Fleet Hub for AWS IoT Device Management ガイド

Fleet Hub for AWS IoT Device Management

Fleet Hub for AWS IoT Device Management: Fleet Hub for AWS IoT Device Management ガイド

Table of Contents

AWS は AWS IoT Device Management 2025 年 10 月 18 日に Fleet Hub 機能を停止し、新規顧客を受け入れなくなります。既存の AWS IoT Device Management Fleet Hub のお客様は、2025 年 10 月 17 日まで Fleet Hub を使用できます。詳細については、「Fleet Hub サービス終了のよくある質問」を参照してください。

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。

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認可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 `AWSIoTFleetHubFederationAccess` 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。

管理者向けの Fleet Hub for AWS IoT Device Management

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を作成および管理するための管理者向けガイダンスを示します。

トピック

入門

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

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

次の手順では、Fleet Hub for AWS IoT Device Management ウェブアプリケーション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、次に Applications 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 アイデンティティセンターのセットアップページで (AWS IAM Identity Center IAM アイデンティティセンター) をアクティブ化していない場合は、手順に従ってアクティブ化します。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？」および「Connect to your external ID provider」を参照してください。
   > Fleet Hub アプリケーションを作成するときは、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 アプリケーションは、IAM Identity Center の組織インスタンスと同じ AWS リージョン にある必要があります。詳細については、「IAM Identity Center の有効化」と「IAM Identity Center インスタンスの組織インスタンス」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. インデックス AWS IoT データページで、 から 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ます。このページでは、フリー AWS IoT Core トインデックス作成をアクティブ化および管理できる AWS IoT Core コンソールのページにリンクします。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。フリー AWS IoT Core トインデックス作成がデフォルトでインデックスを作成するマネージド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。`AWSIotFleetHub_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作成 AWS CLI をアクティブ化し、インデックスを作成するようにデータソースを設定できます。AWS IoT レジストリデータ、AWS IoT デバイスシャドウデータ、AWS IoT 接続データ、AWS IoT Device Defender 違反データです。次の手順では、 AWS IoT Core 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にする方法について説明します。を使用してステップを表示するには AWS CLI、「モノのインデックス作成の管理」を参照してください。

> **Important**
>
> 2022 年 7 月 20 日は、 AWS IoT Device Management フリートインデックス作成と AWS IoT Core 名前付きシャドウの統合の一般提供リリースであり、違反 AWS IoT Device Defender を検出します。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作成の管理ページの「設定」セクションで、モノのインデックス作成と AWS IoT インデックスを作成するデータソースを選択します。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い追加する

Fleet Hub for AWS IoT Device Management ウェブアプリケーションには、新しく作成されたユーザーは含まれません。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。

アカウントの 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)	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。 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。
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	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。 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。

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)	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の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。 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。

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

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。	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。 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。

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、管理者向けの Fleet Hub for AWS IoT Device Management を参照してください。

トピック

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

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。

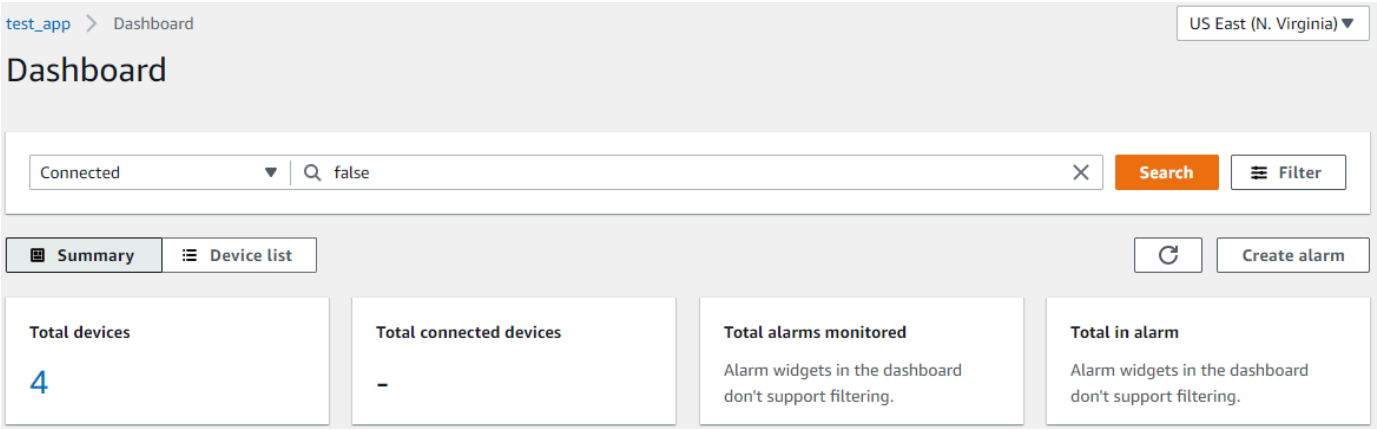
最初のFleet Hub クエリを作成する

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

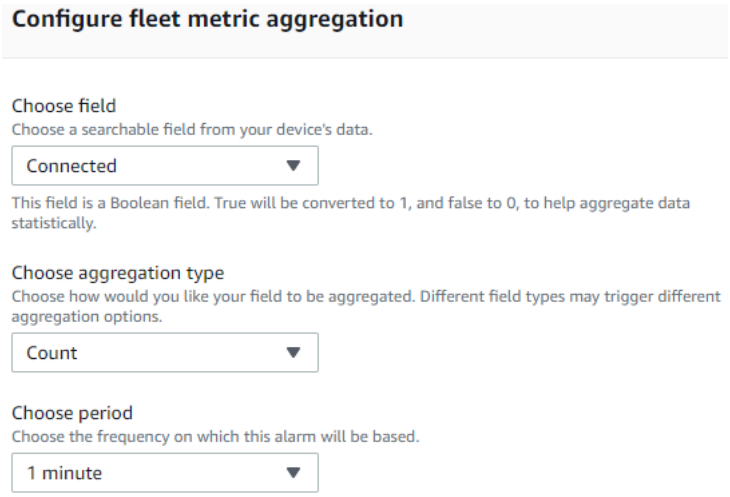
- デバイス (モノ) を含む AWS IoT Core アカウントに関連付けられた Fleet Hub アプリケーション。
- Fleet Hub アプリケーションを使用する権限を持つ組織内のアカウント。

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。



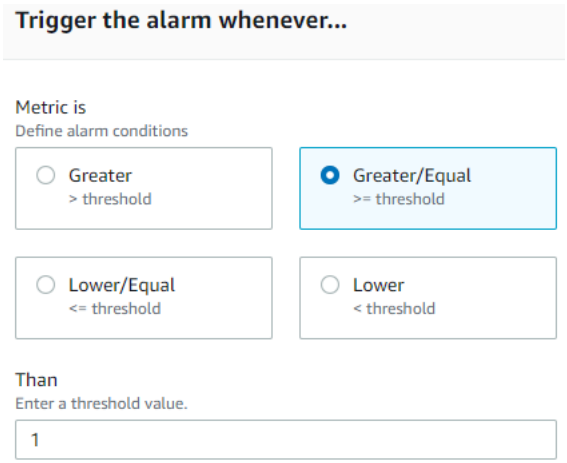
[Next] を選択します。

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。

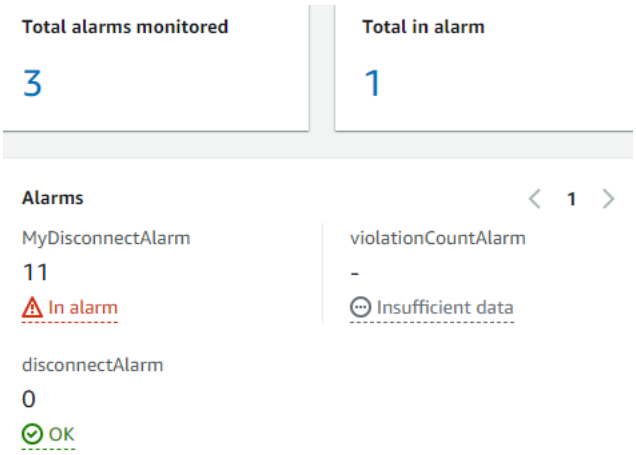
8. [Than] (よりも) テキストボックスに、アラームのしきい値として使用する値を指定します。

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

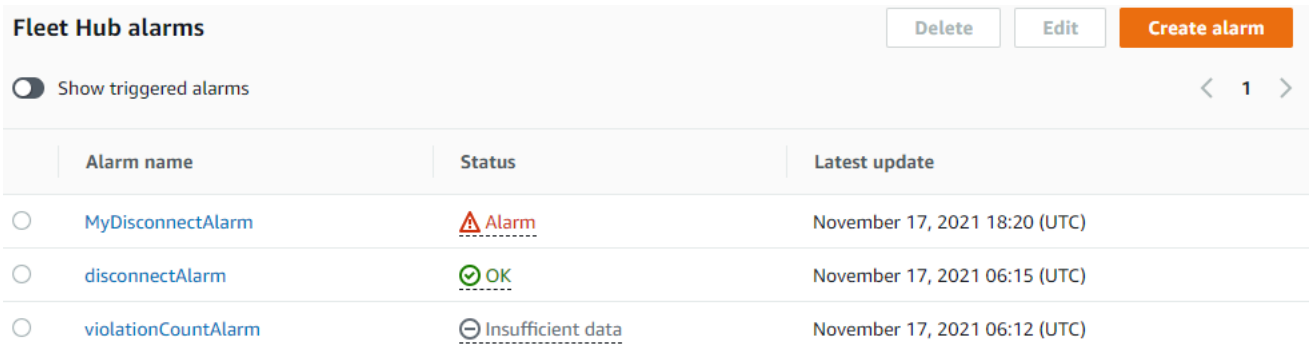


[Next] を選択します。

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。



デバイスの詳細を表示

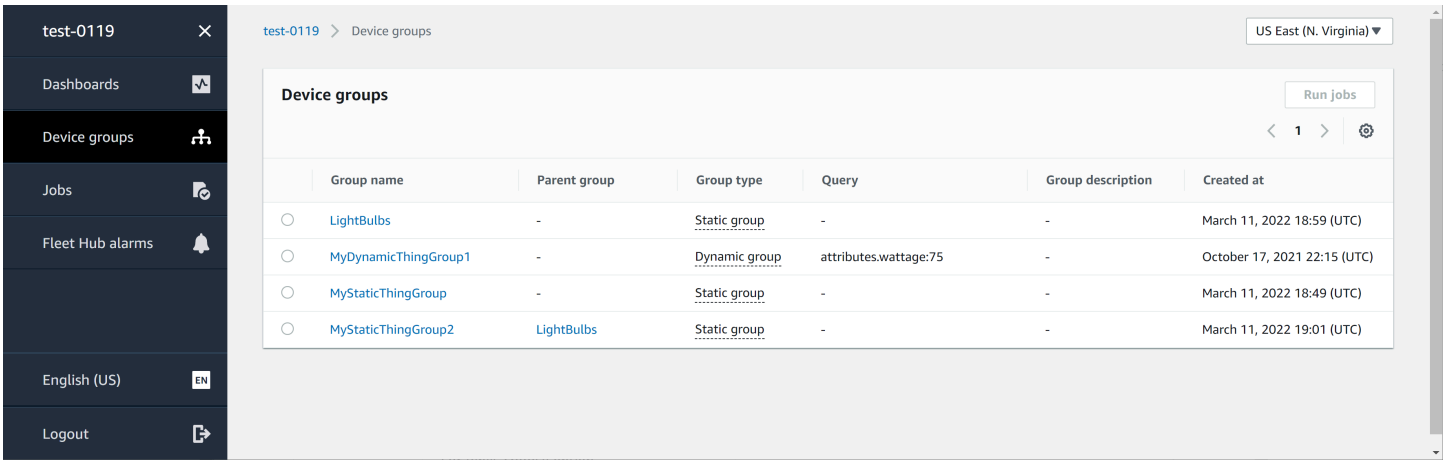
このトピックでは、デバイスグループおよびデバイスに関する詳細を表示する手順を説明します。

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。

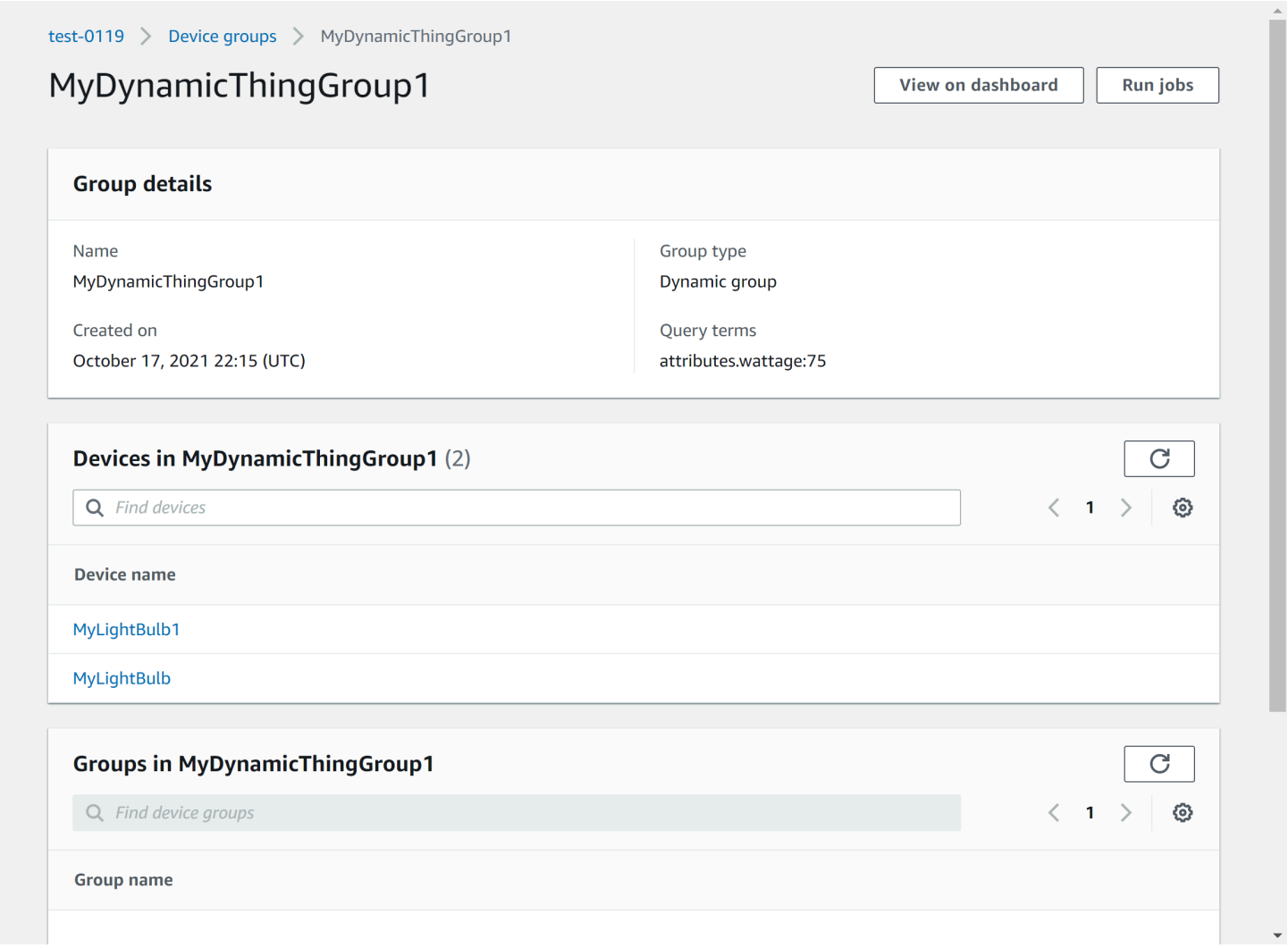
デバイスグループ

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。



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。



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。

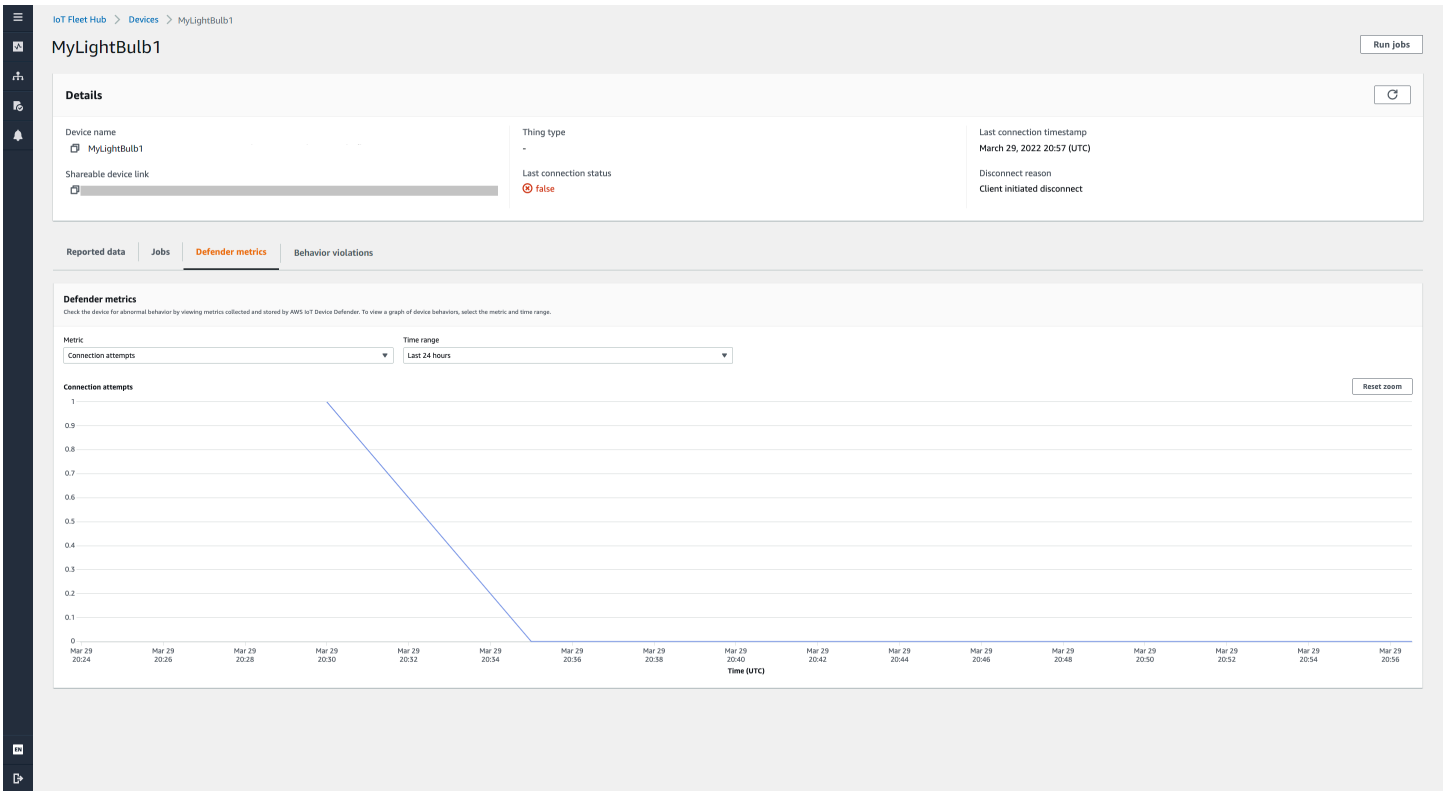
- デバイスグループ — デバイスに関連付けられているデバイスグループ。デバイスグループには、モノの静的グループと動的グループの両方を含めることができます。詳細については、「モノの静的グループ」および「モノの動的グループ」を参照してください。

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

ケー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のすべての AWS 管理対象フィールド、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を使用してカスタムフィールドを作成し、the section called “アラーム” の集約を有効化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

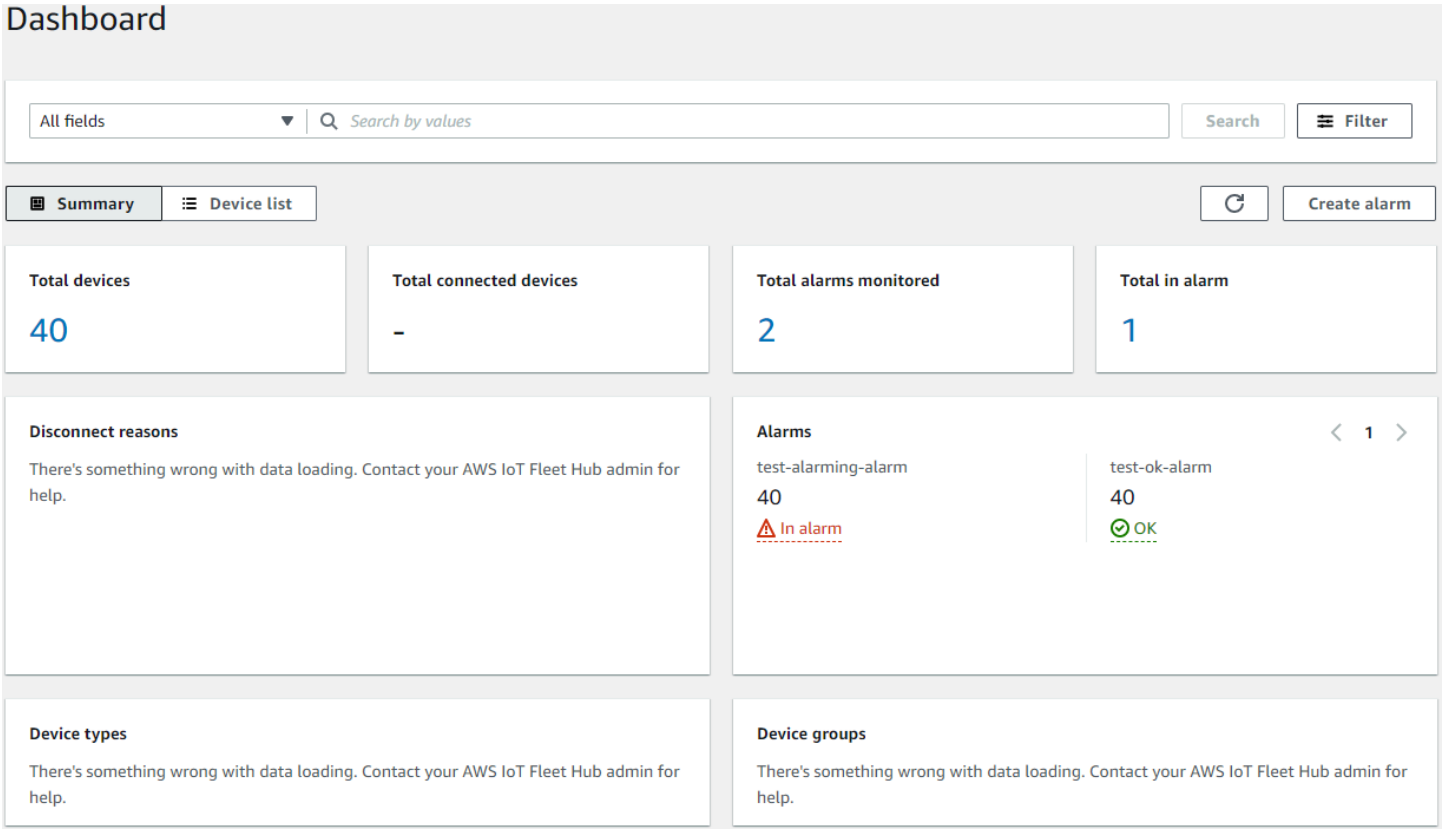
ダッシュボードを表示する

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、ダッシュボードが表示され、フリート内のデバイスに関するデータの 2 つのビューが表示されます。

[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。

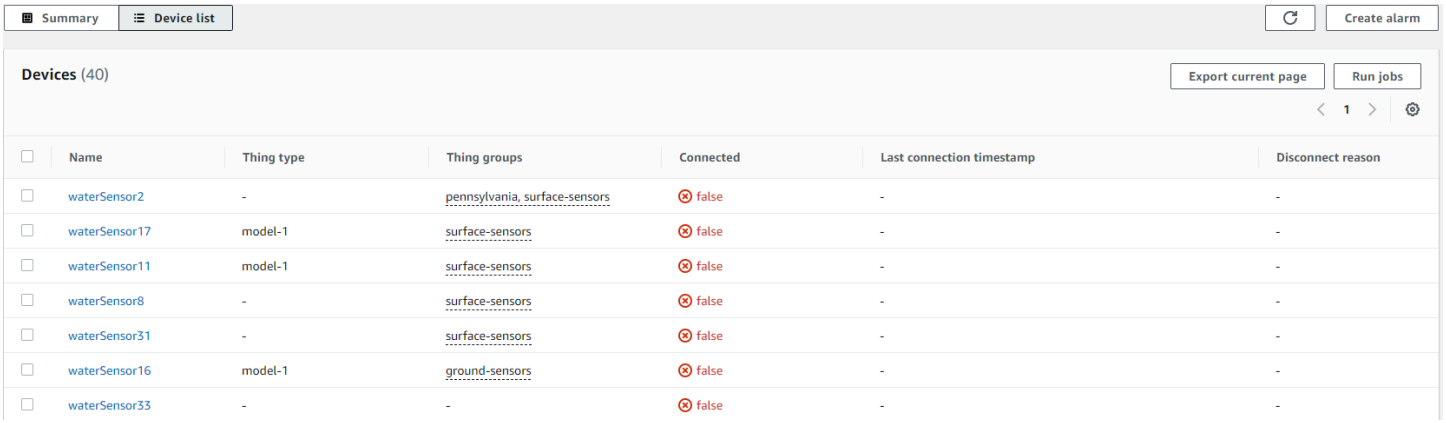
- デバイスの総数
- コネクテッドデバイスの数
- デバイスが切断された理由のリスト
- フリート用に作成したモノのタイプと各タイプのデバイスの数
- フリート用に作成したモノのグループと各グループ内のデバイスの数



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



ページに表示されているデバイスを含む 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 管理対象フィールド、カスタムフィールド、および AWS IoT フリートインデックス作成からインデックス付けされたデータソースの属性を使用して、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、関連する AWS IoT Core アカウントの [Device list] (デバイスリスト) タブとデバイス (モノ) の合計数が表示され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す。
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。

アラーム

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。	• 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)	• 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

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。最近のイベントは、AWSアカウントで表示、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、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。証跡は、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」
- CloudTrail ログファイルの複数のリージョンからの受け取り
- 複数のアカウントから CloudTrail ログファイルを受け取る

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。アイデンティティ情報は、以下を判別するのに役立ちます:

- 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 エレメント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 のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。

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": "9ffb5d72-9267-4f4e-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 、セキュリティを最も重視する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を活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。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。 AWS また、 では、安全に使用できるサービスも提供しています。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、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – 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 を使用する際の責任共有モデルの適用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や保護に役立つ他の 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

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。ユーザーは、このインフラストラクチャでホストされ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に関するよくある質問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 セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR 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 (IAM) 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。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。TLS 1.2 が必須で、TLS 1.3 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。CloudTrail 証跡を使用して 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 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中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 などの高度な管理された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 API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、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、「連邦情報処理規格 (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を、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含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Fleet Hub AWS CLIまたは他の AWS のサービス を使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL 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の場合、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 Identity and Access Management 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、誰を認証 (サインイン) し、誰に Fleet Hub リソースの使用を承認する (アクセス権限を持たせる) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス 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
- が IAM と Fleet Hub for AWS IoT Device Management 連携する方法
- 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権限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、IAM の基本概念を理解してください。お客様の会社で Fleet Hub で IAM を利用する方法の詳細については、が IAM と Fleet Hub for AWS IoT Device Management 連携する方法 を参照してください。

IAM 管理者 - IAM 管理者は、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について確認する場合があります。IAM 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、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。

アイデンティティを使用した認証

認証とは、ID 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によって、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、フェデレーティッド 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 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。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になります。

ユーザーの種類に応じて、 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 AWS アカウント方法」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を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。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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。たとえば、 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」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

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 つのサインインアイデンティティから始めます。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することでアクセスできます。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に使用します。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「ルートユーザー認証情報が必要なタスク」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、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、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

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 ID 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 ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッドアイデンティティがアクセスすると AWS アカウント、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「What is IAM Identity Center?」(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 ユーザーは、単一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保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な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ために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 ユーザーの集団を指定するアイデンティティです。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、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

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「IAM ユーザーに関するユースケース」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。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。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ための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次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 – フェデレーティッド 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。フェデレーティッド 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 (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで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、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では 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における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「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス – 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。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、 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 へのリクエストをリクエストする 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アクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – 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 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、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、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」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 AWS には、ポリシーを作成し、ID AWS 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 のオブジェクトです。 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 に保存されます。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 ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、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方法を問わず、アクションの許可を定義します。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 API からロール情報を取得できます。

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ポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

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す。管理ポリシーは、 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のいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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では、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) 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ための許可を持つかを制御します。ACL 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しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「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) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートしています。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ポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限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 (SCP) を一部またはすべてのアカウントに適用できます。SCP 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を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- 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もあります。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、「IAM 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。

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、「IAM 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。

が IAM と Fleet Hub for AWS IoT Device Management 連携する方法

IAM を使用して Fleet Hub へのアクセスを管理する前に、Fleet Hub で利用できる IAM の機能について学びます。

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

IAM の機能	Fleet Hub のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	あり
ポリシー条件キー	Yes
ACL	いいえ
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	はい
プリンシパル権限	はい
サービスロール	はい
サービスリンクロール	いいえ

Fleet Hub およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」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

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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 ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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では、許可または拒否するアクションとリソース、およびアクションを許可または拒否す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学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。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「IAM でのクロスアカウントリソースアクセス」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 `AWSIoTFleetHubFederationAccess` 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 JSON AWS ポリシーを使用して、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` 要素に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が記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない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、「サービス認可リファレンス」の「Fleet Hub for AWS IoT Device Managementで定義されるアクション」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 JSON AWS ポリシーを使用して、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 リソースネーム (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、リソースレベルのアクセス許可をサポートしないアクションの場合は、ワイルドカード (*) を使用して、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します。

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

Fleet Hub リソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「Fleet Hub for AWS IoT Device Managementで定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、Fleet Hub for AWS IoT Device Managementで定義されるアクション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 JSON AWS ポリシーを使用して、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して、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 ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細

については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

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ています。すべての AWS グローバル条件キーを確認するには、「IAM 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。

Fleet Hub の条件キーのリストを確認するには、「サービス認可リファレンス」の「Fleet Hub for AWS IoT Device Managementの条件キー」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 (ACL)

ACL のサポート: なし

アクセスコントロールリスト (ACL) 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ための許可を持つかを制御します。ACL 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しません。

Fleet Hub での属性ベースのアクセスコントロール (ABAC)

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。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、ABAC の最初の手順です。その後、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した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「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 (ABAC) を使用する」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 などの詳細については、IAM ユーザーガイドの「IAM AWS のサービス と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。たとえば、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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して 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、「IAM の一時的セキュリティ認証情報」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 (FAS) のサポート: あり

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 へのリクエストをリクエストする 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アクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」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

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスにリンクされた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 AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティ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 ポリシーを作成する (コンソール)」を参照してください。

Fleet Hub が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」の「Fleet Hub for AWS IoT Device Managementのアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーに関する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

ポリシーに関する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 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードに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にアクセス許可を付与するAWS 管理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「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な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「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで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、アクションや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 SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、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、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは

100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – 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、MFA をオンに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ときに MFA を必須にするには、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 を使用した安全な API アクセス」を参照してください。

IAM で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「IAM でのセキュリティのベストプラクティス」を参照してください。

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、 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 AWS API のみを呼び出すユーザーには、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。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が許可されます。

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、エンティティに Fleet Hub `ConsoleAccess`または `ReadOnly` AWS 管理ポリシーもアタッチします。詳細については、「IAM 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。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API 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。

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

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

次の情報は、Fleet Hub と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Fleet Hub でアクションを実行する権限がない
- iam:PassRole を実行する権限がない
- AWS 自分の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

にアクションを実行する権限がないと AWS Management Console 通知された場合は、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 AWSIoTFleetHubFederationAccess 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。

以下のエラー例は、mateojackson IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細情報を表示しようとしているが、架空の iotfleethub:*GetWidget* 許可がないという場合に発生します。

```
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* リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam:PassRole を実行する権限がない

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。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Fleet Hub でアクションを実行しようする場合に発生します。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アクセス許可が必要です。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。サインイン資格情報を提供した担当者が管理者です。

AWS 自分の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が、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 (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

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、が IAM と Fleet Hub for AWS IoT Device Management 連携する方法 を参照してください。
- 所有 AWS アカウント している の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。
- リソースへのアクセスをサードパーティーに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「サードパーティーが所有する へのアクセスを提供する AWS アカウント」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「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」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。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

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対象範囲内」を参照して、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 「 Compliance ProgramsAssurance」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できます AWS Artifact。詳細については、「Downloading Reports in 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、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および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。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA の対象となるわけではありません。
- 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、お客様の業界や地域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、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) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス 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。
- 「 デベロッパーガイド」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 Config
- 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把握できます 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一覧については、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 – 不審な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 AWS アカウント、、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 を検出します。GuardDuty を使用すると、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知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。

- 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、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Fleet Hub for AWS IoT Device Management 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ー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、高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、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。アベイラビリティーゾーンは、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ー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 マネージドポリシー

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。チームに必要な権限のみを提供する IAM カスタマーマネージド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、IAM ユーザーガイドの「 AWS 管理ポリシー」を参照してください。

AWS サービスは、 AWS 管理ポリシーを維持および更新します。 AWS 管理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 管理ポリシーは、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。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、Fleet Hub for AWS IoT Device Management フェデレーティッドユーザーに、AWS IoT および Fleet Hub ウェブアプリケーションからの他の 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。

アクセス許可の詳細

このポリシーには、以下のアクセス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 アラームとメトリクスデータの取得。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の範囲は、Fleet Hub SNS トピックに限定されます。

JSON

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

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

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

AWS 管理ポリシーに対する Fleet Hub の更新

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 の AWS 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 - 既存のポリシーを更新します	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	2022 年 4 月 4 日

変更	説明	日付
	にする新しいアクセス許可が追加されました。	
AWSIoTFleetHubFederationAccess - 既存のポリシーを更新します	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。アプリユーザーがアプリ内で 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
AWSIoTFleetHubFederationAccess - 既存のポリシーを更新します	Fleet Hub は、アプリユーザーが 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
AWSIoTFleetHubFederationAccess - 既存のポリシーを更新します	Fleet Hub から、サポートされていない Fleet Hub ダッシュボード API のアクセス許可が削除されました。	2021 年 4 月 12 日
AWSIoTFleetHubFederationAccess – 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 が 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、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で Fleet Hub にアクセスします。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。TLS 1.3 の使用をお勧めします。また、一時的ディフィー・ヘルマン Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM 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、テンポラ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。

不分別な代理処理の問題から保護するための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) を指定しながら、グローバル条件コンテキストキー aws:SourceArn 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。*region* が Fleet Hub リージョンと一致し、*account-id* がお客様のカスタマーアカウント ID と一致することを確認してください。

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 ARN を検索するには、 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。

JSON

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

Fleet Hub end-of-life (EOL) FAQs

フリートハブ end-of-life FAQs

Fleet Hub はいつ になります end-of-lifeか？

AWS は、2025 年 10 月 18 日に Fleet Hub for AWS IoT Device Management を中止します。Fleet Hub はEOL段階的に に移行します。Fleet Hub から利用できる機能は、ビジネスニーズを引き続きサポートするために AWS IoT Device Management コンソールでも利用できます。

1. 2024 年 10 月 17 日、 AWS は Fleet Hub への新規顧客のオンボーディングを停止します。2024 年 10 月 17 日より前に Fleet Hub アプリケーションをお持ちでない場合は、新しい Fleet Hub のカスタマーとして識別されます。それ以外の場合は、既存の Fleet Hub カスタマーとして識別されます。
2. 既存の Fleet Hub のカスタマーは、2025 年 10 月 17 日まで Fleet Hub アプリケーションを引き続き使用できます。2024 年 10 月 17 日から 2025 年 10 月 17 日の間、Fleet Hub には新機能の更新はなく、重要なバグ修正がサポートされ AWS ます。
3. 2025 年 10 月 18 日、 AWS は Fleet Hub for AWS IoT Device Management のサポートを停止します。この日、Fleet Hub は end-of-lifeに到達し、Fleet Hub を使用することはできません。Fleet Hub の終了は他の AWS IoT Device Management 機能には影響しません。が提供する既存の機能を引き続き使用できます AWS IoT Device Management。詳細については、「???」を参照してください。

その日に Fleet Hub アプリケーションは end-of-lifeどうなりますか？

2025 年 10 月 18 EOL日をもって、Fleet Hub アプリケーションは削除され、Fleet Hub にアクセスできなくなります。Fleet Hub に関連付けられた AWS リソースは自動的に削除されません。これらのリソースには、 AWS IoT Device Management ジョブ、フリート AWS IoT Device Management メトリクスなどの Fleet Hub アラームコンポーネント、 CloudWatchアラーム、Amazon SNSトピックが含まれます。これらのリソースには、 から独立して AWS Management Console AWS CLI、または AWS SDKモニタリングのニーズに応じて引き続きアクセスできます。基盤となる AWS リソースを削除するには、「???」を参照してください。

日付以降の基盤となる AWS リソースは end-of-lifeどうなりますか？

Fleet Hub に関連付けられた基盤となる AWS リソースには、モニタリングのニーズ AWS Management Console に応じて から独立して引き続きアクセスできます。これらのリソースには、AWS IoT Device Management ジョブ、 AWS IoT Device Management フリートメトリクスなどの Fleet Hub アラームコンポーネント、 CloudWatchアラーム、Amazon SNSトピックが含まれます。Fleet Hub アプリケーションユーザーは、IAMIdentity Center ユーザープールから自身で割り当てられます。IAM Identity Center ユーザーが Fleet Hub アプリケーションにのみアクセスするために作成されていて、他の AWS サービスに使用していない場合は、コンソール内の IAM Identity Center のユーザーおよびアプリケーションタブから削除できます。詳細については、「???」を参照してください。

日付より前に end-of-life Fleet Hub アプリケーションを削除する方法

EOL 日付より前に Fleet Hub アプリケーションを削除するには、 AWS IoT コンソールまたは `--delete-application` AWS CLI コマンドを使用します。

> **Note**
>
> Fleet Hub アプリケーションを削除しても、Fleet Hub に関連付けられた基盤となる AWS リソースは削除されません。これらのリソースを削除するには、「the section called “基盤となる AWS リソースを削除するにはどうすればよいですか？”」を参照してください。

AWS IoT コンソールを使用して Fleet Hub アプリケーションを削除するには、次の手順に従います。

1. AWS IoT コンソールに移動し、左側のナビゲーションから 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] ページで、削除する Fleet Hub アプリケーションを選択します。[削除] を選択します。アプリケーションの削除を確認するプロンプトウィンドウが表示されます。「delete」と入力して削除を確認し、[delete] を選択します。

を使用して Fleet Hub アプリケーションを削除するには AWS CLI、次の手順に従います。

1. を使用して Fleet Hub アプリケーションを削除するには AWS CLI、アプリケーション ID を知る必要があります。最初に `--list-applications` CLI コマンドを実行して、すべての Fleet Hub アプリケーションとそのアプリケーション を一覧表示しますIDs。

   Fleet Hub アプリケーションを で一覧表示するにはIDs、次のコマンドを実行します。

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

   コマンドの出力は以下のようになります。

   ```
   {
    "applicationSummaries": [
     {
      "applicationId": "68d0603a-66c9-43bf-b93f-a90e7ee5cf76",
      "applicationName": "test_app1",
      "applicationUrl": "https://12ad0603a-66c9-43bf-b93f-
   a90e7ee5cf76.app.iotfleethub.aws",
      "applicationCreationDate": 1698174116,
      "applicationLastUpdateDate": 1698174117,
      "applicationState": "ACTIVE"
     },
     {
      "applicationId": "b6198497-cd5b-400c-9b82-1c82b69cb66c",
      "applicationName": "test_app2",
      "applicationUrl": "https://c6198490-
   cd5a-400c-9b82-1c82b69cb66c.app.iotfleethub.aws",
      "applicationCreationDate": 1684355213,
      "applicationLastUpdateDate": 1684355214,
      "applicationState": "ACTIVE"
   ```

```
  }
 ]
}
```

2. Fleet Hub アプリケーションを削除するには、次の AWS CLI コマンドを実行します。

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

コマンドでは、出力が生成されません。--list-applications CLI コマンドを実行して、指定したアプリケーションが削除されたかどうかを確認できます。

Fleet Hub アプリケーションを削除すると、基盤となるリソースは自動的に削除されますか？

いいえ。Fleet Hub アプリケーションを削除しても、基盤となるリソースは自動的に削除されません。Fleet Hub に関連付けられている AWS リソースを削除するには、「」を参照してください???。

基盤となる AWS リソースを削除するにはどうすればよいですか？

Fleet Hub では、ジョブ AWS IoT Device Management や Fleet Hub アラームなどの AWS リソースを作成できます。Fleet Hub アプリケーションを削除しても、これらのリソースは削除されません。また、??? で説明されているように、ビジネスニーズをサポートするために引き続きアクセスすることができます。これらの基盤となるリソースを削除するには、以下の手順に従います。

ジョブを削除するにはどうすればよいですか？

ジョブを削除するには、まずジョブをキャンセルする必要があります。EOL 日付より前に Fleet Hub から直接ジョブをキャンセルできます。 AWS IoT コンソールを使用して、いつでもジョブをキャンセルおよび削除することもできます。

Fleet Hub アプリケーションからジョブをキャンセルするには

1. Fleet Hub アプリケーションに移動し、[ジョブ] タブを選択します。
2. キャンセルするジョブを選択します。
3. [ジョブをキャンセル] を選択します。

AWS IoT コンソールからジョブをキャンセルおよび削除するには

1. [リモートアクション] に移動し、[ジョブ] タブを選択します。
2. キャンセルするジョブを選択します。
3. [キャンセル] を選択します。
4. 同じ [ジョブ] タブで、削除するジョブを選択します。
5. [削除] を選択します。

Fleet Hub アラームを削除するにはどうすればよいですか？

Fleet Hub アラームは、Fleet Hub アプリケーション内で直接削除できます。これにより、フリートメトリクス、 CloudWatch アラーム、Amazon SNSトピックなど、基盤となるすべてのコンポーネントが自動的に削除されます。Fleet Hub アプリケーションで、[Fleet Hub アラーム] タブに移動し、削除するアラームを選択し、[削除] を選択します。または、 を使用して Fleet Hub アラームを削除することもできます AWS Management Console。 AWS リージョン間で複数のアプリケーションを削除するには、次のステップに従うことをお勧めします。

Fleet Hub アプリケーションから Fleet Hub アラームを削除するには

1. Fleet Hub アプリケーションで、[Fleet Hub アラーム] タブに移動します。
2. 削除するアラームを選択して、[削除] を選択します。このアクションにより、基盤となるすべてのコンポーネントが削除されます。

AWS IoT コンソールからフリートメトリクスを削除するには

1. AWS IoT コンソールから左側のナビゲーションから [管理] に移動します。[すべてのデバイス] から、[フリートメトリクス] を選択します。
2. 名前に「iotfleethub」というプレフィックスが付いたフリートメトリクスをすべて選択します。
3. [削除] を選択します。

CloudWatch コンソールから CloudWatch アラームを削除するには

1. CloudWatch コンソール内のすべてのアラームタブに移動します。
2. 名前に「iotfleethub」というプレフィックスが付いたすべてのメトリクスを選択します。
3. [アクション] に移動し、[削除] を選択します。

Amazon SNSコンソールから作成されたアラームを受信する Amazon SNSトピックを削除するには

1. Amazon SNSコンソールのトピックタブに移動します。
2. 名前に「iotfleethub」というプレフィックスが付いたトピックをすべて選択します。
3. [削除] を選択します。

Fleet Hub から作成された IAM Identity Center ユーザーを削除する方法

IAM Identity Center のユーザーが Fleet Hub アプリケーションにのみアクセスするために作成されていて、他の AWS サービスに使用していない場合は、コンソール内の IAM Identity Center のユーザーおよびアプリケーションタブから削除できます。

日付以降に機能APIsしなくなるもの end-of-lifeは何ですか？

Fleet Hub アプリケーションのライフサイクル管理APIsに関連する はすべて、2025 年 10 月 18 日に廃止されます。APIs これらは Fleet Hub にのみ関連付けられ、他の AWS IoT Device Management 機能には影響しないことに注意してください。既存の Fleet Hub のお客様は、2025 年 10 月 17 APIs 日までこれらを引き続き使用できます。

- CreateApplication
- DeleteApplication
- DescribeApplication
- ListApplication
- ListTagsForResource
- TagResource
- UntagResource
- UpdateApplication

Fleet Hub の既存の機能は何で、コンソールでそれらにアクセスするにはどうすればよいですか？

Fleet Hub には、 機能を使用して構築された以下の主要なモニタリングおよび管理 AWS IoT Device Management 機能があります。これらの機能はすべて Fleet Hub アプリケーション外で利用でき

ます。これらは、ビジネスニーズをサポートするために引き続きアクセスできる AWS IoT Device Management コンソール内に直接存在します。

フリート接続状態の概要

Fleet Hub ダッシュボードは、IoT フリートの接続状態と接続の詳細をまとめたものです。接続されたデバイスの数、切断されたデバイスの数および切断されたデバイスの分散を切断理由別に表示します。同等の接続状態モニタリングダッシュボードは、 AWS IoT コンソールの Monitor タブで使用できます。ウィジェットを有効にして、接続されているデバイスの数、切断率、切断理由を監視できます。詳細については、「AWS IoT Device Management adds a unified connectivity metrics monitoring dashboard」を参照してください。

Fleet Hub アラーム

Fleet Hub アラームを使用すると、しきい値ベースのアラームを作成およびモニタリングできます。Fleet Hub アラームは、フリートインデックス作成と Amazon CloudWatch アラームによって提供される AWS IoT Device Management フリートメトリクスを活用します。これらのフリートメトリクスは、Amazon CloudWatch コンソールで直接モニタリングし、 AWS IoT コンソールで再設定できます。「iotfleethub」というプレフィックスが付いた名前が Fleet Hub に関連付けられているフリートメトリクスと CloudWatchアラーム。これらにはコンソールから引き続きアクセスできます。Amazon CloudWatch を使用して、これらのメトリクスを経時的にモニタリングし、傾向を表示できます。 AWS IoT コンソールから追加のフリートメトリクスを作成してモニタリングし、Amazon でアラームを設定することもできます CloudWatch。詳細については、「でフリートメトリクスを表示する CloudWatch」を参照してください。

デバイス検索

Fleet Hub では、インデックス付きデータソースの条件を使用して複数のフィルターを適用して、デバイス検索を絞り込むことができます。この機能は、フリートのインデックス作成の検索機能を利用します。デバイス検索は、[モノの高度な検索] ページから AWS IoT Device Management コンソールで直接使用できます。[モノの高度な検索] ページを検索するには、[管理] から [モノ] を選択し、[すべてのデバイス] を選択します。[モノ] ページの右上隅にある [高度な検索] を選択します。

ジョブの実行

モノまたはグループをターゲットとして選択することで、Fleet Hub から直接ジョブを実行できます。 AWS IoT Device Management コンソールの [ジョブ] ページからジョブを実行することもできます。ここでは、ジョブ実行のターゲットとしてモノ、静的グループ、または動的グループを定義できます。

[デバイスの詳細] の表示

Fleet Hub は、[すべてのデバイス] ページからデバイス (モノ) レベルの詳細なビューを提供します。同様のデバイスレベルの詳細ビューは、 AWS IoT Device Management コンソールの Things タブから直接、またはフリートインデックス作成の検索結果から返された特定のモノをクリックすることによって利用できます。

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