイン ユーザーガイドの [「へのサインイン方法 AWS アカウント」](#) を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。推奨される方法を使用してリクエストに署名する方法の詳細については、IAM 「ユーザーガイド」の [「リクエストの署名 AWS API」](#) を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、AWS IAM Identity Center 「ユーザーガイド」の[「多要素認証の使用」](#)および[「ユーザーガイド」の「多要素認証の使用 \(MFA\) AWS」](#)を参照してください。IAM

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての および リソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインイン ID から始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインしてアクセスします。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するとき使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM 「ユーザーガイド」の[「ルートユーザーの認証情報を必要とするタスク」](#)を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、では、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報 AWS のサービス を使用してアクセスするために ID プロバイダーとのフェデレーションの使用を要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブアイデンティティプロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用してアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、それらはロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソース内のユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、AWS IAM Identity Center 「ユーザーガイド」の[IAM 「Identity Center とは」](#)を参照してください。

IAM ユーザーとグループ

[IAM ユーザー](#)とは、1 人のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成する代わりに、一時的な認証情報に依存することをお勧めします。ただ

し、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM「ユーザーガイド」の[「長期的な認証情報を必要とするユースケースのアクセスキーを定期的にローテーションする」](#)を参照してください。

[IAM グループ](#)は、IAMユーザーのコレクションを指定する ID です。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、という名前のグループがありIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、IAM ユーザーガイドの[（ロールではなく）IAM ユーザーを作成するタイミング](#)を参照してください。

IAM ロール

[IAM ロール](#)は、特定のアクセス許可 AWS アカウント を持つ 内の ID です。ユーザーと似ていますがIAM、特定の人物には関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、[でロールを](#)一時的に引き受けることができます。または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用してロールを引き受けることができますURL。ロールを使用する方法の詳細については、IAM ユーザーガイドの[「ロールを引き受ける方法」](#)を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーテッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、IAM ユーザーガイドの[「サードパーティー ID プロバイダーのロールの作成」](#)を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証された後にアクセスできる内容を制御するために、IAM Identity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の[「アクセス許可セット」](#)を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、特定のタスクに対して異なるアクセス許可を一時的に引き受けるIAMロールを引き受けることができます。

- クロスアカウントアクセス — IAMロールを使用して、別のアカウントの誰か (信頼できるプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の AWS のサービス、(プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、IAM「ユーザーガイド」の「[のクロスアカウントリソースアクセスIAM](#)」を参照してください。
- クロスサービスアクセス — 他の機能 AWS のサービス を使用するものもあります AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したりAmazon S3にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して アクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス または リソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「[アクセスセッションの転送](#)」を参照してください。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受けるIAMロールです。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、IAM「ユーザーガイド」の「[にアクセス許可を委任するロールの作成 AWS のサービス](#)」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示することはできますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な

認証情報を取得できるようにします。詳細については、IAM「[ユーザーガイド](#)」のIAM「[ロールを使用して Amazon EC2 インスタンスで実行されているアプリケーションにアクセス許可を付与する](#)」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、IAM「[ユーザーガイド](#)」の「[\(ユーザーではなく\) IAMロールを作成するタイミング](#)」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御するには、ポリシー AWS を作成し、AWS ID またはリソースにアタッチします。ポリシーは AWS、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義するオブジェクトです。は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM「[ユーザーガイド](#)」のJSON「[ポリシーの概要](#)」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するには、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、iam:GetRoleアクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、AWS Management Console、AWS CLIまたは AWS からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーを作成する方法については、「[ユーザーガイド](#)」のIAM「[ポリシーの作成](#)」を参照してください。IAM

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれてい

まず。マネージドポリシーは、内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには AWS、管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーを選択する方法については、IAM ユーザーガイドの「[マネージドポリシーとインラインポリシーの選択](#)」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。リソースベースのポリシーの例としては、IAM ロール信頼ポリシー と Amazon S3 バケットポリシー があります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはを含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシー IAM では、 から AWS 管理ポリシーを使用することはできません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするアクセス許可を持つかを制御します。ACLs はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用されません。

Amazon S3、および Amazon VPC は AWS WAF、 をサポートするサービスの例です ACLs。の詳細については ACLs、「[Amazon Simple Storage Service デベロッパーガイド](#)」の「[アクセスコントロールリスト \(ACL\) 概要](#)」を参照してください。

その他のポリシータイプ

AWS は、追加の低頻度ポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- **アクセス許可の境界** – アクセス許可の境界は、アイデンティティベースのポリシーが IAM エンティティ (IAM ユーザーまたはロール) に付与できる最大アクセス許可を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境

界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM「ユーザーガイド」の[IAM「エンティティのアクセス許可の境界」](#)を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウントです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します AWS アカウントのルートユーザー。 Organizations との詳細についてはSCPs、AWS Organizations「ユーザーガイド」の[「サービスコントロールポリシー」](#)を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合があります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「ユーザーガイド」の[「セッションポリシー」](#)を参照してください。 IAM

複数のポリシータイプ

1つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「ユーザーガイド」の[「ポリシー評価ロジック」](#)を参照してください。 IAM

での Fleet Hub for AWS IoT Device Management の仕組み IAM

IAM を使用して Fleet Hub へのアクセスを管理する前に、Fleet Hub で使用できるIAM機能について説明します。

IAM で使用できる機能 Fleet Hub for AWS IoT Device Management

IAM 機能	Fleet Hub のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし

IAM 機能	Fleet Hub のサポート
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	可能
ACLs	不可
ABAC (ポリシーのタグ)	可能
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	あり
サービスリンクロール	不可

Fleet Hub およびその他の AWS サービスがほとんどの IAM 機能をどのように動作させるかの概要については、IAM ユーザーガイドの [AWS 「が動作するのサービスIAM」](#) を参照してください。

Fleet Hub の アイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAM ユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーを作成する方法については、IAM 「ユーザーガイド」の [IAM 「ポリシーの作成」](#) を参照してください。

IAM ID ベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、IAM 「ユーザーガイド」の [IAM JSON 「ポリシー要素リファレンス」](#) を参照してください。

Fleet Hub のアイデンティティベースのポリシーの例

Fleet Hub アイデンティティベースのポリシーの例を表示するには、[のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#) を参照してください。

Fleet Hub 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロール信頼ポリシーと Amazon S3 バケットポリシーがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#)必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはを含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、別のアカウントのアカウントまたはIAMエンティティ全体を指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる がある場合 AWS アカウント、信頼されたアカウントのIAM管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、IAM 「ユーザーガイド」の「[のクロスアカウントリソースアクセスIAM](#)」を参照してください。

Fleet Hub のポリシーアクション

Note

Fleet Hub のアプリケーションは AWSIoT FleetHubFederationAccess 管理ポリシーを使用します。詳細については、「[???](#)」を参照してください。

ポリシーアクションのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素は、ポリシー内のアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションは通常、関連付けられた AWS API オペレーションと同じ名前です。一致する API オペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Fleet Hub アクションのリストを確認するには、「サービス認証リファレンス」の「[で定義されるアクション Fleet Hub for AWS IoT Device Management](#)」を参照してください。

Fleet Hub のポリシーアクションは、アクションの前に以下のプレフィックスを使用します。

```
iotfleethub
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

Fleet Hub アイデンティティベースのポリシーの例を表示するには、[のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#) を参照してください。

Fleet Hub のポリシーリソース

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソース [名前 \(ARN\) を使用してリソース](#) を指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Fleet Hub リソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」の「[で定義されるリソース Fleet Hub for AWS IoT Device Management](#)」を参照してください。各リソースARNの を指定できるアクションについては、「[で定義されるアクション Fleet Hub for AWS IoT Device Management](#)」を参照してください。

Fleet Hub アイデンティティベースのポリシーの例を表示するには、[のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#) を参照してください。

Fleet Hub のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの [条件演算子](#) を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1つのステートメントに複数の Condition 要素を指定する場合、または 1つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。1つの条件キーに複数の値を指定すると、は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、IAMユーザー名でタグ付けされている場合のみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「ユーザーガイド」の [IAM 「ポリシー要素: 変数とタグ」](#) を参照してください。IAM

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、ユーザーガイドの [AWS 「グローバル条件コンテキストキー」](#) を参照してください。IAM

Fleet Hub 条件キーのリストを確認するには、「サービス認証リファレンス」の「[の条件キー Fleet Hub for AWS IoT Device Management](#)」を参照してください。条件キーを使用できるアクションとリソースについては、「[で定義されるアクション Fleet Hub for AWS IoT Device Management](#)」を参照してください。

Fleet Hub アイデンティティベースのポリシーの例を表示するには、[のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management](#) を参照してください。

Fleet Hub のアクセスコントロールリスト (ACLs)

をサポートACLs : なし

アクセスコントロールリスト (ACLs) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするアクセス許可を持つかを制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式は使用されません。

Fleet Hub を使用した属性ベースのアクセスコントロール (ABAC)

サポート ABAC (ポリシーのタグ): はい

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認証戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAMエンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、の最初のステップです ABAC。次に、プリンシパルのタグが、アクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可する ABAC ポリシーを設計します。

ABAC は、急速に成長している環境で役立ち、ポリシー管理が面倒になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの[条件要素](#)でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細については ABAC、IAM ユーザーガイドの「[とは ABAC](#)」を参照してください。を設定する手順を含むチュートリアルを表示するには ABAC、IAM ユーザーガイドの「[属性ベースのアクセスコントロールを使用する \(ABAC \)](#)」を参照してください。

Fleet Hub での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービスは、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービスを使用する方法などの詳細については、IAM ユーザーガイドの [AWS のサービスを使用する方法IAM](#)を参照してください。

ユーザー名とパスワード以外のメソッド AWS Management Console を使用して にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、IAM 「ユーザーガイド」の「[ロールへの切り替え \(コンソール\)](#)」を参照してください。

AWS CLI または を使用して、一時的な認証情報を手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して にアクセスできます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「[」の「一時的なセキュリティ認証情報IAM](#)」を参照してください。

Fleet Hub のクロスサービスプリンシパル許可

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービスまたは リソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「[アクセスセッションの転送](#)」を参照してください。

Fleet Hub のサービスロール

サービスロールのサポート: あり

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAM ロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、IAM 「ユーザーガイド」の「[にアクセス許可を委任するロールの作成 AWS のサービス](#)」を参照してください。

⚠ Warning

サービスロールの許可を変更すると、Fleet Hub の機能が破損する可能性があります。Fleet Hub が指示する場合以外は、サービスロールを編集しないでください。

Fleet Hub 用のサービスにリンクされたロール

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示することはできますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、[AWS 「と連携するサービス IAM」](#) を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

のアイデンティティベースのポリシーの例 Fleet Hub for AWS IoT Device Management

デフォルトでは、ユーザーおよびロールには、Fleet Hub リソースを作成または変更するアクセス許可はありません。また、AWS Command Line Interface (AWS CLI) AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するには、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用して IAM ID ベースのJSONポリシーを作成する方法については、IAM 「ユーザーガイド」の[IAM 「ポリシーの作成」](#) を参照してください。

Fleet Hub で定義されるアクションとリソースタイプ、ARNsおよび各リソースタイプの の形式の詳細については、「サービス認証リファレンス」の「[のアクション、リソース、および条件キー Fleet Hub for AWS IoT Device Management](#)」を参照してください。

トピック

- [ポリシーのベストプラクティス](#)
- [Fleet Hub コンソールの使用](#)
- [自分の権限の表示をユーザーに許可する](#)

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Fleet Hub リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを開始し、最小権限のアクセス許可に移行 – ユーザーとワークロードへのアクセス許可の付与を開始するには、多くの一般的なユースケースのアクセス許可を付与する AWS マネージドポリシーを使用します。これらはで使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM 「ユーザーガイド」の「[管理AWS ポリシー](#)」またはジョブ機能の [管理ポリシー](#) を参照してください。 [AWS](#)
- 最小権限のアクセス許可を適用する – IAM ポリシーでアクセス許可を設定する場合、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、IAM 「ユーザーガイド」の「[のポリシーとアクセス許可IAM](#)」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを [を使用して送信する必要があることを指定できますSSL](#)。また、[などの特定の](#) [を通じてサービスアクションが使用されている場合](#) AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「ユーザーガイド」の [IAMJSON 「ポリシー要素: 条件」](#) を参照してください。 IAM
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、IAM 「ユーザーガイド」の [IAM 「Access Analyzer ポリシーの検証」](#) を参照してください。
- 多要素認証が必要 (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、[をオンにMFAしてセキュリティを強化します](#)。API オペレーションが

呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、IAM「ユーザーガイド」の[MFA「保護APIアクセスの設定」](#)を参照してください。

のベストプラクティスの詳細についてはIAM、「ユーザーガイド」の[「のセキュリティのベストプラクティスIAM」](#)を参照してください。IAM

Fleet Hub コンソールの使用

Fleet Hub for AWS IoT Device Management コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、内の Fleet Hub リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または のみを呼び出すユーザーに対して、最小限のコンソールアクセス許可を付与する必要はありません AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションのみへのアクセスを許可します。

ユーザーとロールが引き続き Fleet Hub コンソールを使用できるようにするには、Fleet Hub ConsoleAccessまたは ReadOnly AWS マネージドポリシーをエンティティにアタッチします。詳細については、「ユーザーガイド」の[「ユーザーへのアクセス許可の追加」](#)を参照してください。IAM

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーとマネージドポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
]
```

Fleet Hub for AWS IoT Device Management ID とアクセスのトラブルシューティング

以下の情報は、Fleet Hub と の使用時に発生する可能性のある一般的な問題を診断して修正するのに役立ちますIAM。

トピック

- [Fleet Hub でアクションを実行する権限がない](#)
- [iam を実行する権限がありません。PassRole](#)
- [自分の AWS アカウント以外のユーザーに Fleet Hub リソースへのアクセスを許可したい](#)

Fleet Hub でアクションを実行する権限がない

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

Note

Fleet Hub のアプリケーションは `AWSIoT FleetHubFederationAccess` 管理ポリシーを使用します。詳細については、「[???](#)」を参照してください。

次のエラー例は、`mateojackson` IAM ユーザーがコンソールを使用して架空の `my-example-widget` リソースの詳細を表示しようとしても、架空の `iotfleethub: GetWidget` アクセス許可がない場合に発生します。

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

この場合、Mateo は、`iotfleethub: GetWidget` アクションを使用して `my-example-widget` リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam を実行する権限がありません。PassRole

`iam: PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Fleet Hub にロールを渡すことができるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次のエラー例は、`Mary` という名前の IAM ユーザーがコンソールを使用して Fleet Hub `marymajor` でアクションを実行しようとするると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam: PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント以外のユーザーに Fleet Hub リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、リソースへのアクセスをユーザーに許可できます。

詳細については、以下を参照してください。

- Fleet Hub でこれらの機能がサポートされるかどうかを確認するには、[での Fleet Hub for AWS IoT Device Management の仕組み IAM](#) を参照してください。
- 所有 AWS アカウントしている リソースへのアクセスを提供する方法については、IAM ユーザーガイドの「[所有 AWS アカウントしている別の のIAMユーザーへのアクセスを提供する](#)」を参照してください。
- サードパーティーにリソースへのアクセスを提供する方法については AWS アカウント、IAM ユーザーガイドの「[サードパーティー AWS アカウント が所有する へのアクセスを提供する](#)」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの「[外部認証されたユーザーへのアクセスを提供する \(ID フェデレーション\)](#)」を参照してください。
- クロスアカウントアクセスにロールとリソースベースのポリシーを使用する違いについては、IAM ユーザーガイドの「[のクロスアカウントリソースアクセスIAM](#)」を参照してください。

Fleet Hub for AWS IoT Device Management のコンプライアンス検証


サードパーティーの監査者は、複数のコンプライアンスプログラムの一環として Fleet Hub のセキュリティと AWS コンプライアンスを評価します。これには SOC、PCI、Fed RAMP、HIPAA、その他が含まれます。

AWS のサービスが特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、[AWS のサービス「コンプライアンスプログラムによるスコープ」](#)の「」の「」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードすることができます AWS Artifact。詳細については、「[」の AWS Artifact](#)」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、データの機密性、会社のコンプライアンス目的、および適用される法律と規制によって決まります。は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- [Amazon Web Services HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

 Note

すべての AWS のサービスが HIPAA 対象となるわけではありません。詳細については、[HIPAA 「対象サービスリファレンス」](#)を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界とロケーションに適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- AWS Config デベロッパガイドの [ルールによるリソースの評価](#) – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。
- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、[Security Hub のコントロールリファレンス](#)を参照してください。
- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出できます。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検出要件を満たすことで DSS、PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。

- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクと規制や業界標準へのコンプライアンスの管理を簡素化できます。

AWS IoT デバイス管理用の Fleet Hub の耐障害性

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、および冗長性の高いネットワークで接続された、物理的に分離および分離された複数のアベイラビリティゾーンを提供します。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#)を参照してください。

AWS Fleet Hub for AWS IoT Device Management の 管理ポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも AWS 管理ポリシーを使用する方が簡単です。必要なアクセス許可のみをチームに提供する[IAMカスタマー管理ポリシーを作成するには](#)、時間と専門知識が必要です。すぐに開始するには、AWS マネージドポリシーを使用できます。これらのポリシーは一般的なユースケースを対象としており、AWS アカウントで利用できます。AWS 管理ポリシーの詳細については、「ユーザーガイド」の[AWS 「管理ポリシー」](#)を参照してください。IAM

AWS サービスは、AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が損なわれることはありません。

さらに、は、複数の サービスにまたがるジョブ関数のマネージドポリシー AWS をサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーは、すべての AWS サービスとリソース

への読み取り専用アクセスを提供します。サービスが新機能を起動すると、は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。ジョブ関数ポリシーのリストと説明については、「ユーザーガイド」の[AWS 「ジョブ関数のマネージドポリシー」](#)を参照してください。IAM

AWS マネージドポリシー : AWSIoT FleetHubFederationAccess

ID IAM にAWSIoT FleetHubFederationAccessポリシーをアタッチできます。

このポリシーは、Fleet Hub for AWS IoT Device Management フェデレーテッドユーザーに、Fleet Hub ウェブアプリケーションから AWS IoT やその他の AWS サービスでアクションを実行するために必要なアクセス許可を付与します。

Fleet Hub ウェブアプリケーションへのユーザーの追加の詳細については、[???](#)を参照してください。

このポリシーを [AWS コンソール](#)で表示します。

許可の詳細

このポリシーには、以下の許可が含まれています。

- iot - AWS IoT デバイスデータを取得し、フリートレベルのアクションを実行します。
- iotfleethub - Fleet Hub アプリケーションのメタデータの取得。
- cloudwatch - CloudWatch アラームデータとメトリクスデータを取得します。また、Fleet Hub アラームの範囲内にあるアクションの作成と削除を許可します。
- sns - 作成、読み取り、削除、サブスクライブ、サブスクライブの解除のオペレーションの実行。これらのオペレーションは Fleet Hub SNSトピックを対象としています。

```
{
  "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*"
  }
]
}

```

AWS 管理ポリシーへの Fleet Hub 更新

このサービスがこれらの変更の追跡を開始してからの Fleet Hub AWS の管理ポリシーの更新に関する詳細を表示します。詳細については、Fleet Hub の「[ドキュメント履歴](#)」ページを参照してください。

変更	説明	日付
AWSIoTfleethubFederationAccess - 既存ポリシーへの更新	Fleet Hub に、アプリユーザーが Fleet Hub アプリで AWS IoT Device Defender のメトリクスデータを取得できるようにする新しいアクセス許可が追加されました。	2022 年 4 月 4 日

変更	説明	日付
AWSIoT FleetHub FederationAccess – 既存ポリシーへの更新	Fleet Hub に、アプリケーションユーザーがインデックス作成のために追加のデータソースを取得できるようにする新しいアクセス許可が追加されました。また、アプリケーションユーザーがアプリケーション内で AWS IoT ジョブ実行をキャンセルできるようにするアクセス許可も追加されます。	2021 年 11 月 15 日
AWSIoT FleetHub FederationAccess – 既存ポリシーへの更新	Fleet Hub は、アプリケーションユーザーが Thing Group データを取得し、AWS IoT ジョブに対して CRUD オペレーションを実行するための新しいアクセス許可を追加しました。	2021 年 5 月 24 日
AWSIoT FleetHub FederationAccess – 既存ポリシーへの更新	Fleet Hub は、サポートされていない Fleet Hub ダッシュボードのアクセス許可を削除しました APIs。	2021 年 4 月 12 日
AWSIoT FleetHub FederationAccess – 新しいポリシー	Fleet Hub は、Fleet Hub アプリケーションユーザーがデバイスデータを取得して AWS IoT アクションを実行するために必要なアクセス許可を付与する新しいポリシーを追加しました。	2021 年 4 月 12 日

変更	説明	日付
Fleet Hub は変更の追跡を開始しました	Fleet Hub は AWS 、管理ポリシーの変更の追跡を開始しました。	2021 年 4 月 12 日

Fleet Hub for AWS IoT Device Management のインフラストラクチャセキュリティ

マネージドサービスである Fleet Hub for AWS IoT Device Management は、[Amazon Web Services: セキュリティプロセスの概要](#) ホワイトペーパーで説明されている AWS グローバルネットワークセキュリティ手順によって保護されています。

ネットワーク経由で Fleet Hub にアクセスするには、AWS 公開された API 呼び出しを使用します。クライアントは Transport Layer Security (TLS) 1.2 以降をサポートする必要があります。1.3 TLS を使用することをお勧めします。また、クライアントは、エフェメラルディフィヘルマン (PFS) や楕円曲線エフェメラルディフィヘルマン () など、完全なフォワードシークレット (DHE) を持つ暗号スイートもサポートする必要があります ECDHE。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service \(AWS STS\)](#) を使用して、テナンタリセキュリティ認証情報を生成し、リクエストに署名することもできます。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、あるサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスが操作され、それ自身のアクセス許可を使用して、本来アクセス許可が付与されるべきではない方法で別の顧客のリソースに対して働きかけることがあります。これを防ぐため、AWS では、アカウント内のリソースへのアクセス許可が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシー内では [aws:SourceArn](#) および [aws:SourceAccount](#) のグローバル条件コンテキストキーを使用して、Fleet Hub が別のサービスに付与する、リソースへのアクセス許可を制限することをお勧めします。両方のグローバル条件コンテキストキーを同じポリシーステートメントで使用する場合は、aws:SourceAccount 値と、aws:SourceArn 値に含まれるアカウントが、同じアカウント ID を示している必要があります。

混乱した代理問題から保護する最も効果的な方法は、リソースの完全な Amazon リソースネーム (ARN) でaws:SourceArnグローバル条件コンテキストキーを使用することです。Fleet Hub の場合、aws:SourceArn は arn:aws:iot:*region*:*account-id*:* という形式に従う必要があります。が *region* は Fleet Hub リージョンと *account-id* はカスタマーアカウント ID と一致します。

次の例では、Fleet Hub ロールの信頼ポリシーで aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、「混乱した代理」問題を防ぐ方法を示しています。Fleet Hub ロールを検索するにはARN、AWS IoT コンソールの Fleet Hub セクションに移動し、Fleet Hub アプリケーションを選択してアプリケーションの詳細ページを表示します。

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

ドキュメント履歴

以下の表で、Fleet Hub のドキュメントに対する更新について説明します。Fleet Hub の AWS 管理ポリシーの変更点については、「[Fleet Hub for AWS IoT Device Management の AWS 管理ポリシー](#)」を参照してください。

変更	説明	日付
Fleet Hub for AWS IoT Device Management の一般公開リリース	プレビュー期間中の Fleet Hub for AWS IoT Device Management の改善を反映するためにコンテンツを更新しました。	2021 年 5 月 25 日
Fleet Hub for AWS IoT Device Management のプレビューリリース	Fleet Hub for AWS IoT Device Management ユーザーガイドのプレビューリリースバージョンを公開しました。	2020 年 12 月 16 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。