デベロッパーガイド

AWS IoT FleetWise

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

AWS IoT FleetWise: デベロッパーガイド

Copyright © 2025 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

とは AWS IoT FleetWise 1
利点 2
ユースケース 3
AWS IoT FleetWise は初めてですか？ 3
AWS IoT FleetWise へのアクセス 4
AWS IoT FleetWise の料金 4
関連サービス 4
主要なコンセプト 4
主要なコンセプト 5
AWS IoT FleetWise の機能 10
サポートされている AWS リージョン 10
AWS IoT FleetWise をセットアップする 13
をセットアップする AWS アカウント 13
にサインアップする AWS アカウント 13
管理アクセスを持つユーザーを作成する 14
コンソールの開始方法 15
設定を構成する 16
設定の構成 (コンソール) 16
設定の構成 (AWS CLI) 17
AWS IoT FleetWise での IPv6 の使用 18
コントロールプレーンエンドポイントの IPv6 前提条件 18
AWS PrivateLink エンドポイントの IPv6 サポート 18
IPv6 アドレスの互換性のテスト 18
IAM ポリシーでの IPv6 アドレスの使用 19
デュアルスタックのエンドポイントの使用 20
はじめに 22
序章 22
前提条件 23
ステップ 1: AWS IoT FleetWise 用のエッジエージェントソフトウェアを設定する 24
ステップ 2: 車両モデルを作成する 25
ステップ 3: デコーダーマニフェストを作成する 27
ステップ 4: デコーダーマニフェストを構成する 28
ステップ 5: 車両を作成する 29
ステップ 6: キャンペーンを作成する 30

ステップ 7: クリーンアップする ... 32
次のステップ ... 32
データを取り込む ... 33
車両をモデル化する ... 37
シグナルカタログ ... 40
シグナルの構成 ... 42
シグナルカタログを作成する ... 48
シグナルカタログのインポート ... 53
シグナルカタログを更新する ... 63
シグナルカタログを削除する ... 66
シグナルカタログ情報の取得 ... 68
車両モデル ... 69
車両モデルの作成 ... 70
車両モデルを更新する ... 76
車両モデルの削除 ... 78
車両モデル情報を取得する ... 80
デコーダーマニフェスト ... 81
インターフェイスとシグナルを設定する ... 84
デコーダーマニフェストの作成 ... 87
デコーダーマニフェストを更新する ... 97
デコーダーマニフェストの削除 ... 100
デコーダーマニフェスト情報の取得 ... 102
車両を管理する ... 103
車両のプロビジョニング ... 104
車両の認証 ... 105
車両の認可 ... 107
予約済みトピック ... 108
車両の作成 ... 113
車両の作成 (コンソール) ... 113
車両の作成 (AWS CLI) ... 115
複数の車両を作成する ... 118
車両を更新する ... 120
複数の車両を更新する ... 122
車両の削除 ... 124
車両の削除 (コンソール) ... 124
車両の削除 (AWS CLI) ... 124

車両情報の取得 ... 125
フリートを管理する ... 128
フリートを作成する ... 129
車両をフリートに関連付ける ... 130
フリートから車両の関連付けを解除する ... 131
フリートを更新する ... 132
フリートを削除する ... 133
フリートの削除を検証する ... 133
フリート情報を取得する ... 134
キャンペーンでデータを管理する ... 137
キャンペーンの作成 ... 143
キャンペーンの作成 (コンソール) ... 144
キャンペーンの作成 (AWS CLI) ... 152
AWS IoT FleetWise キャンペーンの論理式 ... 158
キャンペーンを更新する ... 159
キャンペーンを削除する ... 160
キャンペーンの削除 (コンソール) ... 160
キャンペーンの削除 (AWS CLI) ... 161
キャンペーンの削除を確認する ... 161
キャンペーン情報を取得する ... 161
保存および転送 ... 162
データパーティションを作成する ... 163
キャンペーンデータをアップロードする ... 166
ジョブを使用して AWS IoT データをアップロードする ... 167
診断問題コードデータを収集する ... 169
診断問題コードキーワード ... 170
診断問題コードのデータ収集キャンペーンを作成する ... 173
診断問題コードのユースケース ... 175
車両データを視覚化する ... 179
MQTT トピックに送信される車両データの処理 ... 179
Timestream で車両データを処理する ... 180
Timestream に保存されている車両データを視覚化する ... 181
Amazon S3 で車両データを処理する ... 181
Amazon S3 オブジェクト形式 ... 183
Amazon S3 に保存されている車両データを分析する ... 184
コマンド ... 186

コマンドの概念 187
コマンドの主な概念 187
コマンド実行ステータス 190
車両とコマンド 195
ワークフローの概要 196
車両ワークフロー 197
コマンドワークフロー 200
(オプション) コマンド通知 201
コマンドの作成と管理 203
コマンドリソースを作成する 203
コマンドに関する情報を取得する 205
アカウントのコマンドを一覧表示する 206
コマンドリソースを更新または廃止する 207
コマンドリソースを削除する 209
コマンド実行の開始とモニタリング 210
コマンド実行結果を更新する 214
コマンド実行の取得 216
アカウントのコマンド実行を一覧表示する 217
コマンド実行を削除する 219
例: コマンドの使用 220
車両ステアリングモードの概要の例 220
前提条件 221
リモートコマンドを使用するための IAM ポリシー 221
AWS IoT コマンドを実行する (AWS CLI) 223
クリーンアップ 228
コマンドの使用シナリオ 230
パラメータなしでコマンドを作成する 231
パラメータのデフォルト値を使用したコマンドの作成 232
パラメータ値を使用したコマンドの作成 233
状態テンプレートでのコマンドの使用 234
最後の既知の状態 237
状態テンプレートを作成する 238
AWS IoT FleetWise 状態テンプレートを車両に関連付ける 240
状態テンプレートを更新する 241
状態テンプレートを削除する 242
状態テンプレート情報の取得 243

状態テンプレートオペレーション 244
状態データ収集のアクティブ化と非アクティブ化 244
車両状態のスナップショットを取得する 250
MQTT メッセージングを使用して最後の既知の状態車両データを処理する 252
ネットワークに依存しないデータ収集を設定する 256
序章 256
環境設定 256
データモデル 256
シグナルカタログの更新 257
車両モデルとデコーダー 258
Send コマンド 261
AWS CLI および SDKs 263
トラブルシューティング 264
デコーダーマニフェストの問題 264
エッジエージェントの問題 268
問題: エッジエージェントソフトウェアが起動しない。 268
問題: [ERROR] [IoTFleetWiseEngine::connect]: [Failed to init persistency library] 270
問題: エッジエージェントソフトウェアがオンボードダイアグノーシス (OBD) II の PID と故障診断コード (DTC) を収集しない。 270
問題: Edge Agent for AWS IoT FleetWise ソフトウェアがネットワークからデータを収集しないか、データ検査ルールを適用できません。 270
問題: [ERROR] [AwsIotConnectivityModule::connect]: [Connection failed with error] または [WARN] [AwsIotChannel::send]: [No alive MQTT Connection.] 271
問題の保存と転送 272
問題: 必要なすべての IAM アクセス許可`AccessDeniedException`を持つ の受信 272
問題: Jobs にアップロード AWS IoT されたデータは を無視します。 `endTime` 272
問題: ジョブへの AWS IoT データアップロード`REJECTED`の実行ステータスがあります。 272
セキュリティ 273
データ保護 274
AWS IoT FleetWise での保管時の暗号化 275
転送中の暗号化 275
AWS IoT FleetWise でのデータ暗号化 275
アクセスコントロール 288
MQTT トピックでデータを送受信する AWS IoT FleetWise アクセス許可を付与する 288
Amazon S3 送信先 AWS IoT FleetWise へのアクセスを許可する 291

Amazon Timestream 送信先 AWS IoT FleetWise へのアクセスを許可する 294
を使用してコマンドのペイロードを生成する AWS IoT Device Management アクセス許可を付与する AWS IoT FleetWise 297
Identity and Access Management 302
対象者 302
アイデンティティを使用した認証 303
ポリシーを使用したアクセスの管理 306
IoT FleetWise AWS IoT が IAM と連携する方法 309
アイデンティティベースのポリシーの例 318
トラブルシューティング 322
API アクセス許可のリファレンス 324
コンプライアンス検証 335
耐障害性 336
インフラストラクチャセキュリティ 337
インターフェイス VPC エンドポイントを介した AWS IoT FleetWise への接続 338
設定と脆弱性の分析 341
セキュリティに関するベストプラクティス 342
最小限のアクセス許可を付与する 342
機密情報を記録しない 342
AWS CloudTrail を使用して API コール履歴を表示する 342
デバイスのクロックを同期させる 343
AWS IoT FleetWise のモニタリング 344
CloudWatch によるモニタリング 344
CloudWatch Logs でモニタリングする 349
CloudWatch コンソールで AWS IoT FleetWise ログを表示する 349
ログ記録の構成 356
CloudTrail ログ 359
CloudTrail のAWS IoT FleetWise 情報 359
ログファイルエントリについて理解する 360
ドキュメント履歴 362
..... ccclxv

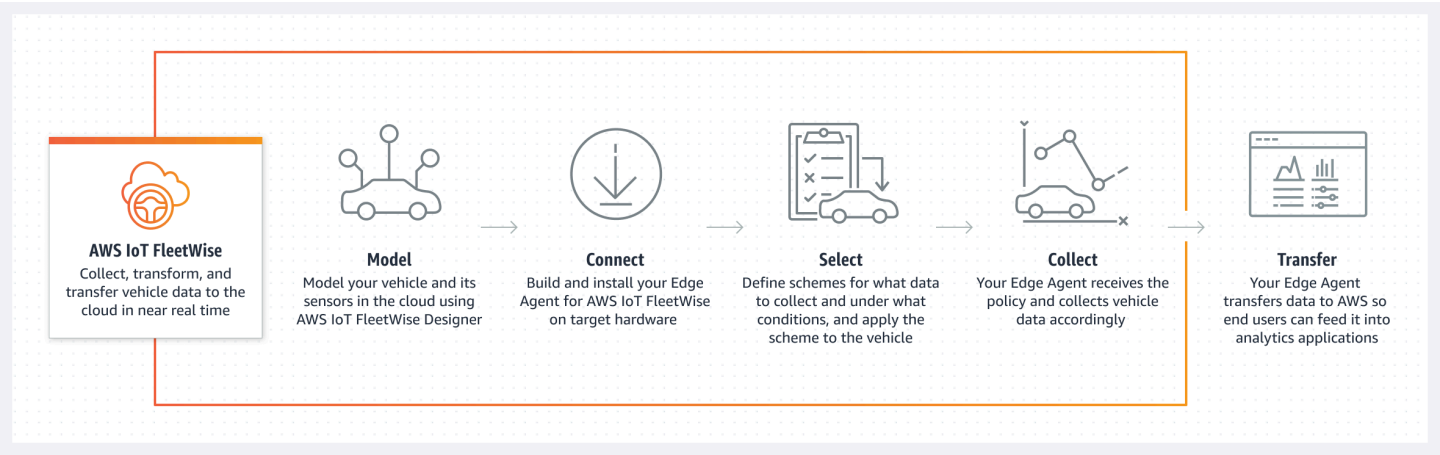
AWS IoT FleetWise とは

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise は、車両データを収集してクラウドに整理するために使用できるマネージドサービスです。収集したデータを使用して、車両の品質、性能、自律性を改善できます。 AWS IoT FleetWise を使用すると、さまざまなプロトコルとデータ形式を使用する車両からデータを収集して整理できます。 AWS IoT FleetWise は、低レベルのメッセージを人間が読める値に変換し、データ分析のためにクラウド内のデータ形式を標準化するのに役立ちます。また、データ収集キャンペーンを定義して、収集する車両データと、そのデータをクラウドに転送するタイミングを制御することもできます。

クラウドに配置された車両データは、車両のフリートの状態を分析するアプリケーションで使用できます。このデータは、潜在的なメンテナンス問題の特定、車載インフォテインメントシステムのスマート化、分析と機械学習 (ML) による自動運転や運転支援システムなどの高度なテクノロジーの改良に役立ちます。

次の図は、 AWS IoT FleetWise の基本的なアーキテクチャを示しています。



トピック

- 利点
- ユースケース

- AWS IoT FleetWise は初めてですか？
- AWS IoT FleetWise へのアクセス
- AWS IoT FleetWise の料金
- 関連サービス
- AWS IoT FleetWise の主な概念と機能
- AWSAWS IoT FleetWise でのリージョンと機能の可用性

利点

AWS IoT FleetWise の主な利点は次のとおりです。

車両データをよりインテリジェントに収集

必要なデータだけをクラウドに送信して分析するインテリジェントなデータ収集により、データの関連性を向上させます。

標準化されたフリート全体のデータを簡単に分析

カスタムのデータ収集システムやログ記録システムを開発しなくても、車両のフリートからの標準化されたデータを分析します。

クラウドでの自動データ同期

標準センサー (テレメトリデータ) とビジョンシステム (カメラ、レーダー、ライダーのデータ) の両方から収集されたデータの統合ビューを取得し、クラウドで自動的に同期された状態を維持します。 AWS IoT FleetWise は、構造化されたビジョンシステムデータ、非構造化ビジョンシステムデータ、メタデータ、標準センサーデータの両方をクラウドで自動的に同期させます。これにより、イベントの全体像を把握してインサイトを得るプロセスが効率化されます。

Edge にデータを保存し、最適な条件下で転送する

車両にデータを一時的に保存することで、送信コストを削減します。車両の Wi-Fi 接続時など、指定された最適な条件下で、選択したデータをクラウドに転送できます。

> **Note**
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

ユースケース

AWS IoT FleetWise を使用できるシナリオは次のとおりです。

AI/ML モデルのトレーニング

実稼働車両からデータを収集することで、自動運転支援システムや先進運転支援システムに使用される機械学習モデルを継続的に改善します。

デジタルカスタマーエクスペリエンスの強化

車載インフォテインメントシステムのデータを使用して、オーディオビジュアルコンテンツとアプリ内インサイトの関連性を高めます。

車両フリートのヘルスの維持

フリートデータからのインサイトを使用して、EV バッテリーのヘルスや充電レベルのモニタリング、メンテナンススケジュールの管理、燃料消費量の分析などを行います。

コマンドの作成と管理

コマンドを使用して、クラウドから車両でコマンドを実行します。リモートで車両にコマンドを送信でき、数秒以内に車両はコマンドを実行します。たとえば、車両のドアをロックしたり、温度を設定したりするようにコマンドを設定できます。

状態テンプレートの作成と管理

状態テンプレートは、車両所有者が車両の状態を追跡するメカニズムを提供します。車両で実行される AWS IoT FleetWise Edge エージェントは、シグナル更新を収集してクラウドに送信します。

AWS IoT FleetWise は初めてですか？

AWS IoT FleetWise を初めて使用する場合は、まず以下のセクションを読むことをお勧めします。

- AWS IoT FleetWise の主な概念と機能
- AWS IoT FleetWise をセットアップする
- チュートリアル: AWS IoT FleetWise の使用を開始する
- クラウドへの AWS IoT FleetWise データの取り込み

AWS IoT FleetWise へのアクセス

AWS IoT FleetWise コンソールまたは API を使用して AWS IoT FleetWise にアクセスできます。

AWS IoT FleetWise の料金

各車両は MQTT メッセージを通じてクラウドにデータを送信します。 AWS IoT FleetWise で作成した車両の料金を毎月月末に支払います。また、車両から収集するメッセージにも料金がかかります。料金に関する最新の情報については、「AWS IoT FleetWise の料金」を参照してください。MQTT メッセージングプロトコルの詳細については、「AWS IoT Core デベロッパーガイド」の「MQTT」を参照してください。

関連サービス

AWS IoT FleetWise は、以下の AWS サービスと統合して、クラウドソリューションの可用性とスケーラビリティを向上させます。

- AWS IoT Core – 車両データを AWS IoT FleetWise にアップロードする AWS IoT デバイスを登録して制御し、リモートで車両にコマンドを送信します。詳細については、「AWS IoT デベロッパーガイド」の「AWS IoTとは」を参照してください。
- Amazon Timestream - 時系列データベースを使用して、車両データを保存および分析します。詳細については、「Amazon Timestream Developer Guide」の「What is Amazon Timestream」を参照してください。
- Amazon S3 - オブジェクトストレージサービスを使用して、車両データを保存および管理します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 とは」を参照してください。

AWS IoT FleetWise の主な概念と機能

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

以下のセクションでは、 AWS IoT FleetWise サービスコンポーネントの概要と、それらの相互作用について説明します。

この概要を読んだら、AWS IoT FleetWise をセットアップする「」セクションを参照して、 AWS IoT FleetWise をセットアップする方法について説明します。

トピック

- 主要なコンセプト
- AWS IoT FleetWise の機能

主要なコンセプト

AWS IoT FleetWise は、クラウド内の車両とそのセンサーとアクチュエータをモデル化するための車両モデリングフレームワークを提供します。車両とクラウド間の安全な通信を可能にするために、AWS IoT FleetWise には、車両にインストールできるエッジエージェントソフトウェアの開発に役立つリファレンス実装も用意されています。データ収集スキームをクラウドで定義し、車両にデプロイできます。車両で動作するエッジエージェントソフトウェアは、データ収集スキームを使用して、収集するデータとクラウドに転送するタイミングを制御します。

以下は、 AWS IoT FleetWise の主要な概念です。

シグナル

シグナルは、車両データとそのメタデータを格納するために定義する基本構造です。シグナルには、属性、ブランチ、センサー、アクチュエータがあります。例えば、車内の温度値を受け取るセンサーを作成し、そのメタデータ (センサー名、データ型、単位など) を格納できます。詳細については、「Manage AWS IoT FleetWise シグナルカタログ」を参照してください。

属性

属性は、製造元や製造日など、通常は変更されない静的な情報を表します。

ブランチ

ブランチとは、ネストされた構造内のシグナルを表します。ブランチは、シグナルの階層を明確に示します。例えば、`Vehicle` というブランチに `Powertrain` という子ブランチがあるとします。`Powertrain` ブランチには `combustionEngine` という子ブランチがあります。`combustionEngine` ブランチを特定するには、`Vehicle.Powertrain.combustionEngine` という式を使用します。

センサー

センサーデータは、液面、温度、振動、電圧などの車両の状態について、現在の状態と経時的な変化を報告します。

アクチュエータ

アクチュエータデータは、モーター、ヒーター、ドアロックなど、車両デバイスの状態を報告します。車両デバイスの状態を変更すると、アクチュエータデータが更新される可能性があります。例えば、ヒーターを表すアクチュエータを定義できます。このアクチュエータは、ヒーターをオンまたはオフにしたときに新しいデータを受け取ります。

カスタム構造

カスタム構造 (構造体とも呼ばれる) は、複雑なデータ構造または高次のデータ構造を表します。これにより、同じソースから生成されたデータの論理的なバインドやグループ化が容易になります。構造体は、複雑なデータ型や高次の形状を表すなど、アトミック操作でデータを読み書きする場合に使用します。

構造体型のシグナルは、プリミティブデータ型の代わりに構造体データ型への参照を使用してシグナルカタログで定義します。構造体は、センサー、属性、アクチュエータ、ビジョンシステムデータ型など、あらゆるタイプのシグナルに使用できます。構造体タイプのシグナルが送受信される場合、 AWS IoT FleetWise は、含まれるすべての項目に有効な値があることを期待するため、すべての項目が必須です。例えば、構造体内に項目として Vehicle.Camera.Image.height、Vehicle.Camera.Image.width、Vehicle.Camera.Image.data が含まれている場合、送信されたシグナルには、これらすべての項目の値が含まれていることが期待されます。

> **Note**
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

カスタムプロパティ

カスタムプロパティは複雑なデータ構造のメンバーを表します。プロパティのデータ型は、プリミティブまたは別の構造体のいずれかになります。

構造体とカスタムプロパティを使用して高次の形状を表現する場合、意図した高次の形状は常にツリー構造として定義され、視覚化されます。カスタムプロパティはすべてのリーフノードを定義するために使用し、構造体はリーフ以外のすべてのノードを定義するために使用します。

シグナルカタログ

シグナルカタログには、シグナルのコレクションが格納されます。シグナルカタログ内のシグナルを使用して、さまざまなプロトコルやデータ形式を使用する車両をモデル化できます。例えば、異なる自動車メーカーの 2 台の車があるとします。1 台はコントローラーエリアネットワーク (CAN バス) プロトコルを使用し、もう 1 台はオンボードダイアグノーシス (OBD) プロトコルを使用しています。シグナルカタログには、車内の温度値を受信するセンサーを定義することができます。このセンサーを、両方の車の熱電対を表すために使用できます。詳細については、「Manage AWS IoT FleetWise シグナルカタログ」を参照してください。

車両モデル (モデルマニフェスト)

車両モデルとは、車両の形式を標準化し、車両内のシグナル間の関係を定義するために使用できる宣言的な構造です。車両モデルにより、同じタイプの複数の車両に一貫した情報が適用されます。車両モデルを作成するには、シグナルを追加します。詳細については、「Manage AWS IoT FleetWise 車両モデル」を参照してください。

デコーダーマニフェスト

デコーダーマニフェストには、車両モデル内の各シグナルのデコード情報が含まれています。車両内のセンサーやアクチュエータが送信するのは、低レベルのメッセージ (バイナリデータ) です。デコーダーマニフェストを使用すると、 AWS IoT FleetWise はバイナリデータを人間が読み取れる値に変換できます。すべてのデコーダーマニフェストは車両モデルに関連付けられます。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

ネットワークインターフェイス

車載ネットワークが使用するプロトコルに関する情報が含まれています。 AWS IoT FleetWise は、次のプロトコルをサポートしています。

コントローラーエリアネットワーク (CAN バス)

電子制御ユニット (ECU) 間でのデータの通信方法を定義するプロトコル。ECU には、エンジンコントロールユニット、エアバッグ、オーディオシステムなどがあります。

オンボードダイアグノーシス (OBD) II

ECU 間の自己診断データの通信方法を定義する、より進化したプロトコル。車両の問題を特定するために役立つ標準の故障診断コード (DTC) が多数定義されています。

車両ミドルウェア

車両ミドルウェアは、ネットワークインターフェイスの一種として定義します。車両ミドルウェアの例としては、ロボットオペレーティングシステム (ROS 2) や Scalable service-Oriented MiddlewarE over IP (SOME/IP) が挙げられます。

> **Note**
>
> AWS IoT FleetWise は、ビジョンシステムデータ用の ROS 2 ミドルウェアをサポートしています。

カスタムインターフェイス

独自のインターフェイスを使用して Edge でシグナルをデコードすることもできます。クラウドでデコードルールを作成する必要がないため、時間を節約できます。

シグナルデコーダー

特定のシグナルについて詳細なデコード情報を提供します。車両モデルで指定されたすべてのシグナルは、シグナルデコーダーとペアリングする必要があります。デコーダーマニフェストに CAN ネットワークインターフェイスが含まれている場合は、CAN デコーダーシグナルも含まれている必要があります。デコーダーマニフェストに OBD ネットワークインターフェイスが含まれている場合は、OBD シグナルデコーダーが含まれている必要があります。

車両のミドルウェアインターフェイスも含まれている場合、デコーダーマニフェストにはメッセージシグナルデコーダーが含まれている必要があります。または、デコーダーマニフェストにカスタムデコードインターフェイスが含まれている場合は、カスタムデコードシグナルも含める必要があります。

車両

車やトラックなどの物理的な車両を仮想的に表現したものです。車両とは、車両モデルのインスタンスです。同じ車両モデルから作成された車両は、同じシグナルのグループを継承します。各車両は AWS IoT モノに相当します。

フリート

フリートは、車両のグループを表します。車両のフリートを簡単に管理できるようにするには、事前に個々の車両をフリートに関連付ける必要があります。

キャンペーン

データ収集スキームが含まれています。キャンペーンはクラウドで定義し、車両またはフリートにデプロイします。キャンペーンにより、データをどのように選択して収集し、クラウドに転送するかに関する指示がエッジエージェントソフトウェアに与えられます。

データパーティション

キャンペーンでパーティション化されたデータを設定し、シグナルデータを一時的に保存します。データをクラウドに転送するタイミングと方法を設定します。

データ収集スキーム

データ収集スキームは、エッジエージェントソフトウェアにデータの収集方法を指示します。現在、 AWS IoT FleetWise は条件ベースのコレクションスキームと時間ベースのコレクションスキームをサポートしています。

条件ベースの収集スキーム

論理式を使用して、収集するデータを認識します。エッジエージェントソフトウェアは、条件が満たされたときにデータを収集します。例えば、`$variable.myVehicle.InVehicleTemperature >35.0` という式を使用すると、エッジエージェントソフトウェアは 35.0 より大きい温度値を収集します。

時間ベースの収集スキーム

データ収集の頻度を定義する時間間隔をミリ秒単位で指定します。例えば、時間間隔が 10,000 ミリ秒の場合、エッジエージェントソフトウェアはデータを 10 秒ごとに 1 回収集します。

コマンド

コマンドは、クラウドから車両に対してコマンドを実行します。リモートで車両にコマンドを送信でき、数秒以内に車両はコマンドを実行します。たとえば、車両のドアをロックしたり、温度を設定したりするようにコマンドを設定できます。

コマンドは、 によって管理されるリソースです AWS IoT Device Management。これには、車両にコマンド実行を送信するときに適用される再利用可能な設定が含まれています。詳細については、「 AWS IoT Core デベロッパーガイド」のAWS IoT 「 コマンド」を参照してください。

状態テンプレート

状態テンプレートは、車両所有者が車両の状態を追跡するメカニズムを提供します。車両で実行されるエッジエージェントソフトウェアエージェントは、シグナル更新を収集してクラウドに送信します。各状態テンプレートには、データが収集されるシグナルのリストが含まれています。

AWS IoT FleetWise の機能

以下は、 AWS IoT FleetWise の主な機能です。

車両のモデリング

車両の仮想表現を構築し、共通の形式を適用して車両信号を整理します。 AWS IoT FleetWise は、車両信号の標準化に使用できる車両信号仕様 (VSS) をサポートしています。

スキームベースのデータ収集

価値の高い車両データのみをクラウドに転送するスキームを定義します。条件ベースのスキームを定義すると、収集するデータを制御できます。例えば、車内の温度値データを、値が 40 度を超える場合に収集できます。時間ベースのスキームを定義して、データの収集頻度を制御することもできます。

Edge Agent for AWS IoT FleetWise ソフトウェア

車両内で実行されるエッジエージェントソフトウェアは、車両とクラウド間の通信を支援するものです。車両がクラウドに接続されている間、エッジエージェントソフトウェアは継続的にデータ収集スキームを受信し、それに従ってデータを収集します。

AWSAWS IoT FleetWise でのリージョンと機能の可用性

AWS IoT FleetWise をサポートする AWS リージョンのリストについては、AWS IoT FleetWise エンドポイントとクォータ」を参照してください。 AWS IoT FleetWise の機能は、リージョンのサポートが異なります。

> **Note**
>
> アジアパシフィック (ムンバイ) リージョンと一部の AWS IoT FleetWise 機能へのアクセスは現在ゲートされています。この AWS リージョンとすべてのゲート機能へのアクセスをリクエストするには、アカウントマネージャーまたは AWS サポートセンターにお問い合わせください。

次の表は、リージョン別の機能サポートを示しています。

機能/リージョン	米国東部 (バージニア北部)	欧州 (フランクフルト)	アジアパシフィック (ムンバイ) 注: ゲートアクセスのみ
シグナルカタログ	はい	はい	制限あり
車両モデル	はい	はい	制限あり
デコーダーマニフェスト	はい	はい	制限あり
車両	はい	はい	制限あり
群数	はい	はい	制限あり
キャンペーン	はい	はい	制限あり
ビジョンシステムデータ (プレビューリリース)	はい	はい	制限あり
キャンペーンデータ送信先としての MQTT トピック	制限あり	制限あり	制限あり
保存および転送	制限あり	制限あり	制限あり
コマンド	制限あり	制限あり	制限あり
最後の既知の状態	制限あり	制限あり	制限あり
カスタムデコードインターフェイスを使用したネットワークに依存しないデータ収集	制限あり	制限あり	制限あり
診断トラブルコード (DTC) フェッチ*	制限あり	制限あり	制限あり

*DTC フェッチは、基本的な DTC データ取得を超えるさまざまな機能を提供します。この機能には、エッジで関数を定義し、条件ベースのキャンペーン式内で名前で呼び出すことができるカスタム機能が含まれています。さらに、無制限の文字列のコレクションをサポートし、柔軟な文字列データ型処理を提供します。エッジエージェントは、定期的にデータを取得するか、特定の条件によってトリガーされ、データ収集プロセスの適応性と効率を向上させることができます。詳細については、「 Edge エージェントデベロッパーガイド」の「カスタム関数ガイド」と「DTC データ収集リファレンスの実装」を参照してください。

AWS IoT FleetWise をセットアップする

AWS IoT FleetWise を初めて使用する前に、以下のセクションのステップを完了してください。

トピック

- をセットアップする AWS アカウント
- コンソールの開始方法
- AWS IoT FleetWise 設定を構成する
- IPv6 を使用して AWS IoT FleetWise にリクエストを行う

をセットアップする AWS アカウント

にサインアップ AWS して管理ユーザーを作成するには、次のタスクを実行します。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一部では、電話またはテキストメッセージを受信し、電話のキーパッドに検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、AWS IAM Identity Center 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

> **Note**
>
> AWS IoT FleetWise では、サービスにリンクされたロールを使用できます。サービスにリンクされたロールは、 AWS IoT FleetWise によって事前定義されており、 AWS IoT FleetWise が Amazon CloudWatch にメトリクスを送信するために必要なアクセス許可が含まれています。詳細については、「AWS IoT FleetWise のサービスリンクロールの使用」を参照してください。

コンソールの開始方法

にまだサインインしていない場合は AWS アカウント、サインインして IoT AWS FleetWise IoT コンソールを開きます。 AWS IoT FleetWise の使用を開始するには、車両モデルを作成します。車両モデルは、車両の形式を標準化するものです。

1. AWS IoT FleetWise コンソールを開きます。
2. 「Get started with AWS IoT FleetWise」で「Get started」を選択します。

車両モデルの作成の詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

AWS IoT FleetWise 設定を構成する

AWS IoT FleetWise コンソールまたは API を使用して、Amazon CloudWatch Logs メトリクス、Amazon CloudWatch Logs の設定を行い、 を使用してデータを暗号化できます AWS マネージドキー。

CloudWatch メトリクスを使用すると、 AWS IoT FleetWise やその他の AWS リソースをモニタリングできます。CloudWatch メトリクスは、サービス制限を超過していないかどうかを確認するなどの目的で、メトリクスを収集して追跡するために使用できます。CloudWatch のメトリクスの詳細については、「Amazon CloudWatch で AWS IoT FleetWise をモニタリングする」を参照してください。

CloudWatch Logs を使用すると、 AWS IoT FleetWise はログデータを CloudWatch ロググループに送信し、これを使用して問題を特定して軽減できます。CloudWatch Logs の詳細については、「Configure AWS IoT FleetWise ログ記録」を参照してください。

データ暗号化を使用すると、 AWS IoT FleetWise は を使用してデータを暗号化 AWS マネージドキー します。を使用してキーを作成および管理することもできます AWS KMS。暗号化の詳細については、「AWS IoT FleetWise でのデータ暗号化」を参照してください。

設定の構成 (コンソール)

にまだサインインしていない場合は AWS アカウント、サインインして IoT AWS FleetWise IoT コンソールを開きます。

1. AWS IoT FleetWise コンソールを開きます。
2. 左側のペインで、[設定] を選択します。
3. メトリクスで、Enable. AWS IoT FleetWise はサービスにリンクされたロールに CloudWatch 管理ポリシーを自動的にアタッチし、CloudWatch メトリクスを有効にします。
4. [ログ記録] で、[編集] を選択します。
   a. [CloudWatch ログ記録] セクションで、[ロググループ] を入力します。
   b. 変更を保存するには、[送信] を選択します。
5. [暗号化] セクションで、[編集] を選択します。
   a. 使用するキーの種類を選択します。詳細については、「AWS IoT FleetWise でのキー管理」を参照してください。
      i. AWS キーを使用する – AWS IoT FleetWise はキーを所有および管理します。

ii. 別の AWS Key Management Service キーを選択する – アカウントにある AWS KMS keys を管理します。

b. 変更を保存するには、[送信] を選択します。

設定の構成 (AWS CLI)

で AWS CLI、アカウントを登録して設定を行います。

1. 設定を構成するには、次のコマンドを実行します。

```
aws iotfleetwise register-account
```

2. 設定を確認するには、次のコマンドを実行して登録ステータスを取得します。

> **Note**
>
> サービスにリンクされたロールは、 AWS IoT FleetWise メトリクスを CloudWatch に発行する場合にのみ使用されます。詳細については、「AWS IoT FleetWise のサービスリンクロールの使用」を参照してください。

```
aws iotfleetwise get-register-account-status
```

Example レスポンス

```
{
    "accountStatus": "REGISTRATION_SUCCESS",
    "creationTime": "2022-07-28T11:31:22.603000-07:00",
    "customerAccountId": "012345678912",
    "iamRegistrationResponse": {
        "errorMessage": "",
        "registrationStatus": "REGISTRATION_SUCCESS",
        "roleArn": "arn:aws:iam::012345678912:role/AWSIoTFleetwiseServiceRole"
    },
    "lastModificationTime": "2022-07-28T11:31:22.854000-07:00",
    }
}
```

登録ステータスは次のいずれかになります。

- `REGISTRATION_SUCCESS` – AWS リソースは正常に登録されました。
- `REGISTRATION_PENDING` – AWS IoT FleetWise は登録リクエストを処理しています。このプロセスの完了には約 5 分かかります。
- `REGISTRATION_FAILURE` – AWS IoT FleetWise は AWS リソースを登録できません。後でもう一度お試しください。

IPv6 を使用して AWS IoT FleetWise にリクエストを行う

インターネットプロトコルバージョン 6 (IPv6) および IPv4 経由で AWS IoT FleetWise と通信して、リソースを管理できます。デュアルスタックエンドポイントは、IPv6 および IPv4 を介した AWS IoT FleetWise APIs へのリクエストをサポートします。IPv6 経由の通信には追加料金はかかりません。

IPv6 プロトコルは、追加のセキュリティ機能を備えた次世代 IP 標準です。IPv4 には 32 ビットのロングアドレスがあり、128 ビットのロングアドレススペースを提供します。IPv4 は 4.29 x 10^9 アドレスを生成でき、IPv6 は 3.4 x 10^38 アドレスを生成できます。

コントロールプレーンエンドポイントの IPv6 前提条件

IPv6 プロトコルのサポートは、コントロールプレーンエンドポイントに対して自動的に有効になります。コントロールプレーンクライアントにエンドポイントを使用する場合は、サーバー名表示 (SNI) 拡張機能を指定する必要があります。クライアントは SNI 拡張機能を使用して、接続するサーバーの名前と、通常のエンドポイントとデュアルスタックエンドポイントのどちらを使用しているかを指定できます。「デュアルスタックのエンドポイントの使用」を参照してください。

AWS PrivateLink エンドポイントの IPv6 サポート

AWS IoT FleetWise は、 を使用して VPC エンドポイントをインターフェイスするための IPv6 通信をサポートしています AWS PrivateLink。

IPv6 アドレスの互換性のテスト

Linux/Unix または Mac OS X を使用している場合は、次の例に示すように curl コマンドを使用して、IPv6 経由でデュアルスタックエンドポイントにアクセスできるかどうかをテストできます。

```
curl -v https://iotfleetwise.<us-east-1>.api.aws
```

次の例のような情報を取得できます。IPv6 経由で接続している場合、接続された IP アドレスは IPv6 アドレスになります。

```
* Host iotfleetwise.us-east-1.api.aws:443 was resolved.
* IPv6: ::ffff:3.82.78.135, ::ffff:54.211.220.216, ::ffff:54.211.201.157
* IPv4: (none)
*   Trying [::ffff:3.82.78.135]:443...
* Connected to iotfleetwise.us-east-1.api.aws (::ffff:3.82.78.135) port 443
* ALPN: curl offers h2,http/1.1
```

Microsoft Windows 7 または Windows 10 を使用している場合は、次の例に示すように ping コマンドを使用して、IPv6 または IPv4 経由でデュアルスタックエンドポイントにアクセスできるかどうかをテストできます。

```
ping iotfleetwise.<us-east-1>.api.aws
```

IAM ポリシーでの IPv6 アドレスの使用

リソースに IPv6 を使用する前に、IP アドレスフィルタリングに使用される IAM ポリシーに IPv6 アドレス範囲が含まれていることを確認する必要があります。IAM でのアクセス許可管理の詳細については、「AWS IoT FleetWise の Identity and Access Management」を参照してください。

IP アドレスをフィルタリングする IAM ポリシーは、IP アドレス条件演算子を使用します。次のポリシーは、IP アドレス条件演算子を使用して、許可された IPv4 アドレス`54.240.143.*`の範囲を識別します。すべての IPv6 アドレスが許容範囲外であるため、このポリシーは IPv6 アドレスを使用した通信を防止します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "iotfleetwise:*",
      "Resource": "arn:aws:iotfleetwise:*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"}
      }
    }
  ]
```

```
}
```

IPv6 アドレスを含めるには、次の例に示すように、ポリシーの条件要素を変更してIPv4 (54.240.143.0/24) と IPv6 (2001:DB8:1234:5678::/64) の両方のアドレス範囲を許可できます。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": [
      "54.240.143.0/24",
      "2001:DB8:1234:5678::/64"
    ]
  }
}
```

デュアルスタックのエンドポイントの使用

AWS IoT FleetWise デュアルスタックエンドポイントは、IPv6 および IPv4 を介した AWS IoT FleetWise APIs へのリクエストをサポートします。デュアルスタックエンドポイントにリクエストを行うと、IPv4 アドレスまたは IPv6 アドレスに自動的に解決されます。デュアルスタックモードでは、IPv4 クライアント接続と IPv6 クライアント接続の両方が受け入れられます。

REST API を使用している場合は、エンドポイント名 (URI) を使用して、 AWS IoT FleetWise エンドポイントに直接アクセスできます。 AWS IoT FleetWise は、リージョンのデュアルスタックエンドポイント名のみをサポートします。つまり、名前 AWS リージョン の一部として を指定する必要があります。

次の表は、IPv4 モードとデュアルスタックモードを使用する場合の AWS IoT FleetWise のコントロールプレーンエンドポイントの形式を示しています。これらのエンドポイントの詳細については、AWS 「 IoT FleetWise エンドポイント」を参照してください。

Endpoint	IPv4 アドレス	デュアルスタックモード
コントロールプレーン	iotfleetwise.*<region>*.amazonaws.com	iotfleetwise.*<region>*.api.aws

AWS CLI および AWS SDKs を使用する場合、`AWS_USE_DUALSTACK_ENDPOINT`環境変数、または共有設定ファイル設定である `use_dualstack_endpoint`パラメータを使用して、デュアルスタッ

クエンドポイントに変更できます。設定ファイルで AWS IoT FleetWise エンドポイントのオーバーライドとしてデュアルスタックエンドポイントを直接指定することもできます。詳細については、「デュアルスタックと FIPS エンドポイント」を参照してください。

を使用する場合 AWS CLI、Config ファイルのプロファイル`true`で設定値を AWS `use_dualstack_endpoint`として設定できます。これにより、 コマンドによって行われたすべての AWS IoT FleetWise リクエストが、指定されたリージョンのデュアルスタックエンドポイントに転送されます。`--region` オプションを使用して設定ファイルまたはコマンドでリージョンを指定します。

```
$ aws configure set default.iotfleetwise.use_dualstack_endpoint true
```

すべてのコマンドにデュアルスタックエンドポイントを使用する代わりに、特定のコマンドにこれらのエンドポイントを使用します。

- これらのコマンドの `--endpoint-url`パラメータを設定することで、特定のコマンドにデュアルスタックエンドポイントを使用できます。たとえば、次のコマンドでは、*<endpoint-url>* を に置き換えることができます`iotfleetwise.`*<region>*`.api.aws`。

  ```
  aws iotfleetwise list-fleets \
    --endpoint-url <endpoint-url>
  ```

- AWS Config ファイルに個別のプロファイルを設定できます。たとえば、 を true `use_dualstack_endpoint` に設定するプロファイルを 1 つ作成し、 を設定しないプロファイルを作成します`use_dualstack_endpoint`。コマンドを実行する際には、デュアルスタックのエンドポイントを使用するかどうかによって、適切なプロファイルを指定します。

チュートリアル: AWS IoT FleetWise の使用を開始する

AWS IoT FleetWise を使用すると、車両データを収集、変換、転送できます。このセクションのチュートリアルを使用して、 AWS IoT FleetWise の使用を開始します。

AWS IoT FleetWise の詳細については、以下のトピックを参照してください。

- クラウドへの AWS IoT FleetWise データの取り込み
- Model AWS IoT FleetWise 車両
- Manage AWS IoT FleetWise 車両
- AWS IoT FleetWise でフリートを管理する
- キャンペーンを使用して AWS IoT FleetWise データを収集する

序章

AWS IoT FleetWise を使用して、自動車両から一意のデータ形式をほぼリアルタイムで収集、変換、クラウドに転送します。フリート全体のインサイトにアクセスできます。これにより、車両のヘルスに関する問題の効率的な検出と軽減、価値の高いデータシグナルの転送、問題のリモート診断を、コストを抑えながら行うことができます。

このチュートリアルでは、 AWS IoT FleetWise の使用を開始する方法を示します。車両モデル (モデルマニフェスト)、デコーダーマニフェスト、車両、キャンペーンの作成方法を学ぶことができます。

AWS IoT FleetWise の主要なコンポーネントと概念の詳細については、「」を参照してくださいAWS IoT FleetWise の主な概念と機能。

推定所要時間: 約 45 分。

> **Important**
>
> このデモが作成および消費する AWS IoT FleetWise リソースに対して課金されます。詳細については、AWS 「 IoT FleetWise AWS 料金表」ページの「 IoT FleetWise」を参照してください。

前提条件

この入門チュートリアルを完了するには、まず以下の準備が必要です。

- AWS アカウント。がない場合は AWS アカウント、「 AWS アカウント管理 リファレンスガイド」の「 の作成 AWS アカウント」を参照してください。
- AWS IoT FleetWise AWS リージョン をサポートする へのアクセス。現在、 AWS IoT FleetWise は米国東部 (バージニア北部) および欧州 (フランクフルト) でサポートされています。のリージョンセレクタを使用して AWS Management Console 、これらのリージョンのいずれかに切り替えることができます。詳細については、AWS 「 IoT FleetWise エンドポイントとクォータ」を参照してください。
- Amazon Timestream リソース:
  - Amazon Timestream データベース。詳細については、「Amazon Timestream Developer Guide」の「Create a database」を参照してください。
  - Amazon Timestream で作成された、データを保持するための Amazon Timestream テーブル。詳細については、「Amazon Timestream Developer Guide」の「Create a table」を参照してください。
- Edge Agent ソフトウェアデモ。 (デモの設定手順については、次のステップで説明します。)
  - Explore Edge Agent クイックスタートデモを使用して、 AWS IoT FleetWise を試し、 AWS IoT FleetWise 用の Edge Agent ソフトウェアを開発する方法を学習できます。このデモでは、AWS CloudFormation テンプレートを使用します。エッジエージェントのリファレンス実装を詳しく紹介し、エッジエージェントの開発、Amazon EC2 Graviton へのエッジエージェントソフトウェアのデプロイ、サンプル車両データの生成の手順を示します。また、このデモには、シグナルカタログ、車両モデル、デコーダーマニフェスト、車両、フリート、キャンペーンをクラウド内で作成するために使用できるスクリプトも用意されています。
  - デモをダウンロードするには、AWS IoT FleetWise コンソールに移動します。サービスのホームページで、[AWS IoT FleetWise の使用を開始する] セクションの [エッジエージェントを調べる] を選択します。

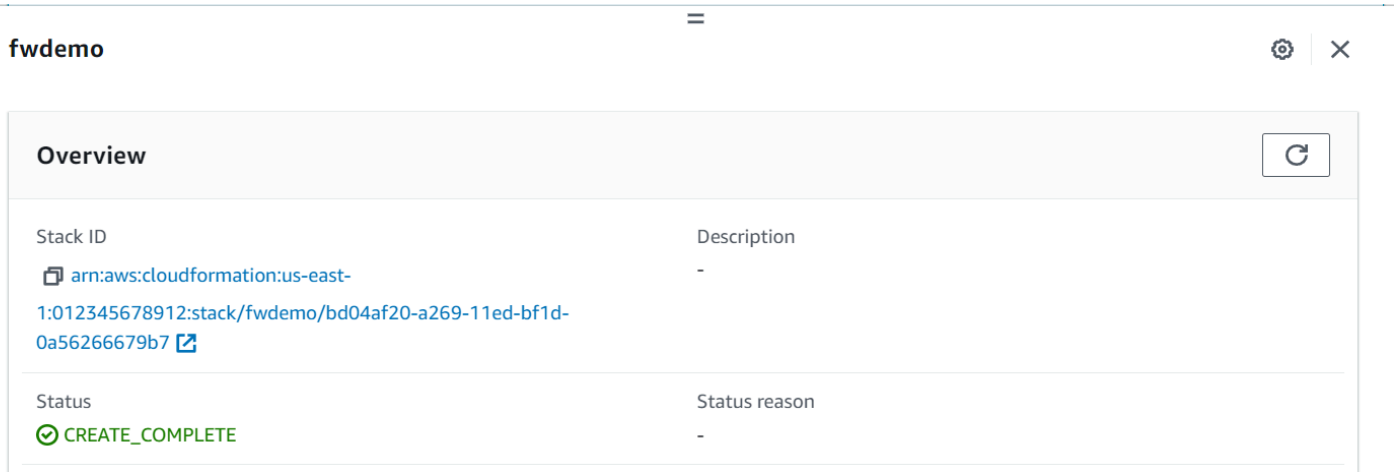
ステップ 1: AWS IoT FleetWise 用のエッジエージェントソフトウェアを設定する

> **Note**
>
> このステップの CloudFormation スタックでは、テレメトリーデータを使用します。ビジョンシステムデータを使用して CloudFormation スタックを作成することもできます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

AWS IoT FleetWise 用エッジエージェントソフトウェアは、車両とクラウド間の通信を容易にします。クラウドに接続された車両からデータを収集する方法についての指示は、データ収集スキームから受け取ります。

エッジエージェントソフトウェアをセットアップするには、[一般的な情報] で次の操作を行います。

1. [CloudFormation テンプレートを起動] を開きます。
2. スタックのクイック作成ページのスタック名に、 AWS IoT FleetWise リソースのスタックの名前を入力します。スタックは、この AWS CloudFormation テンプレートが作成するリソースの名前のプレフィックスとして表示されるわかりやすい名前です。
3. [パラメータ] で、スタックに関連するパラメータのカスタム値を入力します。
   a. [Fleetsize] - Fleetsize パラメータを更新すると、フリート内の車両の数を増やすことができます。
   b. IoTCoreRegion - IoTCoreRegion パラメータを更新することで、 AWS IoT モノが作成されるリージョンを指定できます。 AWS IoT FleetWise 車両の作成に使用したのと同じリージョンを使用する必要があります。詳細については AWS リージョン、「リージョンとゾーン - Amazon Elastic Compute Cloud」を参照してください。
4. 機能セクションで、 が IAM リソース AWS CloudFormation を作成することを確認するボックスを選択します。
5. [スタックの作成] を選択し、スタックのステータスに CREATE_COMPLETE が表示されるまで約 15 分待ちます。
6. スタックが作成されたことを確認するには、[スタックの情報] タブを選択し、ビューを更新して、CREATE_COMPLETE を探します。



> **Important**
>
> このデモが作成および消費する AWS IoT FleetWise リソースに対して課金されます。詳細については、AWS 「 IoT FleetWise AWS 料金表」ページの「 IoT FleetWise」を参照してください。

ステップ 2: 車両モデルを作成する

> **Important**
>
> AWS IoT FleetWise コンソールでは、ビジョンシステムデータシグナルを使用して車両モデルを作成することはできません。代わりに、 AWS CLIを使用してください。

車両モデルを使用して、車両の形式を標準化し、作成する車両のシグナル間の関係を定義できます。車両モデルを作成すると、シグナルカタログも作成されます。シグナルカタログは、車両モデルの作成に再利用できる標準化されたシグナルのコレクションです。シグナルは、車両データとそのメタデータを格納するために定義する基本構造です。現時点では、 AWS IoT FleetWise サービスは、アカウント AWS リージョン ごとに 1 つのシグナルカタログのみをサポートします。これにより、車両のフリートからの処理データが整合していることを検証できます。

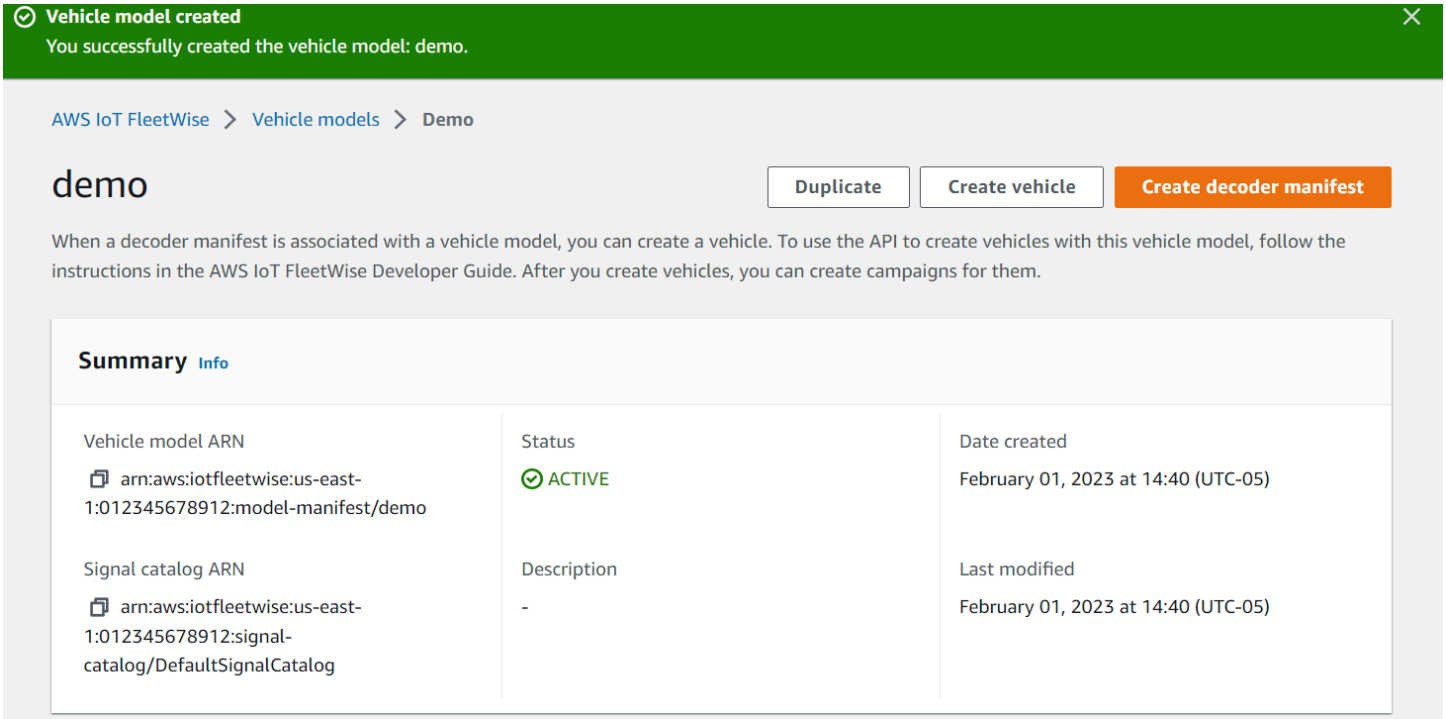
車両モデルを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。

3. [車両モデル] ページで、[車両モデルを作成] を選択します。
4. [一般的な情報] セクションに、車両モデルの名前 (Vehicle1 など) と、必要に応じて説明を入力します。[次へ] を選択します。
5. シグナルカタログから 1 つ以上のシグナルを選択します。カタログの検索でシグナルを名前でフィルタリングするか、リストからシグナルを選択できます。例えば、タイヤ空気圧とブレーキ圧力のシグナルを選択すると、これらのシグナルに関連するデータを収集できます。[次へ] を選択します。
6. ローカルデバイスから .dbc ファイルを選択してアップロードします。[Next (次へ)] を選択します。

> **Note**
>
> このチュートリアルでは、サンプル .dbc ファイルをダウンロードして、このステップ用にアップロードできます。

7. 車両モデルに属性を追加し、[次へ] を選択します。
   a. [名前] - 車両属性の名前を入力します (製造元の名前や製造日など)。
   b. [データ型] - [データ型] メニューで、データ型を選択します。
   c. [単位] - (オプション) 単位の値を入力します (キロメートルや摂氏など)。
   d. [パス] - (オプション) シグナルのパスの名前を入力します (`Vehicle.Engine.Light.` など)。ドット (.) は子シグナルであることを示します。
   e. [デフォルト値] - (オプション) デフォルト値を入力します。
   f. [説明] - (オプション) 属性の説明を入力します。
8. 構成を確認します。準備が完了したら、[作成] を選択します。車両モデルが正常に作成されたことを示す通知が表示されます。



ステップ 3: デコーダーマニフェストを作成する

作成した車両モデルにはデコーダーマニフェストが関連付けられます。これには、 AWS IoT FleetWise が車両データをバイナリ形式から人間が読める値にデコードして変換し、分析できるようにする情報が含まれています。デコーダーマニフェストの構成に役立つコンポーネントが、ネットワークインターフェイスとデコーダーシグナルです。ネットワークインターフェイスには、車両ネットワークが使用する CAN または OBD プロトコルに関する情報が含まれています。デコーダーシグナルは、特定のシグナルのデコード情報を提供します。

デコーダーマニフェストを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. [車両モデル] セクションで、デコーダーマニフェストの作成に使用する車両モデルを選択します。
4. [デコーダーマニフェストを作成] を選択します。

ステップ 4: デコーダーマニフェストを構成する

デコーダーマニフェストを構成するには

> **Important**
>
> AWS IoT FleetWise コンソールを使用してデコーダーマニフェストでビジョンシステムデータシグナルを設定することはできません。代わりに、 AWS CLIを使用してください。詳細については、「デコーダーマニフェストの作成 (AWS CLI)」を参照してください。

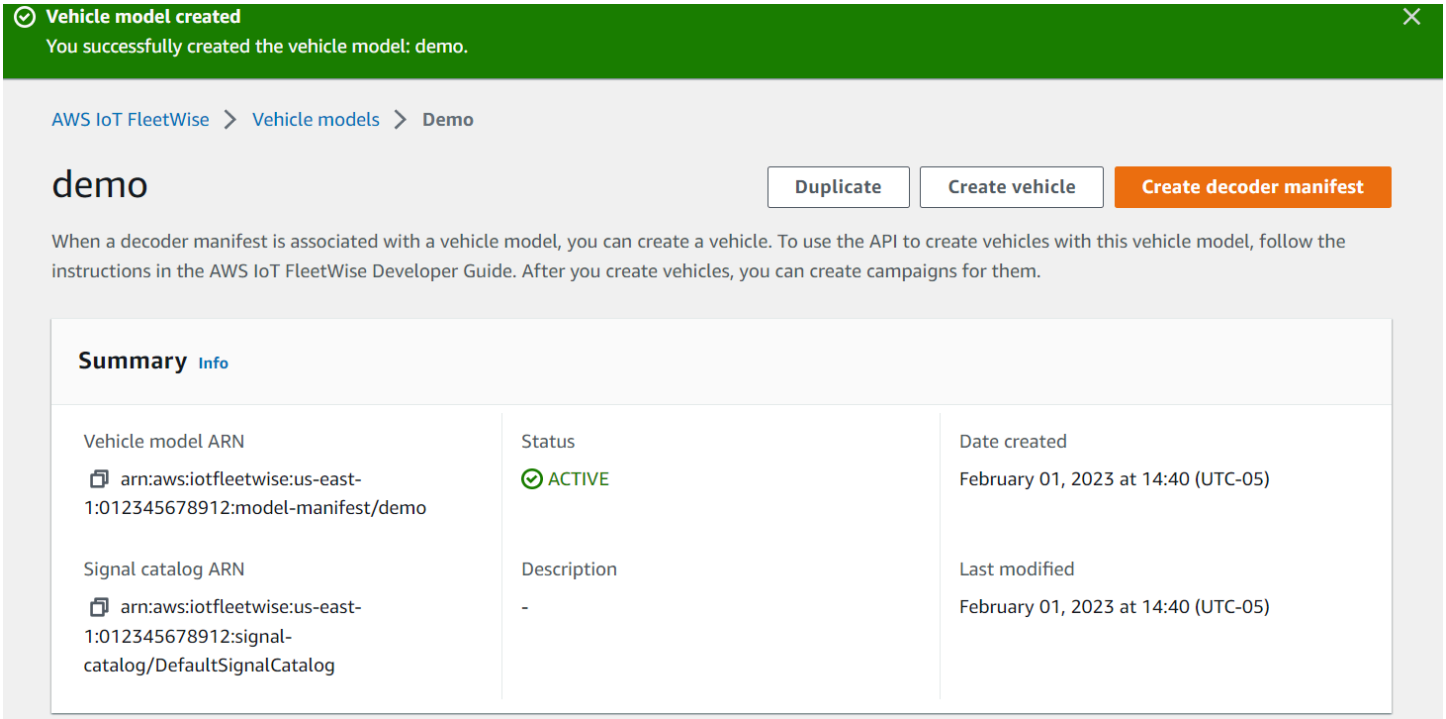
1. デコーダーマニフェストを識別しやすくするために、名前と必要に応じて説明を入力します。[次へ] を選択します。
2. 1 つ以上のネットワークインターフェイスを追加するには、CAN_INTERFACE タイプまたは OBD_INTERFACE タイプを選択します。
   - オンボードダイアグノーシス (OBD) インターフェイス - 電子制御ユニット (ECU) 間での自己診断データの通信方法を定義するプロトコルが必要な場合は、このインターフェイスタイプを選択します。このプロトコルには、車両の問題のトラブルシューティングに役立つ標準の故障診断コード (DTC) が多数定義されています。
   - コントローラーエリアネットワーク (CAN バス) インターフェイス - ECU 間でのデータの通信方法を定義するプロトコルが必要な場合は、このインターフェイスタイプを選択します。ECU には、エンジンコントロールユニット、エアバッグ、オーディオシステムなどがあります。
3. ネットワークインターフェイス名を入力します。
4. ネットワークインターフェイスにシグナルを追加するには、リストから 1 つ以上のシグナルを選択します。
5. 前のステップで追加したシグナル用のデコーダーシグナルを選択します。デコード情報を提供するには、.dbc ファイルをアップロードします。車両モデル内の各シグナルは、リストから選択できるデコーダーシグナルとペアにする必要があります。
6. 別のネットワークインターフェイスを追加するには、[ネットワークインターフェイスを追加] を選択します。ネットワークインターフェイスの追加が完了したら、[次へ] を選択します。
7. 構成を確認し、[作成] を選択します。デコーダーマニフェストが正常に作成されたことを示す通知が表示されます。

ステップ 5: 車両を作成する

AWS IoT FleetWise では、車両は実際の物理的な車両の仮想表現です。同じ車両モデルから作成したすべての車両は、同じシグナルグループを継承します。作成した各車両は、新しく作成した IoT モノに対応します。すべての車両は、デコーダーマニフェストに関連付ける必要があります。

前提条件

1. 車両モデルとデコーダーマニフェストを作成済みであることを確認します。また、車両モデルのステータスが ACTIVE であることも確認します。
   a. 車両モデルのステータスが ACTIVE であることを確認するには、 AWS IoT FleetWise コンソールを開きます。
   b. ナビゲーションペインで、[車両モデル] を選択します。
   c. [概要] セクションの [ステータス] で、車両のステータスを確認します。



車両を作成するには

1. AWS FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両] を選択します。
3. [車両を作成] を選択します。

4. 車両のプロパティを定義するには、車両名を入力し、モデルマニフェスト (車両モデル) とデコーダーマニフェストを選択します。
5. (オプション) 車両の属性を定義するには、キーと値のペアを入力し、[属性を追加] を選択します。
6. (オプション) AWS リソースにラベルを付けるには、タグを追加し、[新しいタグを追加] を選択します。
7. [次へ] を選択します。
8. 車両証明書を構成するには、独自の証明書をアップロードするか、[新しい証明書の自動生成] を選択します。セットアップを迅速に行うには、証明書を自動生成することをお勧めします。既に証明書がある場合は、代わりにそれを使用できます。
9. パブリックキーとプライベートキーのファイルをダウンロードし、[次へ] を選択します。
10. 車両証明書にポリシーをアタッチするには、既存のポリシー名を入力するか、新しいポリシーを作成します。新しいポリシーを作成するには、[ポリシーを作成] を選択し、[次へ] を選択します。
11. 構成を確認します。完了したら、[車両を作成] を選択します。

ステップ 6: キャンペーンを作成する

AWS IoT FleetWise では、キャンペーンは車両からクラウドへのデータの選択、収集、転送を容易にするために使用されます。キャンペーンにはデータ収集スキームが含まれています。データ収集スキームは、条件ベースの収集スキームまたは時間ベースの収集スキームを使用したデータの収集方法をエッジエージェントソフトウェアに指示します。

キャンペーンを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[キャンペーン] を選択します。
3. [キャンペーンを作成] を選択します。
4. キャンペーンの名前と、必要に応じて説明を入力します。
5. キャンペーンのデータ収集スキームを設定するには、データ収集スキームを手動で定義するか、.json ファイルをローカルデバイスからアップロードできます。.json ファイルをアップロードすると、データ収集スキームが自動的に定義されます。

a. データ収集スキームを手動で定義するには、[データ収集スキームを定義] を選択し、キャンペーンに使用するデータ収集スキームのタイプを選択します。[条件ベース] の収集スキームまたは [時間ベース] の収集スキームを選択できます。

b. [時間ベース] の収集スキームを選択した場合は、キャンペーンで車両データを収集する期間を指定する必要があります。

c. 条件ベースの収集スキームを選択した場合は、収集するデータを認識する式を指定する必要があります。シグナルの名前を表す変数、比較演算子、比較値を指定してください。

d. (オプション) 式の言語バージョンを選択するか、デフォルト値の 1 のままにします。

e. (オプション) 2 つのデータ収集イベント間のトリガー間隔を指定します。

f. データを収集するには、エッジエージェントソフトウェアの [トリガーモード] 条件を選択します。デフォルトでは、 Edge Agent for AWS IoT FleetWise ソフトウェアは、条件が満たされるたびに常にデータを収集します。または、[最初のトリガー時] を選択して、条件が初めて満たされたときにのみデータを収集することもできます。

g. (オプション) その他の高度なスキームオプションを選択できます。

6. データ収集スキームでデータを収集するシグナルを指定するには、メニューからシグナルの名前を検索します。

7. (オプション) 最大サンプル数または最小サンプリング間隔を選択できます。シグナルをさらに追加することもできます。

8. [Next (次へ)] を選択します。

9. キャンペーンでデータを転送する先のストレージを定義します。Amazon S3 または Amazon Timestream にデータを保存できます。

   a. Amazon S3 – アクセス許可 AWS IoT FleetWise を持つ S3 バケットを選択します。

   b. Amazon Timestream - Timestream データベースとテーブル名を選択します。が Timestream にデータを送信 AWS IoT FleetWise できるようにする IAM ロールを入力します。

10. [Next (次へ)] を選択します。

11. 検索ボックスから車両属性または車両名を選択します。

12. 車両に選択した属性または名前に関連する値を入力します。

13. キャンペーンでデータを収集する車両を選択します。[次へ] を選択します。

14. キャンペーンの構成を確認し、[キャンペーンを作成] を選択します。ユーザーまたはユーザーのチームは、このキャンペーンを車両にデプロイする必要があります。

ステップ 7: クリーンアップする

このチュートリアルで使用したリソースの料金がこれ以上発生しないようにするには、 AWS CloudFormation スタックとすべてのスタックリソースを削除します。

AWS CloudFormation スタックを削除するには

1. AWS CloudFormation コンソールを開きます。
2. スタックのリストから、ステップ 1 で作成したスタックを選択します。
3. [削除] を選択します。
4. 削除を確認するには、[削除] を選択します。スタックの消去には約 15 分かかります。

次のステップ

1. キャンペーンで収集した車両データを処理して視覚化できます。詳細については、「Visualize AWS IoT FleetWise 車両データ」を参照してください。
2. AWS IoT FleetWise の問題をトラブルシューティングして解決できます。詳細については、「AWS IoT FleetWise のトラブルシューティング」を参照してください。

クラウドへの AWS IoT FleetWise データの取り込み

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

Edge Agent for AWS IoT FleetWise ソフトウェアは、車両にインストールして実行する場合、車両とクラウド間の安全な通信を容易にするように設計されています。

> **Note**
>
> - AWS IoT FleetWise は、重大な人身事故や死亡、環境や資産への損害につながる可能性のある危険環境や重要なシステムの運用において、またはそれに関連して使用することを意図していません。 AWS IoT FleetWise を使用して収集された車両データは情報提供のみを目的としており、車両の機能を制御または操作するために AWS IoT FleetWise を使用することはできません。
> - AWS IoT FleetWise の使用を通じて収集された車両データは、該当する車両安全規制 (安全監視や報告義務など) に基づくコンプライアンス義務を満たす目的を含め、ユースケースに応じて正確性について評価する必要があります。このような評価には、他の業界標準の手段や情報源 (車両の運転者からの報告など) を通じた情報の収集とレビューを含める必要があります。

データをクラウドに取り込むには、次の操作を行います。

1. エッジエージェント for AWS IoT FleetWise ソフトウェアを開発して車両にインストールします。Edge Agent ソフトウェアの操作方法の詳細については、以下を実行して、 Edge Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイドをダウンロードしてください。

    1. AWS IoT FleetWise コンソールに移動します。
    2. サービスのホームページで、[AWS IoT FleetWise の使用を開始する] セクションの [エッジエージェントを調べる] を選択します。

2. 車両モデルの作成に使用するシグナルを含むシグナルカタログを作成またはインポートします。詳細については、AWS IoT FleetWise シグナルカタログを作成するおよびシグナルカタログのインポート (AWS CLI)を参照してください。

> **Note**
>
> - AWS IoT FleetWise コンソールを使用して最初の車両モデルを作成する場合、シグナルカタログを手動で作成する必要はありません。最初の車両モデルを作成すると、 AWS IoT FleetWise によって自動的にシグナルカタログが作成されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。
> - AWS IoT FleetWise は現在、 ごとに各 AWS アカウントのシグナルカタログをサポートしています AWS リージョン。

3. シグナルカタログ内のシグナルを使用して、車両モデルを作成します。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

> **Note**
>
> - AWS IoT FleetWise コンソールを使用して車両モデルを作成する場合は、.dbc ファイルをアップロードしてシグナルをインポートできます。.dbc は、コントローラーエリアネットワーク (CAN バス) データベースがサポートするファイル形式です。車両モデルが作成された後、新しいシグナルが自動的にシグナルカタログに追加されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。
> - `CreateModelManifest` API オペレーションを使用して車両モデルを作成する場合は、`UpdateModelManifest` API オペレーションを使用して車両モデルをアクティブ化する必要があります。詳細については、「AWS IoT FleetWise 車両モデルを更新する」を参照してください。
> - AWS IoT FleetWise コンソールを使用して車両モデルを作成すると、 AWS IoT FleetWise は自動的に車両モデルをアクティブ化します。

4. デコーダーマニフェストを作成します。デコーダーマニフェストには、前のステップで作成した車両モデルに指定されているすべてのシグナルのデコード情報が格納されます。デコーダーマニフェストは、作成した車両モデルに関連付けられます。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

> **Note**
>
> - `CreateDecoderManifest` API オペレーションを使用してデコーダーマニフェストを作成する場合は、`UpdateDecoderManifest` API オペレーションを使用してデコーダーマニフェストをアクティブ化する必要があります。詳細については、「AWS IoT FleetWise デコーダーマニフェストを更新する」を参照してください。
> - AWS IoT FleetWise コンソールを使用してデコーダーマニフェストを作成すると、AWS IoT FleetWise は自動的にデコーダーマニフェストをアクティブ化します。

5. 車両モデルから車両を作成します。同じ車両モデルから作成された車両は、同じシグナルのグループを継承します。クラウド AWS IoT Core にデータを取り込む前に、 を使用して車両をプロビジョニングする必要があります。詳細については、「Manage AWS IoT FleetWise 車両」を参照してください。
6. (オプション) 車両のグループを表すフリートを作成し、個々の車両をそのフリートに関連付けます。これにより、複数の車両を同時に管理できます。詳細については、「AWS IoT FleetWise でフリートを管理する」を参照してください。
7. (オプション) キャンペーンを作成します。キャンペーンは、車両または車両のフリートにデプロイされます。キャンペーンにより、データをどのように選択して収集し、クラウドに転送するかに関する指示がエッジエージェントソフトウェアに与えられます。詳細については、「キャンペーンを使用して AWS IoT FleetWise データを収集する」を参照してください。キャンペーン、状態テンプレート (以下) 、またはその両方を作成してデータを収集できます。

> **Note**
>
> AWS IoT FleetWise がキャンペーンを車両またはフリートにデプロイする前に、`UpdateCampaign` API オペレーションを使用してキャンペーンを承認する必要があります。詳細については、「AWS IoT FleetWise キャンペーンを更新する」を参照してください。

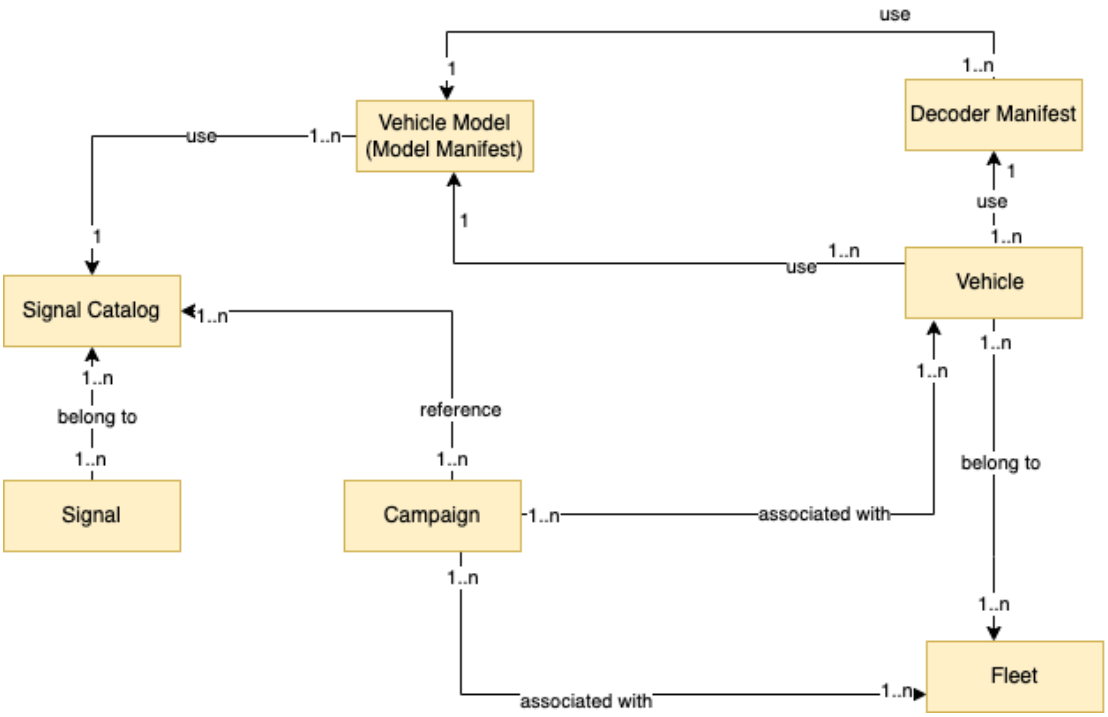
8. (オプション) 状態テンプレートを作成します。状態テンプレートは車両にデプロイされます。状態テンプレートは、車両所有者が車両の状態を追跡するためのメカニズムを提供します。詳細については、「車両の最終状態をモニタリングする」を参照してください。

エッジエージェントソフトウェアは、選択した MQTT トピック AWS IoT Core を使用して車両データを に転送します。キャンペーンのデータを AWS IoT FleetWise に送信するには、予約済

みトピック を使用します`$aws/iotfleetwise/vehicles/vehicleName/signals`。最終既知の状態の場合、エッジエージェントは予約済みトピック を使用します`$aws/iotfleetwise/vehicles/vehicleName/last_known_states/data`。取り込まれたデータの処理方法の詳細については、「」を参照してください[Visualize AWS IoT FleetWise 車両データ](#)。

Model AWS IoT FleetWise 車両

AWS IoT FleetWise は、クラウドで車両の仮想表現を構築するために使用できる車両モデリングフレームワークを提供します。車両のモデル化に使用するコアコンポーネントには、シグナル、シグナルカタログ、車両モデル、デコーダーマニフェストがあります。



シグナル

シグナルは、車両データとそのメタデータを格納するために定義する基本構造です。シグナルには、属性、ブランチ、センサー、アクチュエータがあります。例えば、車内の温度値を受け取るセンサーを作成し、そのメタデータ (センサー名、データ型、単位など) を格納できます。詳細については、「Manage AWS IoT FleetWise シグナルカタログ」を参照してください。

シグナルカタログ

シグナルカタログには、シグナルのコレクションが格納されます。シグナルカタログ内のシグナルを使用して、さまざまなプロトコルやデータ形式を使用する車両をモデル化できます。例えば、異なる自動車メーカーの 2 台の車があるとします。1 台はコントローラーエリアネットワーク (CAN バス) プロトコルを使用し、もう 1 台はオンボードダイアグノーシス (OBD) プロトコルを使用しています。シグナルカタログには、車内の温度値を受信するセンサーを定義することができます。このセンサーを、両方の車の熱電対を表すために使用できます。詳細については、「Manage AWS IoT FleetWise シグナルカタログ」を参照してください。

車両モデル (モデルマニフェスト)

車両モデルとは、車両の形式を標準化し、車両内のシグナル間の関係を定義するために使用できる宣言的な構造です。車両モデルにより、同じタイプの複数の車両に一貫した情報が適用されます。車両モデルを作成するには、シグナルを追加します。詳細については、「Manage AWS IoT FleetWise 車両モデル」を参照してください。

デコーダーマニフェスト

デコーダーマニフェストには、車両モデル内の各シグナルのデコード情報が含まれています。車両内のセンサーやアクチュエータが送信するのは、低レベルのメッセージ (バイナリデータ) です。デコーダーマニフェストを使用すると、 AWS IoT FleetWise はバイナリデータを人間が読み取れる値に変換できます。すべてのデコーダーマニフェストは車両モデルに関連付けられます。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

AWS IoT FleetWise コンソールまたは API を使用して、次の方法で車両をモデル化できます。

1. 車両モデルの作成に使用するシグナルを含むシグナルカタログを作成またはインポートします。詳細については、「AWS IoT FleetWise シグナルカタログを作成する」および「シグナルカタログのインポート (AWS CLI)」を参照してください。

   > **Note**
   >
   > - AWS IoT FleetWise コンソールを使用して最初の車両モデルを作成する場合、シグナルカタログを手動で作成する必要はありません。最初の車両モデルを作成すると、 AWS IoT FleetWise によって自動的にシグナルカタログが作成されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。
   > - AWS IoT FleetWise は現在、 ごとに各 AWS アカウントのシグナルカタログをサポートしています AWS リージョン。

2. シグナルカタログ内のシグナルを使用して、車両モデルを作成します。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

   > **Note**
   >
   > - AWS IoT FleetWise コンソールを使用して車両モデルを作成する場合は、.dbc ファイルをアップロードしてシグナルをインポートできます。.dbc は、コントローラーエリアネットワーク (CAN バス) データベースがサポートするファイル形式です。車両モデル

が作成された後、新しいシグナルが自動的にシグナルカタログに追加されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

- `CreateModelManifest` API オペレーションを使用して車両モデルを作成する場合は、`UpdateModelManifest` API オペレーションを使用して車両モデルをアクティブ化する必要があります。詳細については、「AWS IoT FleetWise 車両モデルを更新する」を参照してください。
- AWS IoT FleetWise コンソールを使用して車両モデルを作成すると、 AWS IoT FleetWise は自動的に車両モデルをアクティブ化します。

3. デコーダーマニフェストを作成します。デコーダーマニフェストには、前のステップで作成した車両モデルに指定されているすべてのシグナルのデコード情報が格納されます。デコーダーマニフェストは、作成した車両モデルに関連付けられます。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

> **Note**
>
> - `CreateDecoderManifest` API オペレーションを使用してデコーダーマニフェストを作成する場合は、`UpdateDecoderManifest` API オペレーションを使用してデコーダーマニフェストをアクティブ化する必要があります。詳細については、「AWS IoT FleetWise デコーダーマニフェストを更新する」を参照してください。
> - AWS IoT FleetWise コンソールを使用してデコーダーマニフェストを作成すると、AWS IoT FleetWise は自動的にデコーダーマニフェストをアクティブ化します。

CAN バスデータベースは .dbc ファイル形式をサポートしています。.dbc ファイルをアップロードして、シグナルとシグナルデコーダーをインポートできます。サンプルの .dbc ファイルを取得するには、次の手順を実行します。

.dbc ファイルを取得するには

1. EngineSignals.zip をダウンロードします。
2. `EngineSignals.zip` ファイルをダウンロードしたディレクトリに移動します。
3. ファイルを解凍し、`EngineSignals.dbc` としてローカルに保存します。

トピック

- Manage AWS IoT FleetWise シグナルカタログ

- Manage AWS IoT FleetWise 車両モデル
- Manage AWS IoT FleetWise デコーダーマニフェスト

Manage AWS IoT FleetWise シグナルカタログ

> **Note**
>
> デモスクリプトをダウンロードして、ROS 2 メッセージをシグナルカタログと互換性のある VSS .json ファイルに変換できます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。

シグナルカタログは、車両モデルを作成するために再利用できる標準化されたシグナルのコレクションです。 AWS IoT FleetWise は、シグナルの定義に使用できる車両シグナル仕様 (VSS) をサポートしています。シグナルには次のタイプがあります。

属性

属性は、製造元や製造日など、通常は変更されない静的な情報を表します。

ブランチ

ブランチとは、ネストされた構造内のシグナルを表します。ブランチは、シグナルの階層を明確に示します。例えば、`Vehicle` というブランチに `Powertrain` という子ブランチがあるとします。`Powertrain` ブランチには `combustionEngine` という子ブランチがあります。`combustionEngine` ブランチを特定するには、`Vehicle.Powertrain.combustionEngine` という式を使用します。

センサー

センサーデータは、液面、温度、振動、電圧などの車両の状態について、現在の状態と経時的な変化を報告します。

アクチュエータ

アクチュエータデータは、モーター、ヒーター、ドアロックなど、車両デバイスの状態を報告します。車両デバイスの状態を変更すると、アクチュエータデータが更新される可能性があります。例えば、ヒーターを表すアクチュエータを定義できます。このアクチュエータは、ヒーターをオンまたはオフにしたときに新しいデータを受け取ります。

カスタム構造

カスタム構造 (構造体とも呼ばれる) は、複雑なデータ構造または高次のデータ構造を表します。これにより、同じソースから生成されたデータの論理的なバインドやグループ化が容易になります。構造体は、複雑なデータ型や高次の形状を表すなど、アトミック操作でデータを読み書きする場合に使用します。

構造体型のシグナルは、プリミティブデータ型の代わりに構造体データ型への参照を使用してシグナルカタログで定義します。構造体は、センサー、属性、アクチュエータ、ビジョンシステムデータ型など、あらゆるタイプのシグナルに使用できます。構造体タイプのシグナルが送受信された場合、 AWS IoT FleetWise は含まれるすべての項目に有効な値があることを期待するため、すべての項目が必須です。例えば、構造体内に項目として Vehicle.Camera.Image.height、Vehicle.Camera.Image.width、Vehicle.Camera.Image.data が含まれている場合、送信されたシグナルには、これらすべての項目の値が含まれていることが期待されます。

> **Note**
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

カスタムプロパティ

カスタムプロパティは複雑なデータ構造のメンバーを表します。プロパティのデータ型は、プリミティブまたは別の構造体のいずれかになります。

構造体とカスタムプロパティを使用して高次の形状を表現する場合、意図した高次の形状は常にツリー構造として定義され、視覚化されます。カスタムプロパティはすべてのリーフノードを定義するために使用し、構造体はリーフ以外のすべてのノードを定義するために使用します。

> **Note**
>
> - AWS IoT FleetWise コンソールを使用して最初の車両モデルを作成する場合、シグナルカタログを手動で作成する必要はありません。最初の車両モデルを作成すると、 AWS IoT FleetWise によって自動的にシグナルカタログが作成されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。
> - AWS IoT FleetWise コンソールを使用して車両モデルを作成する場合は、.dbc ファイルをアップロードしてシグナルをインポートできます。.dbc は、コントローラーエリアネット

ワーク (CAN バス) データベースがサポートするファイル形式です。車両モデルが作成された後、新しいシグナルが自動的にシグナルカタログに追加されます。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

- AWS IoT FleetWise は現在、リージョン AWS アカウント ごとに ごとにシグナルカタログをサポートしています。

AWS IoT FleetWise には、シグナルカタログの作成と管理に使用できる以下の API オペレーションが用意されています。

- CreateSignalCatalog - 新しいシグナルカタログを作成します。
- ImportSignalCatalog – シグナルをインポートして、.json ファイルをアップロードしてシグナルカタログを作成します。シグナルは VSS に従って定義し、JSON 形式で保存する必要があります。
- UpdateSignalCatalog - 既存のシグナルカタログを更新して、シグナルを更新、削除、または追加します。
- DeleteSignalCatalog - 既存のシグナルカタログを削除します。
- ListSignalCatalogs - すべてのシグナルカタログの概要をページ分割されたリストとして取得します。
- ListSignalCatalogNodes - 特定のシグナルカタログに含まれているすべてのシグナル (ノード) の概要をページ分割されたリストとして取得します。
- GetSignalCatalog - シグナルカタログに関する情報を取得します。

チュートリアル

- AWS IoT FleetWise シグナルを設定する
- AWS IoT FleetWise シグナルカタログを作成する
- AWS IoT FleetWise シグナルカタログをインポートする
- AWS IoT FleetWise シグナルカタログを更新する
- AWS IoT FleetWise シグナルカタログを削除する
- Get AWS IoT FleetWise シグナルカタログ情報

AWS IoT FleetWise シグナルを設定する

このセクションでは、ブランチ、属性、センサー、アクチュエータの構成方法を説明します。

トピック

- ブランチの構成
- 属性の構成
- センサーまたはアクチュエータの構成
- 複雑なデータ型の設定

ブランチの構成

ブランチを構成するには、以下の情報を指定します。

- `fullyQualifiedName` - ブランチの完全修飾名。ブランチのパスにブランチの名前を続けたものです。子ブランチを参照するには、ドット (.) を使用します。例えば、`Vehicle.Chassis.SteeringWheel` は `SteeringWheel` ブランチの完全修飾名です。`Vehicle.Chassis.` はこのブランチのパスを示します。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、コロン (:)、アンダースコア (_) です。
- (オプション) `Description` - ブランチの説明。

  説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `deprecationMessage` - 移動または削除されるノードやブランチに関する非推奨メッセージ。

  deprecationMessage には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `comment` - 説明に追加するコメント。コメントは、ブランチに関する追加情報を提供するために使用できます。例えば、ブランチの意図や、関連するブランチへの参照を示すことができます。

  コメントには最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。

属性の構成

属性を構成するには、以下の情報を指定します。

- `dataType` - 属性のデータ型は、INT8、UINT8、INT16、UINT16、INT32、UINT32、INT64、UINT64、BOOLEAN、FLOAT、DOUBL またはデータ型ブランチに定義されているカスタム構造体のいずれかである必要があります。
- `fullyQualifiedName` - 属性の完全修飾名は、属性のパスに属性名を続けたものです。子シグナルを参照するには、ドット (.) を使用します。例えば、`Vehicle.Chassis.SteeringWheel.Diameter` は `Diameter` 属性の完全修飾名です。`Vehicle.Chassis.SteeringWheel.` はこの属性のパスを示します。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
- (オプション) `Description` - 属性の説明。

  説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `unit` - 属性の科学単位 (km、摂氏など)。
- (オプション) `min` - 属性の最小値。
- (オプション) `max` - 属性の最大値。
- (オプション) `defaultValue` - 属性のデフォルト値。
- (オプション) `assignedValue` - 属性に割り当てられた値。
- (オプション) `allowedValues` - 属性が受け入れる値のリスト。
- (オプション) `deprecationMessage` - 移動または削除されるノードやブランチに関する非推奨メッセージ。

  deprecationMessage には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `comment` - 説明に追加するコメント。コメントは、属性に関する追加情報を提供するために使用できます。例えば、属性の意図や、関連する属性への参照を示すことができます。

  コメントには最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。

センサーまたはアクチュエータの構成

センサーまたはアクチュエータを構成するには、以下の情報を指定します。

- `dataType` - シグナルのデータ型は、INT8、UINT8、INT16、UINT16、INT32、UINT32、INT64、UINT64、BOOLEAN、FLOAT、DOUBL またはデータ型ブランチに定義されているカスタム構造体のいずれかである必要があります。
- `fullyQualifiedName` - シグナルの完全修飾名は、シグナルのパスにシグナルの名前を続けたものです。子シグナルを参照するには、ドット (.) を使用します。例えば、`Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringState` は `HandsOffSteeringState` アクチュエータの完全修飾名です。`Vehicle.Chassis.SteeringWheel.HandsOff.` はこのアクチュエータのパスを示します。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
- (オプション) `Description` - シグナルの説明。

  説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `unit` – km や摂氏など、シグナルの科学単位。
- (オプション) `min` - シグナルの最小値。
- (オプション) `max` - シグナルの最大値。
- (オプション) `assignedValue` - シグナルに割り当てられた値。
- (オプション) `allowedValues` - シグナルが受け入れる値のリスト。
- (オプション) `deprecationMessage` - 移動または削除されるノードやブランチに関する非推奨メッセージ。

  deprecationMessage には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `comment` - 説明に追加するコメント。コメントは、センサーやアクチュエータに関する追加情報を提供するために使用できます。例えば、それらの意図や、関連するセンサーまたはアクチュエータへの参照を示すことができます。

  コメントには最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。

複雑なデータ型の設定

複雑なデータ型は、ビジョンシステムをモデル化するときに使用します。これらのデータ型は、ブランチに加えて、構造 (構造体とも呼ばれる) とプロパティで構成されます。構造体は、画像のように、複数の値で記述されるシグナルです。プロパティは、プリミティブデータ型 (UINT8 など) や別の構造体 (タイムスタンプなど) など、構造体のメンバーを表します。例えば、Vehicle.Cameras.Front はブランチを表し、Vehicle.Cameras.Front.Image は構造体を表し、Vehicle.Cameras.Timestamp はプロパティを表します。

次の複雑なデータ型の例は、シグナルとデータ型を 1 つの .json ファイルにエクスポートする方法を示しています。

Example 複雑なデータ型

```
{
  "Vehicle": {
    "type": "branch"
    // Signal tree
  },
  "ComplexDataTypes": {
    "VehicleDataTypes": {
      // complex data type tree
      "children": {
        "branch": {
          "children": {
            "Struct": {
              "children": {
                "Property": {
                  "type": "property",
                  "datatype": "Data type",
                  "description": "Description",
                  //                  ...
                }
              },
              "description": "Description",
              "type": "struct"
            }
          }
          "description": "Description",
          "type": "branch"
        }
      }
    }
```

```
  }
}
```

> **Note**
>
> デモスクリプトをダウンロードして、ROS 2 メッセージをシグナルカタログと互換性のある VSS .json ファイルに変換できます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

構造体の設定

カスタム構造 (または構造体) を設定するには、以下の情報を指定します。

- `fullyQualifiedName` — カスタム構造の完全修飾名。例えば、カスタム構造の完全修飾名は `ComplexDataTypes.VehicleDataTypes.SVMCamera` です。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
- (オプション) `Description` - シグナルの説明。

  説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `deprecationMessage` - 移動または削除されるノードやブランチに関する非推奨メッセージ。

  deprecationMessage には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `comment` - 説明に追加するコメント。コメントは、センサーやアクチュエータに関する追加情報を提供するために使用できます。例えば、それらの意図や、関連するセンサーまたはアクチュエータへの参照を示すことができます。

  コメントには最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。

プロパティの設定

カスタムプロパティを設定するには、以下の情報を指定します。

- `dataType` - シグナルのデータ型は、INT8、UINT8、INT16、UINT16、INT32、UINT32、INT64、UINT64、BOOLEAN、FLOAT、DOUBL のいずれかである必要があります。
- `fullyQualifiedName` — カスタムプロパティの完全修飾名。例えば、カスタムプロパティの完全修飾名は `ComplexDataTypes.VehicleDataTypes.SVMCamera.FPS` です。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
- (オプション) `Description` - シグナルの説明。

  説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `deprecationMessage` - 移動または削除されるノードやブランチに関する非推奨メッセージ。

  deprecationMessage には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `comment` - 説明に追加するコメント。コメントは、センサーやアクチュエータに関する追加情報を提供するために使用できます。例えば、それらの意図や、関連するセンサーまたはアクチュエータへの参照を示すことができます。

  コメントには最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
- (オプション) `dataEncoding` — プロパティがバイナリデータかどうかを示します。カスタムプロパティのデータエンコーディングは、BINARY または TYPED のいずれかである必要があります。
- (オプション) `structFullyQualifiedName` — カスタムプロパティのデータ型が Struct または StructArray の場合、カスタムプロパティの構造 (構造体) ノードの完全修飾名。

  完全修飾名には最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。

AWS IoT FleetWise シグナルカタログを作成する

CreateSignalCatalog API オペレーションを使用すると、シグナルカタログを作成できます。次の例では、 を使用します AWS CLI。

シグナルカタログを作成するには、次のコマンドを実行します。

signal-catalog-configuration を、設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-signal-catalog --cli-input-json file://signal-catalog-configuration.json
```

- *signal-catalog-name* は、作成するシグナルカタログの名前に置き換えます。
- (オプション) *description* は、シグナルカタログの識別に役立つ説明に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「AWS IoT FleetWise シグナルを設定する」を参照してください。

```
{
    "name": "signal-catalog-name",
    "description": "description",
    "nodes": [
  {
    "branch": {
      "fullyQualifiedName": "Types"
    }
  },
  {
    "struct": {
      "fullyQualifiedName": "Types.sensor_msgs_msg_CompressedImage"
    }
  },
  {
    "struct": {
      "fullyQualifiedName": "Types.std_msgs_Header"
    }
  },
  {
    "struct": {
      "fullyQualifiedName": "Types.builtin_interfaces_Time"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.builtin_interfaces_Time.sec",
      "dataType": "INT32",
      "dataEncoding": "TYPED"
    }
```

```
  },
  {
    "property": {
      "fullyQualifiedName": "Types.builtin_interfaces_Time.nanosec",
      "dataType": "UINT32",
      "dataEncoding": "TYPED"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.std_msgs_Header.stamp",
      "dataType": "STRUCT",
      "structFullyQualifiedName": "Types.builtin_interfaces_Time"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.std_msgs_Header.frame_id",
      "dataType": "STRING",
      "dataEncoding": "TYPED"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.sensor_msgs_msg_CompressedImage.header",
      "dataType": "STRUCT",
      "structFullyQualifiedName": "Types.std_msgs_Header"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.sensor_msgs_msg_CompressedImage.format",
      "dataType": "STRING",
      "dataEncoding": "TYPED"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.sensor_msgs_msg_CompressedImage.data",
      "dataType": "UINT8_ARRAY",
      "dataEncoding": "BINARY"
    }
  },
  {
```

```
    "branch": {
      "fullyQualifiedName": "Vehicle",
      "description": "Vehicle"
    }
  },
  {
    "branch": {
      "fullyQualifiedName": "Vehicle.Cameras"
    }
  },
  {
    "branch": {
      "fullyQualifiedName": "Vehicle.Cameras.Front"
    }
  },
  {
    "sensor": {
      "fullyQualifiedName": "Vehicle.Cameras.Front.Image",
      "dataType": "STRUCT",
      "structFullyQualifiedName": "Types.sensor_msgs_msg_CompressedImage"
    }
  },
  {
    "struct": {
      "fullyQualifiedName": "Types.std_msgs_msg_Float64"
    }
  },
  {
    "property": {
      "fullyQualifiedName": "Types.std_msgs_msg_Float64.data",
      "dataType": "DOUBLE",
      "dataEncoding": "TYPED"
    }
  },
  {
    "sensor": {
      "fullyQualifiedName": "Vehicle.Velocity",
      "dataType": "STRUCT",
      "structFullyQualifiedName": "Types.std_msgs_msg_Float64"
    }
  },
  {
    "struct": {
      "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest"
```

```
      }
    },
    {
      "property": {
        "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest.x_offset",
        "dataType": "UINT32",
        "dataEncoding": "TYPED"
      }
    },
    {
      "property": {
        "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest.y_offset",
        "dataType": "UINT32",
        "dataEncoding": "TYPED"
      }
    },
    {
      "property": {
        "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest.height",
        "dataType": "UINT32",
        "dataEncoding": "TYPED"
      }
    },
    {
      "property": {
        "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest.width",
        "dataType": "UINT32",
        "dataEncoding": "TYPED"
      }
    },
    {
      "property": {
        "fullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest.do_rectify",
        "dataType": "BOOLEAN",
        "dataEncoding": "TYPED"
      }
    },
    {
      "branch": {
        "fullyQualifiedName": "Vehicle.Perception"
      }
    },
    {
      "sensor": {
```

```
      "fullyQualifiedName": "Vehicle.Perception.Obstacle",
      "dataType": "STRUCT",
      "structFullyQualifiedName": "Types.sensor_msgs_msg_RegionOfInterest"
    }
  }
]
}
```

> **Note**
>
> デモスクリプトをダウンロードして、ROS 2 メッセージをシグナルカタログと互換性のある VSS .json ファイルに変換できます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateSignalCatalog` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise シグナルカタログをインポートする

AWS IoT FleetWise コンソールまたは API を使用して、シグナルカタログをインポートできます。

トピック

- シグナルカタログのインポート (コンソール)
- シグナルカタログのインポート (AWS CLI)

シグナルカタログのインポート (コンソール)

AWS IoT FleetWise コンソールを使用して、シグナルカタログをインポートできます。

> **Important**
> 使用できるシグナルカタログは最大 1 つです。シグナルカタログが既に存在する場合、コンソールにはシグナルカタログをインポートするオプションは表示されません。

シグナルカタログをインポートするには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[シグナルカタログ] を選択します。
3. シグナルカタログの概要ページで、[シグナルカタログをインポート] を選択します。
4. シグナルを含むファイルをインポートします。
   - S3 バケットからファイルをアップロードするには:
     a. [S3 からインポート] を選択します。
     b. [S3 を参照] を選択します。
     c. [バケット] で、バケット名またはオブジェクトを入力し、リストから選択します。次に、リストからファイルを選択します。[ファイルを選択] ボタンを選択します。

     または、[S3 URI] に Amazon Simple Storage Service の URI を入力します。詳細については、「Amazon S3 ユーザーガイド」の「バケットへのアクセス方法」を参照してください。
   - コンピュータからファイルをアップロードするには:
     a. [ファイルをインポート] を選択します。
     b. Vehicle Signal Specification (VSS) 形式の .json ファイルをアップロードします。
5. シグナルカタログを確認し、[ファイルをインポート] を選択します。

シグナルカタログのインポート (AWS CLI)

ImportSignalCatalog API オペレーションを使用すると、シグナルカタログを作成するための JSON ファイルをアップロードできます。JSON ファイルにシグナルを保存するには、Vehicle Signal Specification (VSS) に従う必要があります。次の例では、 を使用します AWS CLI。

シグナルカタログをインポートするには、次のコマンドを実行します。

- *signal-catalog-name* は、作成するシグナルカタログの名前に置き換えます。
- (オプション) *description* は、シグナルカタログの識別に役立つ説明に置き換えます。
- *signal-catalog-configuration-vss* は、VSS で定義されたシグナルを含む JSON 文字列ファイルの名前に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「AWS IoT FleetWise シグナルを設定する」を参照してください。

```
aws iotfleetwise import-signal-catalog \
                 --name signal-catalog-name \
                 --description  description \
                 --vss file://signal-catalog-configuration-vss.json
```

JSON は、文字列化して `vssJson` フィールドに渡す必要があります。以下は、VSS で定義されたシグナルの例です。

```
{
 "Vehicle": {
  "type": "branch",
  "children": {
   "Chassis": {
    "type": "branch",
    "description": "All data concerning steering, suspension, wheels, and brakes.",
    "children": {
     "SteeringWheel": {
      "type": "branch",
      "description": "Steering wheel signals",
      "children": {
       "Diameter": {
        "type": "attribute",
        "description": "The diameter of the steering wheel",
        "datatype": "float",
```

```
        "unit": "cm",
        "min": 1,
        "max": 50
       },
       "HandsOff": {
        "type": "branch",
        "children": {
         "HandsOffSteeringState": {
          "type": "actuator",
          "description": "HndsOffStrWhlDtSt. Hands Off Steering State",
          "datatype": "boolean"
         },
         "HandsOffSteeringMode": {
          "type": "actuator",
          "description": "HndsOffStrWhlDtMd. Hands Off Steering Mode",
          "datatype": "int8",
          "min": 0,
          "max": 2
         }
        }
       }
      }
     },
     "Accelerator": {
      "type": "branch",
      "description": "",
      "children": {
       "AcceleratorPedalPosition": {
        "type": "sensor",
        "description": "Throttle__Position. Accelerator pedal position as percent. 0 =
 Not depressed. 100 = Fully depressed.",
        "datatype": "uint8",
        "unit": "%",
        "min": 0,
        "max": 100.000035
       }
      }
     }
    }
   },
   "Powertrain": {
    "type": "branch",
    "description": "Powertrain data for battery management, etc.",
    "children": {
```

```
      "Transmission": {
       "type": "branch",
       "description": "Transmission-specific data, stopping at the drive shafts.",
       "children": {
        "VehicleOdometer": {
         "type": "sensor",
         "description": "Vehicle_Odometer",
         "datatype": "float",
         "unit": "km",
         "min": 0,
         "max": 67108863.984375
        }
       }
      },
      "CombustionEngine": {
       "type": "branch",
       "description": "Engine-specific data, stopping at the bell housing.",
       "children": {
        "Engine": {
         "type": "branch",
         "description": "Engine description",
         "children": {
          "timing": {
           "type": "branch",
           "description": "timing description",
           "children": {
            "run_time": {
             "type": "sensor",
             "description": "Engine run time",
             "datatype": "int16",
             "unit": "ms",
             "min": 0,
             "max": 10000
            },
            "idle_time": {
             "type": "sensor",
             "description": "Engine idle time",
             "datatype": "int16",
             "min": 0,
             "unit": "ms",
             "max": 10000
            }
           }
          }
```

```
        }
       }
      }
     }
    }
   },
   "Axle": {
    "type": "branch",
    "description": "Axle signals",
    "children": {
     "TireRRPrs": {
      "type": "sensor",
      "description": "TireRRPrs. Right rear Tire pressure in kilo-Pascal",
      "datatype": "float",
      "unit": "kPaG",
      "min": 0,
      "max": 1020
     }
    }
   }
  }
 },
 "Cameras": {
  "type": "branch",
  "description": "Branch to aggregate all cameras in the vehicle",
  "children": {
   "FrontViewCamera": {
    "type": "sensor",
    "datatype": "VehicleDataTypes.SVMCamera",
    "description": "Front view camera"
   },
   "RearViewCamera": {
    "type": "sensor",
    "datatype": "VehicleDataTypes.SVMCamera",
    "description": "Rear view camera"
   },
   "LeftSideViewCamera": {
    "type": "sensor",
    "datatype": "VehicleDataTypes.SVMCamera",
    "description": "Left side view camera"
   },
   "RightSideViewCamera": {
    "type": "sensor",
    "datatype": "VehicleDataTypes.SVMCamera",
```

```
    "description": "Right side view camera"
   }
  }
 },
 "ComplexDataTypes": {
  "VehicleDataTypes": {
   "type": "branch",
   "description": "Branch to aggregate all camera related higher order data types",
   "children": {
    "SVMCamera": {
     "type": "struct",
     "description": "This data type represents Surround View Monitor (SVM) camera
system in a vehicle",
     "comment": "Test comment",
     "deprecation": "Test deprecation message",
     "children": {
      "Make": {
       "type": "property",
       "description": "Make of the SVM camera",
       "datatype": "string",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "Description": {
       "type": "property",
       "description": "Description of the SVM camera",
       "datatype": "string",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "FPS": {
       "type": "property",
       "description": "FPS of the SVM camera",
       "datatype": "double",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "Orientation": {
       "type": "property",
       "description": "Orientation of the SVM camera",
       "datatype": "VehicleDataTypes.Orientation",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
```

```
      "Range": {
       "type": "property",
       "description": "Range of the SVM camera",
       "datatype": "VehicleDataTypes.Range",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "RawData": {
       "type": "property",
       "description": "Represents binary data of the SVM camera",
       "datatype": "uint8[]",
       "dataencoding": "binary",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "CapturedFrames": {
       "type": "property",
       "description": "Represents selected frames captured by the SVM camera",
       "datatype": "VehicleDataTypes.Frame[]",
       "dataencoding": "typed",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      }
     }
    },
    "Range": {
     "type": "struct",
     "description": "Range of a camera in centimeters",
     "comment": "Test comment",
     "deprecation": "Test deprecation message",
     "children": {
      "Min": {
       "type": "property",
       "description": "Minimum range of a camera in centimeters",
       "datatype": "uint32",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "Max": {
       "type": "property",
       "description": "Maximum range of a camera in centimeters",
       "datatype": "uint32",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
```

```
      }
     }
    },
    "Orientation": {
     "type": "struct",
     "description": "Orientation of a camera",
     "comment": "Test comment",
     "deprecation": "Test deprecation message",
     "children": {
      "Front": {
       "type": "property",
       "description": "Indicates whether the camera is oriented to the front of the
 vehicle",
       "datatype": "boolean",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "Rear": {
       "type": "property",
       "description": "Indicates whether the camera is oriented to the rear of the
 vehicle",
       "datatype": "boolean",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      },
      "Side": {
       "type": "property",
       "description": "Indicates whether the camera is oriented to the side of the
 vehicle",
       "datatype": "boolean",
       "comment": "Test comment",
       "deprecation": "Test deprecation message"
      }
     }
    },
    "Frame": {
     "type": "struct",
     "description": "Represents a camera frame",
     "comment": "Test comment",
     "deprecation": "Test deprecation message",
     "children": {
      "Data": {
       "type": "property",
       "datatype": "string",
```

```
        "dataencoding": "binary",
        "comment": "Test comment",
        "deprecation": "Test deprecation message"
       }
      }
     }
    }
   }
  }

}
```

次の例は、VSS で定義されたものと同じシグナルを JSON 文字列で示しています。


```
{
   "vssJson": "{\"Vehicle\":{\"type\":\"branch\",\"children\":{\"Chassis\":{\"type
\":\"branch\",\"description\":\"All data concerning steering, suspension, wheels,
 and brakes.\",\"children\":{\"SteeringWheel\":{\"type\":\"branch\",\"description
\":\"Steering wheel signals\",\"children\":{\"Diameter\":{\"type\":\"attribute\",
\"description\":\"The diameter of the steering wheel\",\"datatype\":\"float\",\"unit
\":\"cm\",\"min\":1,\"max\":50},\"HandsOff\":{\"type\":\"branch\",\"children\":
{\"HandsOffSteeringState\":{\"type\":\"actuator\",\"description\":\"HndsOffStrWhlDtSt.
 Hands Off Steering State\",\"datatype\":\"boolean\"},\"HandsOffSteeringMode\":
{\"type\":\"actuator\",\"description\":\"HndsOffStrWhlDtMd. Hands Off Steering Mode
\",\"datatype\":\"int8\",\"min\":0,\"max\":2}}}}},\"Accelerator\":{\"type\":\"branch
\",\"description\":\"\",\"children\":{\"AcceleratorPedalPosition\":{\"type\":\"sensor
\",\"description\":\"Throttle__Position. Accelerator pedal position as percent. 0
 = Not depressed. 100 = Fully depressed.\",\"datatype\":\"uint8\",\"unit\":\"%\",
\"min\":0,\"max\":100.000035}}}}},\"Powertrain\":{\"type\":\"branch\",\"description
\":\"Powertrain data for battery management, etc.\",\"children\":{\"Transmission\":
{\"type\":\"branch\",\"description\":\"Transmission-specific data, stopping at the
 drive shafts.\",\"children\":{\"VehicleOdometer\":{\"type\":\"sensor\",\"description
\":\"Vehicle_Odometer\",\"datatype\":\"float\",\"unit\":\"km\",\"min\":0,\"max
\":67108863.984375}}},\"CombustionEngine\":{\"type\":\"branch\",\"description\":
\"Engine-specific data, stopping at the bell housing.\",\"children\":{\"Engine\":
{\"type\":\"branch\",\"description\":\"Engine description\",\"children\":{\"timing\":
{\"type\":\"branch\",\"description\":\"timing description\",\"children\":{\"run_time\":
{\"type\":\"sensor\",\"description\":\"Engine run time\",\"datatype\":\"int16\",\"unit
\":\"ms\",\"min\":0,\"max\":10000},\"idle_time\":{\"type\":\"sensor\",\"description
\":\"Engine idle time\",\"datatype\":\"int16\",\"min\":0,\"unit\":\"ms\",\"max
\":10000}}}}}}}},\"Axle\":{\"type\":\"branch\",\"description\":\"Axle signals\",
\"children\":{\"TireRRPrs\":{\"type\":\"sensor\",\"description\":\"TireRRPrs. Right
```

```
 rear Tire pressure in kilo-Pascal\",\"datatype\":\"float\",\"unit\":\"kPaG\",\"min
\":0,\"max\":1020}}}}}"
}
```

> **Note**
>
> デモスクリプトをダウンロードして、ROS 2 メッセージを、シグナルカタログと互換性のある VSS JSON ファイルに変換できます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ImportSignalCatalog` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
{
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise シグナルカタログを更新する

既存のシグナルカタログを更新するには、UpdateSignalCatalog API オペレーションを使用します。次の例では、 を使用します AWS CLI。

既存のシグナルカタログを更新するには、次のコマンドを実行します。

`signal-catalog-configuration` を、設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise update-signal-catalog --cli-input-json file://signal-catalog-configuration.json
```

signal-catalog-name は、更新するシグナルカタログの名前に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「AWS IoT FleetWise シグナルを設定する」を参照してください。

> **Important**
>
> カスタム構造はイミュータブルです。既存のカスタム構造 (構造体) にプロパティの順序を変更または挿入する必要がある場合は、その構造を削除し、プロパティの順序でまったく新しい構造を作成します。
> カスタム構造を削除するには、構造の完全修飾名を nodesToRemove に追加します。シグナルが参照している構造は、削除できません。構造を参照するシグナル (そのデータ型はターゲット構造として定義されます) は、シグナルカタログの更新リクエストの前に、更新または削除する必要があります。

```
{
     "name": "signal-catalog-name",
     "nodesToAdd": [{
       "branch": {
        "description": "Front left of vehicle specific data.",
        "fullyQualifiedName": "Vehicle.Front.Left"
       }
      },
      {
       "branch": {
        "description": "Door-specific data for the front left of vehicle.",
        "fullyQualifiedName": "Vehicle.Front.Left.Door"
       }
      },
      {
       "actuator": {
        "fullyQualifiedName": "Vehicle.Front.Left.Door.Lock",
        "description": "Whether the front left door is locked.",
        "dataType": "BOOLEAN"
       }
      },
```

```
      {
       "branch": {
        "fullyQualifiedName": "Vehicle.Camera"
       }
      },
      {
       "struct": {
        "fullyQualifiedName": "Vehicle.Camera.SVMCamera"
       }
      },
      {
       "property": {
        "fullyQualifiedName": "Vehicle.Camera.SVMCamera.ISO",
        "dataType": "STRING"
       }
      }
     ],
     "nodesToRemove": ["Vehicle.Chassis.SteeringWheel.HandsOffSteeringState"],
     "nodesToUpdate": [{
      "attribute": {
       "dataType": "FLOAT",
       "fullyQualifiedName": "Vehicle.Chassis.SteeringWheel.Diameter",
       "max": 55
      }
     }]
    }
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `UpdateSignalCatalog` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
{
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
```

```
    },
  ]
}
```

シグナルカタログの更新を確認する

ListSignalCatalogNodes API オペレーションを使用して、シグナルカタログが更新されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

特定のシグナルカタログに含まれているすべてのシグナル (ノード) の概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

signal-catalog-name は、確認するシグナルカタログの名前に置き換えます。

```
aws iotfleetwise list-signal-catalog-nodes --name signal-catalog-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListSignalCatalogNodes` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise シグナルカタログを削除する

DeleteSignalCatalog API オペレーションを使用すると、シグナルカタログを削除できます。次の例では、 を使用します AWS CLI。

> **Important**
>
> シグナルカタログを削除する前に、関連付けられている車両モデル、デコーダーマニフェスト、車両、フリート、キャンペーンがないことを確認してください。手順については、以下を参照してください。
>
> - AWS IoT FleetWise 車両モデルを削除する
> - AWS IoT FleetWise デコーダーマニフェストを削除する
> - AWS IoT FleetWise 車両を削除する
> - AWS IoT FleetWise フリートを削除する
> - AWS IoT FleetWise キャンペーンを削除する

既存のシグナルカタログを削除するには、次のコマンドを実行します。*signal-catalog-name* は、削除するシグナルカタログの名前に置き換えます。

```
aws iotfleetwise delete-signal-catalog --name signal-catalog-name
```

シグナルカタログの削除を確認する

ListSignalCatalogs API オペレーションを使用すると、シグナルカタログが削除されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

すべてのシグナルカタログの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-signal-catalogs
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListSignalCatalogs` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
```

```
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Get AWS IoT FleetWise シグナルカタログ情報

GetSignalCatalog API オペレーションを使用すると、シグナルカタログの情報を取得できます。次の例では、 を使用します AWS CLI。

シグナルカタログに関する情報を取得するには、次のコマンドを実行します。

signal-catalog-name は、取得するシグナルカタログの名前に置き換えます。

```
aws iotfleetwise get-signal-catalog --name signal-catalog-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `GetSignalCatalog` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、シグナルカタログへの変更はすぐには反映されない場合があります。

Manage AWS IoT FleetWise 車両モデル

車両の形式を標準化するために役立つ車両モデルを作成するには、シグナルを使用します。車両モデルにより、同じタイプの複数の車両に一貫した情報が適用され、車両のフリートからのデータを処理できるようになります。同じ車両モデルから作成された車両は、同じシグナルのグループを継承します。詳細については、「Manage AWS IoT FleetWise 車両」を参照してください。

各車両モデルには、車両モデルの状態を含むステータスフィールドがあります。ステータスは以下のいずれかの値になります。

- `ACTIVE` - 車両モデルはアクティブです。
- `DRAFT` - 車両モデルの構成が保存されています。

> **Important**
>
> - `CreateModelManifest` API オペレーションを使用して車両モデルを作成する前に、シグナルカタログが必要です。詳細については、「AWS IoT FleetWise シグナルカタログを作成する」を参照してください。
> - AWS IoT FleetWise コンソールを使用して車両モデルを作成すると、 AWS IoT FleetWise は自動的に車両モデルをアクティブ化します。
> - `CreateModelManifest` API オペレーションを使用して車両モデルを作成する場合は、車両モデルは `DRAFT` 状態のままになります。
> - `DRAFT` 状態の車両モデルから車両を作成することはできません。車両モデルを `ACTIVE` 状態に変更するには、`UpdateModelManifest` API オペレーションを使用します。
> - `ACTIVE` 状態の車両モデルは編集できません。

トピック

- AWS IoT FleetWise 車両モデルを作成する

- AWS IoT FleetWise 車両モデルを更新する
- AWS IoT FleetWise 車両モデルを削除する
- Get AWS IoT FleetWise 車両モデル情報

AWS IoT FleetWise 車両モデルを作成する

AWS IoT FleetWise コンソールまたは API を使用して車両モデルを作成できます。

トピック

- 車両モデルの作成 (コンソール)
- 車両モデルの作成 (AWS CLI)

車両モデルの作成 (コンソール)

AWS IoT FleetWise コンソールでは、次の方法で車両モデルを作成できます。

- が提供するテンプレートを使用する AWS
- 車両モデルの手動作成
- 車両モデルの複製

が提供するテンプレートを使用する AWS

AWS IoT FleetWise には、シグナルカタログ、車両モデル、デコーダーマニフェストを自動的に作成するオンボード診断 (OBD) II、J1979 テンプレートが用意されています。このテンプレートでは、デコーダーマニフェストに OBD ネットワークインターフェイスも追加されます。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

テンプレートを使用して車両モデルを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. [車両モデル] ページで、[提供されたテンプレートを追加] を選択します。
4. [オンボードダイアグノーシス (OBD) II] を選択します。
5. AWS IoT FleetWise が作成する OBD ネットワークインターフェイスの名前を入力します。
6. [Add] (追加) を選択します。

車両モデルの手動作成

シグナルカタログからシグナルを追加したり、1 つ以上の .dbc ファイルをアップロードしてシグナルをインポートしたりできます。.dbc ファイルは、コントローラーエリアネットワーク (CAN バス) データベースでサポートされるファイル形式です。

> **Important**
>
> AWS IoT FleetWise コンソールを使用してビジョンシステムデータシグナルを持つ車両モデルを作成することはできません。代わりに、 AWS CLI を使用して車両モデルを作成します。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

車両モデルを手動で作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. [車両モデル] ページで、[車両モデルを作成] を選択し、次の操作を行います。

トピック

- ステップ 1: 車両モデルを構成する
- ステップ 2: シグナルを追加する
- ステップ 3: シグナルをインポートする
- (オプション) ステップ 4: 属性を追加する
- ステップ 5: 確認して作成する

ステップ 1: 車両モデルを構成する

[一般的な情報] セクションで、次の操作を行います。

1. 車両モデルの名前を入力します。
2. (オプション) 説明を入力します。
3. [次へ] を選択します。

ステップ 2: シグナルを追加する

> **Note**
>
> - AWS IoT FleetWise を初めて使用する場合、このステップはシグナルカタログを作成するまで使用できません。最初の車両モデルが作成されると、 AWS IoT FleetWise は最初の車両モデルに追加されたシグナルを含むシグナルカタログを自動的に作成します。
> - AWS IoT FleetWise の経験がある場合は、シグナルカタログからシグナルを選択するか、.dbc ファイルをアップロードしてシグナルをインポートすることで、車両モデルにシグナルを追加できます。
> - 車両モデルを作成するには、1 つ以上のシグナルが必要です。

シグナルを追加するには

1. シグナルカタログから、車両モデルに追加するシグナルを 1 つ以上選択します。選択したシグナルは右側のペインで確認できます。

   > **Note**
   >
   > 選択したシグナルだけが車両モデルに追加されます。

2. [次へ] を選択します。

ステップ 3: シグナルをインポートする

> **Note**
>
> - AWS IoT FleetWise を初めて使用する場合は、少なくとも 1 つの .dbc ファイルをアップロードしてシグナルをインポートする必要があります。
> - AWS IoT FleetWise の経験がある場合は、シグナルカタログからシグナルを選択するか、.dbc ファイルをアップロードしてシグナルをインポートすることで、車両モデルにシグナルを追加できます。
> - 車両モデルを作成するには、1 つ以上のシグナルが必要です。

シグナルをインポートするには

1. [ファイルを選択] を選択します。
2. ダイアログボックスで、シグナルを含む .dbc ファイルを選択します。複数の .dbc ファイルをアップロードできます。
3. AWS IoT FleetWise は .dbc ファイルを解析してシグナルを取得します。

   [シグナル] セクションで、シグナルごとに以下のメタデータを指定します。

   - [名前] - シグナルの名前。

     シグナル名は一意である必要があります。シグナルの名前とパスには、合わせて最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
   - [データ型] - シグナルのデータ型は、INT8、UINT8、INT16、UINT16、INT32、UINT32、INT64、UINT64、BOOLEAN、FLOAT、DO のいずれかである必要があります。
   - [シグナルタイプ] - シグナルのタイプ。[センサー] または [アクチュエータ]. を指定できます。
   - (オプション) [単位] - シグナルの科学単位 (km、摂氏など)。
   - (オプション) [パス] - シグナルのパス。JSONPath と同様に、子シグナルを参照するにはドット (.) を使用します。例えば、**`Vehicle.Engine.Light`**。

     シグナルの名前とパスには、合わせて最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。
   - (オプション) [最小値] - シグナルの最小値。
   - (オプション) [最大値] - シグナルの最大値。
   - (オプション) [説明] - シグナルの説明。

     説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。
4. [次へ] を選択します。

(オプション) ステップ 4: 属性を追加する

シグナルカタログには、既存の属性と合わせて最大 100 個の属性を追加できます。

属性を追加するには

1. [属性を追加] で、属性ごとに以下のメタデータを指定します。

   - [名前] - 属性の名前。

     シグナル名は一意である必要があります。シグナルの名前とパスには、合わせて最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。

   - [データ型] - 属性のデータ型は、INT8、UINT8、INT16、UINT16、INT32、UINT32、INT64、UINT64、BOOLEAN、FLOAT、DO のいずれかである必要があります。

   - (オプション) [単位] - 属性の科学単位 (km、摂氏など)。

   - (オプション) [パス] - シグナルのパス。JSONPath と同様に、子シグナルを参照するにはドット (.) を使用します。例えば、**`Vehicle.Engine.Light`**。

     シグナルの名前とパスには、合わせて最大 150 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア) です。

   - (オプション) [最小値] - 属性の最小値。

   - (オプション) [最大値] - 属性の最大値。

   - (オプション) [説明] - 属性の説明。

     説明には最大 2048 文字を入力できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、: (コロン)、_ (アンダースコア)、- (ハイフン) です。

2. [次へ] を選択します。

ステップ 5: 確認して作成する

車両モデルの構成を確認し、[作成] を選択します。

車両モデルの複製

AWS IoT FleetWise は、既存の車両モデルの設定をコピーして新しいモデルを作成できます。選択した車両モデルで指定されているシグナルが、新しい車両モデルにコピーされます。

車両モデルを複製するには

1. AWS IoT FleetWise コンソールを開きます。

2. ナビゲーションペインで、[車両モデル] を選択します。
3. 車両モデルの一覧からモデルを選択し、[モデルの複製] を選択します。

車両モデルを構成するには、「車両モデルの手動作成」チュートリアルに従います。

AWS IoT FleetWise が車両モデルの作成リクエストを処理するまでに数分かかる場合があります。車両モデルが正常に作成されると、[車両モデル] ページの [ステータス] 列に [ACTIVE] と表示されます。車両モデルがアクティブになると、編集することはできなくなります。

車両モデルの作成 (AWS CLI)

CreateModelManifest API オペレーションを使用すると、車両モデル (モデルマニフェスト) を作成できます。次の例では AWS CLIを使用しています。

> **Important**
>
> `CreateModelManifest` API オペレーションを使用して車両モデルを作成する前に、シグナルカタログが必要です。シグナルカタログの作成方法の詳細については、「AWS IoT FleetWise シグナルカタログを作成する」を参照してください。

車両モデルを作成するには、次のコマンドを実行します。

`vehicle-model-configuration` を、設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-model-manifest --cli-input-json file:///vehicle-model-configuration.json
```

- *`vehicle-model-name`* は、作成する車両モデルの名前に置き換えます。
- *`signal-catalog-ARN`* は、シグナルカタログの Amazon リソースネーム (ARN) に置き換えます。
- (オプション) *`description`* は、車両モデルの識別に役立つ説明に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「AWS IoT FleetWise シグナルを設定する」を参照してください。

```
{
```

```
    "name": "vehicle-model-name",
    "signalCatalogArn": "signal-catalog-ARN",
    "description": "description",
    "nodes": ["Vehicle.Chassis"]
}
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateModelManifest` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise 車両モデルを更新する

UpdateModelManifest API オペレーションを使用すると、既存の車両モデル (モデルマニフェスト) を更新できます。次の例では AWS CLIを使用しています。

既存の車両モデルを更新するには、次のコマンドを実行します。

update-vehicle-model-configuration を、設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise update-model-manifest --cli-input-json file://update-vehicle-model-configuration.json
```

- *vehicle-model-name* は、更新する車両モデルの名前に置き換えます。

- (オプション) 車両モデルをアクティブ化するには、*vehicle-model-status* を ACTIVE に置き換えます。

> **Important**
>
> 車両モデルがアクティブになると、その車両モデルは変更できなくなります。

- (オプション) *description* は、車両モデルの識別に役立つ、更新された説明に置き換えます。

```
{
    "name": "vehicle-model-name",
    "status": "vehicle-model-status",
    "description": "description",
    "nodesToAdd": ["Vehicle.Front.Left"],
    "nodesToRemove": ["Vehicle.Chassis.SteeringWheel"],
}
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが UpdateModelManifest API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

車両モデルの更新を確認する

ListModelManifestNodes API オペレーションを使用して、車両モデルが更新されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

特定の車両モデルに含まれているすべてのシグナル (ノード) の概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

vehicle-model-name は、確認する車両モデルの名前に置き換えます。

```
aws iotfleetwise list-model-manifest-nodes /
                 --name vehicle-model-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListModelManifestNodes` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise 車両モデルを削除する

AWS IoT FleetWise コンソールまたは API を使用して、車両モデルを削除できます。

> **Important**
>
> まず、車両モデルに関連付けられている車両とデコーダーマニフェストを削除する必要があります。詳細については、「AWS IoT FleetWise 車両を削除する」および「AWS IoT FleetWise デコーダーマニフェストを削除する」を参照してください。

車両モデルの削除 (コンソール)

車両モデルを削除するには、 AWS IoT FleetWise コンソールを使用します。

車両モデルを削除するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. [車両モデル] ページで、ターゲットの車両モデルを選択します。
4. [削除] を選択します。
5. [**vehicle-model-name** を削除しますか?] で、削除する車両モデルの名前を入力し、[確認] を選択します。

車両モデルの削除 (AWS CLI)

DeleteModelManifest API オペレーションを使用すると、既存の車両モデル (モデルマニフェスト) を削除できます。次の例では AWS CLIを使用しています。

車両モデルを削除するには、次のコマンドを実行します。

model-manifest-name は、削除する車両モデルの名前に置き換えます。

```
aws iotfleetwise delete-model-manifest --name model-manifest-name
```

車両モデルの削除を確認する

ListModelManifests API オペレーションを使用して、車両モデルが削除されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

すべての車両モデルの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-model-manifests
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListModelManifests` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
{
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Get AWS IoT FleetWise 車両モデル情報

GetModelManifest API オペレーションを使用して、車両モデルに関する情報を取得できます。次の例では、 を使用します AWS CLI。

車両モデルに関する情報を取得するには、次のコマンドを実行します。

`vehicle-model` は、取得する車両モデルの名前に置き換えます。

```
aws iotfleetwise get-model-manifest --name vehicle-model
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、車両モデルへの変更はすぐには反映されない場合があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `GetModelManifest` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Manage AWS IoT FleetWise デコーダーマニフェスト

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

デコーダーマニフェストには、 AWS IoT FleetWise が車両データ (バイナリデータ) を人間が読める値に変換し、データ分析のためにデータを準備するために使用するデコード情報が含まれています。ネットワークインターフェイスとシグナルデコーダーは、デコーダーマニフェストの設定に使用するコアコンポーネントです。

ネットワークインターフェイス

車載ネットワークが使用するプロトコルに関する情報が含まれます。 AWS IoT FleetWise は、次のプロトコルをサポートしています。

コントローラーエリアネットワーク (CAN バス)

電子制御ユニット (ECU) 間でのデータの通信方法を定義するプロトコル。ECU には、エンジンコントロールユニット、エアバッグ、オーディオシステムなどがあります。

オンボードダイアグノーシス (OBD) II

ECU 間の自己診断データの通信方法を定義する、より進化したプロトコル。車両の問題を特定するために役立つ標準の故障診断コード (DTC) が多数定義されています。

車両ミドルウェア

車両ミドルウェアは、ネットワークインターフェイスの一種として定義します。車両ミドルウェアの例としては、ロボットオペレーティングシステム (ROS 2) や Scalable service-Oriented MiddlewarE over IP (SOME/IP) が挙げられます。

> **Note**
>
> AWS IoT FleetWise は、ビジョンシステムデータ用の ROS 2 ミドルウェアをサポートしています。

カスタムインターフェイス

独自のインターフェイスを使用して Edge でシグナルをデコードすることもできます。これにより、クラウドでデコードルールを作成する必要がないため、時間を節約できます。

シグナルデコーダー

特定のシグナルについて詳細なデコード情報を提供します。車両モデルで指定されたすべてのシグナルは、シグナルデコーダーとペアリングする必要があります。デコーダーマニフェストに CAN ネットワークインターフェイスが含まれている場合は、CAN デコーダーシグナルも含まれている必要があります。デコーダーマニフェストに OBD ネットワークインターフェイスが含まれている場合は、OBD シグナルデコーダーが含まれている必要があります。

デコーダーマニフェストには、車両ミドルウェアインターフェイスも含まれている場合、メッセージシグナルデコーダーが含まれている必要があります。または、デコーダーマニフェストにカスタムデコードインターフェイスが含まれている場合は、カスタムデコードシグナルも含める必要があります。

各デコーダーマニフェストは車両モデルに関連付ける必要があります。 AWS IoT FleetWise は、関連付けられたデコーダーマニフェストを使用して、車両モデルに基づいて作成された車両からデータをデコードします。

各デコーダーマニフェストには、デコーダーマニフェストの状態を含むステータスフィールドがあります。ステータスは以下のいずれかの値になります。

- `ACTIVE` - デコーダーマニフェストはアクティブです。
- `DRAFT` - デコーダーマニフェストの構成は保存されていません。
- `VALIDATING` — デコーダーマニフェストの適格性が検証中です。これは、少なくとも 1 つのビジョンシステムデータシグナルを含むデコーダーマニフェストにのみ適用されます。
- `INVALID` — デコーダーマニフェストが検証に失敗したため、まだアクティブ化できません。これは、少なくとも 1 つのビジョンシステムデータシグナルを含むデコーダーマニフェストにのみ適用されます。ListDecoderManifests および GetDecoderManifest API を使用して、検証が失敗した原因を確認できます。

> **Important**
>
> - AWS IoT FleetWise コンソールを使用してデコーダーマニフェストを作成すると、 AWS IoT FleetWise は自動的にデコーダーマニフェストをアクティブ化します。
> - `CreateDecoderManifest` API オペレーションを使用してデコーダーマニフェストを作成する場合は、デコーダーマニフェストは `DRAFT` 状態のままになります。
> - `DRAFT` のデコーダーマニフェストに関連付けられている車両モデルから車両を作成することはできません。デコーダーマニフェストを `ACTIVE` 状態に変更するには、`UpdateDecoderManifest` API オペレーションを使用します。
> - `ACTIVE` 状態のデコーダーマニフェストは編集できません。

トピック

- Configure AWS IoT FleetWise ネットワークインターフェイスとデコーダーシグナル
- AWS IoT FleetWise デコーダーマニフェストを作成する
- AWS IoT FleetWise デコーダーマニフェストを更新する
- AWS IoT FleetWise デコーダーマニフェストを削除する
- Get AWS IoT FleetWise デコーダーマニフェスト情報

Configure AWS IoT FleetWise ネットワークインターフェイスとデコーダーシグナル

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

すべてのデコーダーマニフェストには、少なくともネットワークインターフェイスとシグナルデコーダーが、関連する車両モデルで指定されたシグナルとペアになっています。

デコーダーマニフェストに CAN ネットワークインターフェイスが含まれている場合は、CAN シグナルデコーダーが含まれている必要があります。デコーダーマニフェストに OBD ネットワークインターフェイスが含まれている場合は、OBD シグナルデコーダーが含まれている必要があります。

トピック

- ネットワークインターフェイスの構成
- シグナルデコーダーを設定する

ネットワークインターフェイスの構成

CAN ネットワークインターフェイスを構成するには、以下の情報を指定します。

- `name` - CAN インターフェイスの名前。

  インターフェイス名は一意でなければならず、1 ~ 100 文字を使用できます。
- (オプション) `protocolName` - プロトコルの名前。

  有効な値: `CAN-FD` および `CAN`
- (オプション) `protocolVersion` – AWS IoT FleetWise は現在、CAN-FD と CAN 2.0b をサポートしています。

  有効な値: `1.0` および `2.0b`

OBD ネットワークインターフェイスを構成するには、以下の情報を指定します。

- `name` - OBD インターフェイスの名前。

インターフェイス名は一意でなければならず、1 ~ 100 文字を使用できます。

- `requestMessageId` - 車両データをリクエストするメッセージの ID。
- (オプション) `dtcRequestIntervalSeconds` - 車両に故障診断コード (DTC) をリクエストする頻度 (秒単位)。例えば、指定した値が 120 の場合、エッジエージェントソフトウェアは保存された DTC を 2 分に 1 回収集します。
- (オプション) `hasTransmissionEcu` - 車両にトランスミッションコントロールモジュール (TCM) が搭載されているかどうか。

  有効な値: `true` および `false`
- （オプション) `obdStandard` – AWS IoT FleetWise がサポートする OBD 標準。 AWS IoT FleetWise は現在、World Wide Harmonization On-Board Diagnostics (WWH-OBD) ISO15765-4 標準をサポートしています。
- (オプション) `pidRequestIntervalSeconds` - 車両に OBD II PID をリクエストする頻度。例えば、指定した値が 120 の場合、エッジエージェントソフトウェアは OBD II PID を 2 分に 1 回収集します。
- (オプション) `useExtendedIds` - メッセージに拡張 ID を使用するかどうか。

  有効な値: `true` および `false`

車両ミドルウェアネットワークインターフェイスを設定するには、以下の情報を指定します。

- `name` — 車両ミドルウェアインターフェイスの名前。

  インターフェイス名は一意でなければならず、1 ~ 100 文字を使用できます。
- `protocolName` — プロトコル名。

  有効な値: `ROS_2`

カスタムデコードインターフェイスを設定するには、次の情報を指定します。

- `name` – Edge でシグナルをデコードするために使用するデコーダーの名前。

  デコーダーインターフェイス名は 1 ~ 100 文字です。

シグナルデコーダーを設定する

CAN シグナルデコーダーを設定するには、次の情報を指定します。

- `factor` - メッセージのデコードに使用される乗数。
- `isBigEndian` - メッセージのバイト順がビッグエンディアンかどうか。ビッグエンディアンの場合、シーケンス内の最上位の値が最初 (最も低いストレージアドレス) に格納されます。
- `isSigned` - メッセージが符号付きかどうか。符号付きの場合、メッセージは正の数値と負数の両方を表すことができます。
- `length` - メッセージの長さ (バイト単位)。
- `messageId` - メッセージの ID。
- `offset` - シグナル値の計算に使用されるオフセット。factor と組み合わせて、計算は `value = raw_value * factor + offset` となります。
- `startBit` - メッセージの先頭ビットの位置を示します。
- (オプション) `name` - シグナルの名前。
- (オプション) `signalValueType` – シグナルの値タイプ。整数はデフォルト値タイプです。

OBD シグナルデコーダーを設定するには、次の情報を指定します。

- `byteLength` - メッセージの長さ (バイト単位)。
- `offset` - シグナル値の計算に使用されるオフセット。scaling と組み合わせて、計算は `value = raw_value * scaling + offset` となります。
- `pid` - このシグナルについて車両にメッセージをリクエストする際に使用する診断コード。
- `pidResponseLength` - リクエストされたメッセージの長さ。
- `scaling` - メッセージのデコードに使用される乗数。
- `serviceMode` - メッセージ内のオペレーション (診断サービス) のモード。
- `startByte` - メッセージの先頭を示します。
- (オプション) `bitMaskLength` - メッセージ内のマスクされたビット数。
- (オプション) `bitRightShift` - 右にシフトされた位置の数。
- (オプション) `isSigned` – メッセージが署名されているかどうか。符号付きの場合、メッセージは正の数値と負数の両方を表すことができます。メッセージはデフォルトでは署名されません (`false`) 。

- （オプション）`signalValueType` – シグナルの値タイプ。整数はデフォルト値タイプです。

メッセージシグナルデコーダーを設定するには、次の情報を指定します。

- `topicName` — メッセージシグナルのトピック名。この名前は、ROS 2 のトピックに対応しています。構造化メッセージオブジェクトの詳細については、「StructuredMessage」を参照してください。
- `structuredMessage` — メッセージシグナルの構造化メッセージ。primitiveMessageDefinition、structuredMessageListDefinition、または structuredMessageDefinition のいずれかで再帰的に定義できます。

カスタムデコードシグナルを設定するには、次の情報を指定します。

- （オプション）`id` – デコーダーインターフェイスを使用してデコードするシグナルの ID。シグナル ID は 1 ~ 150 文字です。指定しない場合、 `id` はデフォルトでシグナル`fullyQualifiedName`の になります。

AWS IoT FleetWise デコーダーマニフェストを作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise コンソールまたは API を使用して、車両モデルのデコーダーマニフェストを作成できます。

トピック

- デコーダーマニフェストの作成 (コンソール)
- デコーダーマニフェストの作成 (AWS CLI)

デコーダーマニフェストの作成 (コンソール)

AWS IoT FleetWise コンソールを使用して、車両モデルに関連付けられたデコーダーマニフェストを作成できます。

> **Important**
>
> AWS IoT FleetWise コンソールを使用してデコーダーマニフェストでビジョンシステムデータシグナルを設定することはできません。代わりに、 AWS CLIを使用してください。ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

デコーダーマニフェストを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. ターゲットの車両モデルを選択します。
4. 車両モデルの概要ページで、[デコーダーマニフェストを作成] を選択し、次の操作を行います。

トピック

- ステップ 1: デコーダーマニフェストを構成する
- ステップ 2: CAN インターフェイスをマッピングする
- ステップ 3: 確認して作成する

ステップ 1: デコーダーマニフェストを構成する

[一般的な情報] セクションで、次の操作を行います。

1. デコーダーマニフェストの一意の名前を入力します。
2. (オプション) 説明を入力します。
3. [次へ] を選択します。

ネットワークインターフェイスを追加する

各デコーダーマニフェストには、少なくとも 1 つのネットワークインターフェイスが必要です。複数のネットワークインターフェイスをデコーダーマニフェストに追加できます。

ネットワークインターフェイスを作成するには

1. ネットワークインターフェイスファイルをアップロードします。CAN プロトコル用の .dbc ファイル、ROS 2 用の .json ファイル、またはカスタムインターフェイスをアップロードできます。

2. ネットワークインターフェイスの名前を入力します。カスタムインターフェイスをアップロードした場合、名前は既に指定されています。

欠落しているシグナルをマッピングする

アップロードされたネットワークインターフェイスでペアになったシグナルデコーダーが欠落しているシグナルが車両モデルにある場合は、欠落しているシグナルをマッピングするデフォルトのカスタムデコーダーを作成できます。次のステップでシグナルを手動でマッピングできるため、これはオプションです。

デフォルトのカスタムデコーダーを作成するには

1. 欠落しているシグナルのデフォルトのカスタムデコーダーを作成するを選択します。
2. [次へ] を選択します。

ステップ 2: CAN インターフェイスをマッピングする

CAN シグナルデコーダーを使用して CAN シグナルをマッピングできます。欠落シグナルのデフォルトのカスタムデコーダーの作成チェックボックスを選択した場合、デコーダーシグナルが欠落しているシグナルはすべて、デフォルトのカスタムシグナルデコーダーに自動的にマッピングされます。

CAN シグナルをマッピングするには

1. CAN シグナルマッピングで、シグナルデコーダーを選択します。
2. [次へ] を選択します。

> **Note**
>
> ROS 2 またはカスタムインターフェイスを追加した場合は、デコーダーマニフェストを作成する前にマッピングを確認できます。

ステップ 3: 確認して作成する

デコーダーマニフェストの構成を確認し、[作成] を選択します。

デコーダーマニフェストの作成 (AWS CLI)

CreateDecoderManifest API オペレーションを使用すると、デコーダーマニフェストを作成できます。次の例では AWS CLIを使用しています。

> **Important**
>
> デコーダーマニフェストを作成する前に車両モデルが必要です。すべてのデコーダーマニフェストは、車両モデルに関連付ける必要があります。詳細については、「AWS IoT FleetWise 車両モデルを作成する」を参照してください。

デコーダーマニフェストを作成するには、次のコマンドを実行します。

decoder-manifest-configuration を、設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-decoder-manifest --cli-input-json file://decoder-manifest-configuration.json
```

- *decoder-manifest-name* は、作成するデコーダーマニフェストの名前に置き換えます。
- *vehicle-model-ARN* は、車両モデルの Amazon リソースネーム (ARN) に置き換えます。
- (オプション) *description* は、デコーダーマニフェストの識別に役立つ説明に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「Configure AWS IoT FleetWise ネットワークインターフェイスとデコーダーシグナル」を参照してください。

```
{
    "name": "decoder-manifest-name",
    "modelManifestArn": "vehicle-model-arn",
    "description": "description",
    "networkInterfaces": [
        {
            "canInterface": {
                "name": "myNetworkInterface",
                "protocolName": "CAN",
                "protocolVersion": "2.0b"
            },
            "interfaceId": "Qq1acaenByOB3sSM39SYm",
```

```
            "type": "CAN_INTERFACE"
        }
    ],
    "signalDecoders": [
        {
            "canSignal": {
                "name": "Engine_Idle_Time",
                "factor": 1,
                "isBigEndian": true,
                "isSigned": false,
                "length": 24,
                "messageId": 271343712,
                "offset": 0,
                "startBit": 16
            },
            "fullyQualifiedName": "Vehicle.EngineIdleTime",
            "interfaceId": "Qq1acaenByOB3sSM39SYm",
            "type": "CAN_SIGNAL"
        },
        {
            "canSignal": {
                "name": "Engine_Run_Time",
                "factor": 1,
                "isBigEndian": true,
                "isSigned": false,
                "length": 24,
                "messageId": 271343712,
                "offset": 0,
                "startBit": 40
            },
            "fullyQualifiedName": "Vehicle.EngineRunTime",
            "interfaceId": "Qq1acaenByOB3sSM39SYm",
            "type": "CAN_SIGNAL"
        }
    ]
}
```

- *decoder-manifest-name* は、作成するデコーダーマニフェストの名前に置き換えます。
- *vehicle-model-ARN* は、車両モデルの Amazon リソースネーム (ARN) に置き換えます。
- (オプション) *description* は、デコーダーマニフェストの識別に役立つ説明に置き換えます。

構造 (構造体) 内のプロパティノードの順序は、シグナルカタログと車両モデル (モデルマニフェスト) で定義されている順序と一致している必要があります。ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「Configure AWS IoT FleetWise ネットワークインターフェイスとデコーダーシグナル」を参照してください。

```
{
 "name": "decoder-manifest-name",
 "modelManifestArn": "vehicle-model-arn",
 "description": "description",
 "networkInterfaces": [{
  "canInterface": {
   "name": "myNetworkInterface",
   "protocolName": "CAN",
   "protocolVersion": "2.0b"
  },
  "interfaceId": "Qq1acaenByOB3sSM39SYm",
  "type": "CAN_INTERFACE"
 }, {
  "type": "VEHICLE_MIDDLEWARE",
  "interfaceId": "G1KzxkdnmV5Hn7wkV3ZL9",
  "vehicleMiddleware": {
   "name": "ROS2_test",
   "protocolName": "ROS_2"
  }
 }],
 "signalDecoders": [{
   "canSignal": {
    "name": "Engine_Idle_Time",
    "factor": 1,
    "isBigEndian": true,
    "isSigned": false,
    "length": 24,
    "messageId": 271343712,
    "offset": 0,
    "startBit": 16
   },
   "fullyQualifiedName": "Vehicle.EngineIdleTime",
   "interfaceId": "Qq1acaenByOB3sSM39SYm",
   "type": "CAN_SIGNAL"
  },
  {
   "canSignal": {
    "name": "Engine_Run_Time",
```

```
    "factor": 1,
    "isBigEndian": true,
    "isSigned": false,
    "length": 24,
    "messageId": 271343712,
    "offset": 0,
    "startBit": 40
   },
   "fullyQualifiedName": "Vehicle.EngineRunTime",
   "interfaceId": "Qq1acaenByOB3sSM39SYm",
   "type": "CAN_SIGNAL"
  },
  {
   "fullyQualifiedName": "Vehicle.CompressedImageTopic",
   "type": "MESSAGE_SIGNAL",
   "interfaceId": "G1KzxkdnmV5Hn7wkV3ZL9",
   "messageSignal": {
    "topicName": "CompressedImageTopic:sensor_msgs/msg/CompressedImage",
    "structuredMessage": {
     "structuredMessageDefinition": [{
       "fieldName": "header",
       "dataType": {
        "structuredMessageDefinition": [{
          "fieldName": "stamp",
          "dataType": {
           "structuredMessageDefinition": [{
             "fieldName": "sec",
             "dataType": {
              "primitiveMessageDefinition": {
               "ros2PrimitiveMessageDefinition": {
                "primitiveType": "INT32"
               }
              }
             }
           },
           {
             "fieldName": "nanosec",
             "dataType": {
              "primitiveMessageDefinition": {
               "ros2PrimitiveMessageDefinition": {
                "primitiveType": "UINT32"
               }
              }
             }
```

```
            }
           ]
          }
         },
         {
          "fieldName": "frame_id",
          "dataType": {
           "primitiveMessageDefinition": {
            "ros2PrimitiveMessageDefinition": {
             "primitiveType": "STRING"
            }
           }
          }
         }
        ]
       }
      },
      {
       "fieldName": "format",
       "dataType": {
        "primitiveMessageDefinition": {
         "ros2PrimitiveMessageDefinition": {
          "primitiveType": "STRING"
         }
        }
       }
      },
      {
       "fieldName": "data",
       "dataType": {
        "structuredMessageListDefinition": {
         "name": "listType",
         "memberType": {
          "primitiveMessageDefinition": {
           "ros2PrimitiveMessageDefinition": {
            "primitiveType": "UINT8"
           }
          }
         },
         "capacity": 0,
         "listType": "DYNAMIC_UNBOUNDED_CAPACITY"
        }
       }
      }
```

```
      ]
     }
    }
   }
  ]
}
```

- *decoder-manifest-name* は、作成するデコーダーマニフェストの名前に置き換えます。
- *vehicle-model-ARN* は、車両モデルの Amazon リソースネーム (ARN) に置き換えます。
- (オプション) *description* は、デコーダーマニフェストの識別に役立つ説明に置き換えます。

ブランチ、属性、センサー、アクチュエータの構成方法の詳細については、「Configure AWS IoT FleetWise ネットワークインターフェイスとデコーダーシグナル」を参照してください。

```
{
 "name": "decoder-manifest-name",
 "modelManifestArn": "vehicle-model-arn",
 "description": "description",
 "networkInterfaces": [
        {
      "interfaceId": "myCustomInterfaceId",
      "type": "CUSTOM_DECODING_INTERFACE",
            "customDecodingInterface": {
                "name": "myCustomInterface"
            }
        }
    ],
    "signalDecoders": [
        {
            "customDecodingSignal": {
                "fullyQualifiedName": "Vehicle.actuator1",
                "interfaceId": "myCustomInterfaceId",
                "type": "CUSTOM_DECODING_SIGNAL",
                "customDecodingSignal": {
                    "id": "Vehicle.actuator1"
                }
            }
        },
        {
            "customDecodingSignal": {
                "fullyQualifiedName": "Vehicle.actuator2",
```

```
                "interfaceId": "myCustomInterfaceId",
                "type": "CUSTOM_DECODING_SIGNAL",
                "customDecodingSignal": {
                    "id": "Vehicle.actuator2"
                }
            }
        }
    ]
}
```

> **Note**
>
> デモスクリプトをダウンロードして、ビジョンシステムシグナルを含むデコーダーマニフェストを作成できます。詳細については、「ビジョンシステムデータデベロッパーガイド」を参照してください。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateDecoderManifest` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise デコーダーマニフェストを更新する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

UpdateDecoderManifest API オペレーションを使用すると、デコーダーマニフェストを更新できます。ネットワークインターフェイスとシグナルデコーダーの追加、削除、更新が可能です。デコーダーマニフェストのステータスを変更することもできます。次の例では AWS CLIを使用しています。

デコーダーマニフェストを更新するには、次のコマンドを実行します。

decoder-manifest-name は、更新するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise update-decoder-manifest /
                --name decoder-manifest-name /
                --status ACTIVE
```

シグナルに指定されたデコードルールがない場合は、デフォルトのデコードルールを作成できます。シグナルはカスタムデコードされたインターフェイスに追加され、 はシグナルの完全修飾名にCustomDecodingSignal$id設定されます。デフォルトのデコードルールでデコーダーマニフェストを更新するには、次のコマンドを実行します。

decoder-manifest-name は、更新するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise update-decoder-manifest /
                --name decoder-manifest-name /
                --status ACTIVE
                --default-for-unmapped-signals CUSTOM_DECODING
```

> **Important**
>
> デコーダーマニフェストをアクティブ化すると、編集することはできなくなります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが UpdateDecoderManifest API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

デコーダーマニフェストの更新を確認する

ListDecoderManifestSignals API オペレーションを使用して、デコーダーマニフェストのデコーダーシグナルが更新されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

特定のデコーダーマニフェストに含まれているすべてのデコーダーシグナル (ノード) の概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

decoder-manifest-name は、確認するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise list-decoder-manifest-signals /
                 --name decoder-manifest-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが ListDecoderManifestSignals API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

```
  "Statement": [

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

ListDecoderManifestNetworkInterfaces API オペレーションを使用して、デコーダーマニフェストのネットワークインターフェイスが更新されたかどうかを確認できます。次の例では AWS CLIを使用しています。

特定のデコーダーマニフェストに含まれているすべてのネットワークインターフェイスの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

decoder-manifest-name は、確認するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise list-decoder-manifest-network-interfaces /
                 --name decoder-manifest-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが ListDecoderManifestNetworkInterfaces API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
```

```
    },
  ]
}
```

AWS IoT FleetWise デコーダーマニフェストを削除する

AWS IoT FleetWise コンソールまたは API を使用して、デコーダーマニフェストを削除できます。

> **Important**
>
> まず、デコーダーマニフェストに関連付けられている車両を削除する必要があります。詳細については、「AWS IoT FleetWise 車両を削除する」を参照してください。

トピック

- デコーダーマニフェストの削除 (コンソール)
- デコーダーマニフェストの削除 (AWS CLI)

デコーダーマニフェストの削除 (コンソール)

AWS IoT FleetWise コンソールを使用して、デコーダーマニフェストを削除できます。

デコーダーマニフェストを削除するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両モデル] を選択します。
3. ターゲットの車両モデルを選択します。
4. 車両モデルの概要ページで、[デコーダーマニフェスト] タブを選択します。
5. ターゲットのデコーダーマニフェストを選択し、[削除] を選択します。
6. [**`decoder-manifest-name`** を削除しますか?] で、削除するデコーダーマニフェストの名前を入力し、[確認]. を選択します。

デコーダーマニフェストの削除 (AWS CLI)

DeleteDecoderManifest API オペレーションを使用すると、デコーダーマニフェストを削除できます。次の例では、 を使用します AWS CLI。

> **Important**
> デコーダーマニフェストを削除する前に、まず関連付けられている車両を削除してください。詳細については、「AWS IoT FleetWise 車両を削除する」を参照してください。

デコーダーマニフェストを削除するには、次のコマンドを実行します。

decoder-manifest-name は、削除するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise delete-decoder-manifest --name decoder-manifest-name
```

デコーダーマニフェストの削除を検証する

ListDecoderManifests API オペレーションを使用すると、デコーダーマニフェストが削除されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

すべてのデコーダーマニフェストの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-decoder-manifests
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListDecoderManifests` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
```

```
}
```

Get AWS IoT FleetWise デコーダーマニフェスト情報

GetDecoderManifest API オペレーションを使用して、デコーダーマニフェストのネットワークインターフェイスとシグナルデコーダーが更新されたかどうかを確認できます。次の例では、 を使用します AWS CLI。

デコーダーマニフェストに関する情報を取得するには、次のコマンドを実行します。

decoder-manifest は、取得するデコーダーマニフェストの名前に置き換えます。

```
aws iotfleetwise get-decoder-manifest --name decoder-manifest
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、デコーダーマニフェストへの変更はすぐには反映されない場合があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `GetDecoderManifest` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Manage AWS IoT FleetWise 車両

車両とは、車両モデルのインスタンスです。車両は車両モデルから作成し、デコーダーマニフェストに関連付ける必要があります。車両は 1 つ以上のデータストリームをクラウドにアップロードします。例えば、車両は走行距離、エンジン温度、ヒーターの状態に関するデータをクラウドに送信できます。すべての車両には、以下の情報が含まれています。

`vehicleName`

車両を識別する ID。

車両名には、個人を特定できる情報 (PII) や、その他の機密情報または重要情報を追加しないでください。車両名は、Amazon CloudWatch を含む他の AWS のサービスからアクセスできます。車両名でプライベートデータや機密データを使用することは想定されていません。

`modelManifestARN`

車両モデル (モデルマニフェスト) の Amazon リソースネーム (ARN)。すべての車両は車両モデルから作成されます。同じ車両モデルから作成された車両は、その車両モデルから継承された同じシグナルのグループで構成されます。これらのシグナルはシグナルカタログで定義され、標準化されます。

`decoderManifestArn`

デコーダーマニフェストの ARN。デコーダーマニフェストは、 AWS IoT FleetWise が raw シグナルデータ (バイナリデータ) を人間が読み取れる値に変換するために使用できるデコード情報を提供します。デコーダーマニフェストは車両モデルに関連付ける必要があります。 AWS IoT FleetWise は同じデコーダーマニフェストを使用して、同じ車両モデルに基づいて作成された車両から raw データをデコードします。

`attributes`

属性は、静的な情報を含むキーと値のペアです。車両には、車両モデルから継承された属性を含めることができます。同じ車両モデルから作成された他の車両と区別するために、個々の車両に追加の属性を設定することもできます。例えば、黒い車があるとすると、属性として `{"color": "black"}` という値を指定できます。

> **Important**
>
> 個々の車両に属性を追加できるようにするには、関連付けられている車両モデルで、それらの属性を事前に定義する必要があります。

車両モデル、デコーダーマニフェスト、属性の詳細については、「Model AWS IoT FleetWise 車両」を参照してください。

AWS IoT FleetWise には、車両の作成と管理に使用できる以下の API オペレーションが用意されています。

- CreateVehicle - 新しい車両を作成します。
- BatchCreateVehicle - 1 台以上の新しい車両を作成します。
- UpdateVehicle - 既存の車両を更新します。
- BatchUpdateVehicle - 1 台以上の既存の車両を更新します。
- DeleteVehicle - 既存の車両を削除します。
- ListVehicles - すべての車両の概要をページ分割されたリストとして取得します。
- GetVehicle - 車両に関する情報を取得します。

チュートリアル

- Provision AWS IoT FleetWise 車両
- AWS IoT FleetWise の予約済みトピック
- AWS IoT FleetWise 車両を作成する
- 複数の AWS IoT FleetWise 車両を作成する
- AWS IoT FleetWise 車両を更新する
- multiple AWS IoT FleetWise 車両を更新する
- AWS IoT FleetWise 車両を削除する
- Get AWS IoT FleetWise 車両情報

Provision AWS IoT FleetWise 車両

車両で実行されている Edge Agent for AWS IoT FleetWise ソフトウェアはデータを収集し、クラウドに転送します。 AWS IoT FleetWise は と統合 AWS IoT Core され、MQTT を介したエッジエージェントソフトウェアとクラウド間の安全な通信をサポートします。各車両は AWS IoT モノに対応しています。既存の AWS IoT モノを使用して車両を作成するか、Set AWS IoT FleetWise を使用して車両用の AWS IoT モノを自動的に作成できます。詳細については、「AWS IoT FleetWise 車両を作成する」を参照してください。

AWS IoT Core は、 AWS IoT FleetWise リソースへのアクセスを安全に制御するのに役立つ認証と認可をサポートしています。車両は X.509 証明書を使用して認証 (サインイン) され、 AWS IoT FleetWise と AWS IoT Core ポリシーを使用して、指定されたアクションを実行する権限 (アクセス許可を持つ) を取得できます。

車両の認証

車両を認証する AWS IoT Core ポリシーを作成できます。

車両を認証するには

- AWS IoT Core ポリシーを作成するには、次のコマンドを実行します。
  - *policy-name* は、作成するポリシーの名前に置き換えます。
  - *file-name* を、 AWS IoT Core ポリシーを含む JSON ファイルの名前に置き換えます。

```
aws iot create-policy --policy-name policy-name --policy-document file://file-name.json
```

ポリシーの例を使用する前に、次の作業を行ってください。

- *region* を、 AWS IoT FleetWise リソースを作成した AWS リージョンに置き換えます。
- *awsAccount* を自分の AWS アカウント ID に置き換えます。

この例では、 AWS IoT FleetWise によって予約されたトピックが含まれています。これらのトピックをポリシーに追加する必要があります。詳細については、「AWS IoT FleetWise の予約済みトピック」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:Connect"
            ],
            "Resource": [
```

```
                "arn:aws:iot:region:awsAccount:client/
${iot:Connection.Thing.ThingName}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Publish"
            ],
            "Resource": [
                "arn:aws:iot:region:awsAccount:topic/$aws/iotfleetwise/vehicles/
${iot:Connection.Thing.ThingName}/checkins",
                "arn:aws:iot:region:awsAccount:topic/$aws/iotfleetwise/vehicles/
${iot:Connection.Thing.ThingName}/signals"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Subscribe"
            ],
            "Resource": [
                "arn:aws:iot:region:awsAccount:topicfilter/$aws/iotfleetwise/
vehicles/${iot:Connection.Thing.ThingName}/collection_schemes",
                "arn:aws:iot:region:awsAccount:topicfilter/$aws/iotfleetwise/
vehicles/${iot:Connection.Thing.ThingName}/decoder_manifests"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iot:Receive"
            ],
            "Resource": [
                "arn:aws:iot:region:awsAccount:topic/$aws/iotfleetwise/vehicles/
${iot:Connection.Thing.ThingName}/collection_schemes",
                "arn:aws:iot:region:awsAccount:topic/$aws/iotfleetwise/vehicles/
${iot:Connection.Thing.ThingName}/decoder_manifests"
            ]
        }
    ]
}
```

車両の認可

車両を認可する X.509 証明書を作成できます。

車両を認可するには

> **Important**
>
> 車両ごとに新しい証明書を作成することをお勧めします。

1. RSA キーペアを作成して X.509 証明書を発行するには、次のコマンドを実行します。
   - *cert* は、コマンドから出力される certificatePem の内容を保存するファイルの名前に置き換えます。
   - *public-key* は、コマンドから出力される keyPair.PublicKey の内容を保存するファイルの名前に置き換えます。
   - *private-key* は、コマンドから出力される keyPair.PrivateKey の内容を保存するファイルの名前に置き換えます。

```
aws iot create-keys-and-certificate \
    --set-as-active \
    --certificate-pem-outfile cert.pem \
    --public-key-outfile public-key.key" \
    --private-key-outfile  private-key.key"
```

2. 出力から、証明書の Amazon リソースネーム (ARN) をコピーします。
3. 証明書にポリシーをアタッチするには、次のコマンドを実行します。
   - *policy-name* を、作成した AWS IoT Core ポリシーの名前に置き換えます。
   - *certificate-arn* は、コピーした証明書の ARN に置き換えます。

```
aws iot attach-policy \
    --policy-name policy-name\
    --target "certificate-arn"
```

4. 証明書をモノにアタッチするには、次のコマンドを実行します。

- *thing-name* を AWS IoT モノの名前または車両の ID に置き換えます。
- *certificate-arn* は、コピーした証明書の ARN に置き換えます。

```
aws iot attach-thing-principal \
    --thing-name thing-name \
    --principal "certificate-arn"
```

AWS IoT FleetWise の予約済みトピック

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise は、以下のトピックの使用を予約します。予約済みトピックで許可されている場合は、そのトピックにサブスクライブまたは発行することができます。ただし、ドル記号 ($) で始まる新しいトピックを作成することはできません。予約済みトピックでサポートされていない発行オペレーションやサブスクライブオペレーションを使用すると、接続が終了することがあります。

トピック	許可されているクライアントオペレーション	説明	
`$aws/iotfleetwise/vehicles/`*vehicleName*`/checkins`	公開	エッジエージェントソフトウェアは、このトピックに車両のステータス情報を発行します。 車両ステータス情報はプロトコルバッファ (Protobuf) 形式で交換されます。詳細については、「Edge	

トピック	許可されているクライアントオペレーション	説明	
		Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイド」を参照してください。	
$aws/iotfleetwise/vehicles/*vehicleName*/signals	公開	エッジエージェントソフトウェアは、このトピックにシグナルを発行します。 シグナル情報はプロトコルバッファ (Protobuf) 形式で交換されます。詳細については、「Edge Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイド」を参照してください。	
$aws/iotfleetwise/vehicles/*vehicleName*/collection_schemes	Subscribe	AWS IoT FleetWise はこのトピックにデータ収集スキームを発行します。車両はこれらのデータ収集スキームを使用します。	

トピック	許可されているクライアントオペレーション	説明	
`$aws/iotfleetwise/vehicles/vehicleName/decoder_manifests`	Subscribe	AWS IoT FleetWise はこのトピックにデコーダーマニフェストを発行します。車両はこれらのデコーダーマニフェストを使用します。	
`$aws/iotfleetwise/vehicles/vehicleName/command/request`	Subscribe	AWS IoT FleetWise は、このトピックにコマンドを実行するリクエストを発行します。その後、車両はこれらのコマンドリクエストを使用します。	
`$aws/iotfleetwise/vehicles/vehicleName/command/response`	公開	Edge Agent ソフトウェアは、車両からのコマンドレスポンスをこのトピックに発行します。 コマンドレスポンスはプロトコルバッファ (Protobuf) 形式で交換されます。詳細については、「Edge Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイド」を参照してください。	

トピック	許可されているクライアントオペレーション	説明
`$aws/iotfleetwise/vehicles/vehicleName/command/notification`	Subscribe	AWS IoT FleetWise はこのトピックにコマンドステータスの更新を発行します。通知は JSON 形式で送信されます。
`$aws/iotfleetwise/vehicles/$vehicle_name/last_known_states/config`	Subscribe	AWS IoT FleetWise はこのトピックに状態テンプレート設定を発行します。車両はこれらの状態テンプレート設定を使用します。
`$aws/iotfleetwise/vehicles/$vehicle_name/last_known_states/data`	公開	Edge Agent ソフトウェアは、シグナルから収集されたデータをこのトピックに発行します。

トピック	許可されているクライアントオペレーション	説明	
`$aws/iotfleetwise/vehicles/`*`$vehicle_name`*`/last_known_state/`*`$state_template_name`*`/data`	Subscribe	AWS IoT FleetWise は、このトピックに指定された で設定されたシグナルから収集されたデータを発行*`$state_template_name`* します。更新は部分的な場合があります。たとえば、状態テンプレートの関連付けに、変更時の更新戦略を含む複数のシグナルが含まれている場合、変更されたシグナルのみが特定のメッセージに含まれます。 シグナル情報はプロトコルバッファ (Protobuf) 形式で交換されます。詳細については、「Edge Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイド」を参照してください。	

AWS IoT FleetWise 車両を作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise コンソールまたは API を使用して車両を作成できます。

> **Important**
>
> 開始する前に、次の点を確認してください。
>
> - 車両モデルが用意されていて、その車両モデルのステータスが `ACTIVE` になっている必要があります。詳細については、「Manage AWS IoT FleetWise 車両モデル」を参照してください。
> - 車両モデルがデコーダーマニフェストに関連付けられていて、そのデコーダーマニフェストのステータスが `ACTIVE` になっている必要があります。詳細については、「Manage AWS IoT FleetWise デコーダーマニフェスト」を参照してください。

トピック

- 車両の作成 (コンソール)
- 車両の作成 (AWS CLI)

車両の作成 (コンソール)

AWS IoT FleetWise コンソールを使用して車両を作成できます。

車両を作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両] を選択します。
3. 車両の概要ページで、[車両を作成] を選択し、以下の手順を実行します。

トピック

- ステップ 1: 車両のプロパティを定義する
- ステップ 2: 車両証明書を構成する
- ステップ 3: 証明書にポリシーをアタッチする
- ステップ 4: 確認して作成する

ステップ 1: 車両のプロパティを定義する

このステップでは、車両に名前を付け、モデルマニフェストとデコーダーマニフェストに関連付けます。

1. 車両の一意の名前を入力します。

> **Important**
>
> 車両は AWS IoT モノに対応します。同じ名前のモノが既に存在する場合は、[車両を IoT モノに関連付ける] を選択すると、その車両でモノが更新されます。または、別の車両名を選択すると、 AWS IoT FleetWise は自動的に車両の新しいモノを作成します。

2. リストから車両モデル (モデルマニフェスト) を選択します。
3. リストからデコーダーマニフェストを選択します。デコーダーマニフェストが車両モデルに関連付けられます。
4. (オプション) 車両の属性を関連付けるには、[属性を追加] を選択します。このステップを省略した場合、車両をキャンペーンにデプロイできるようにするには、車両の作成後に属性を追加する必要があります。
5. (オプション) 車両にタグを関連付けるには、[新しいタグを追加] を選択します。車両の作成後にタグを追加することもできます。
6. [次へ] を選択します。

ステップ 2: 車両証明書を構成する

車両を AWS IoT モノとして使用するには、ポリシーがアタッチされた車両証明書を設定する必要があります。このステップを省略した場合、車両をキャンペーンにデプロイできるようにするには、車両の作成後に証明書を構成する必要があります。

1. [新しい証明書の自動生成 (推奨)] を選択します。
2. [次へ] を選択します。

ステップ 3: 証明書にポリシーをアタッチする

前のステップで構成した証明書にポリシーをアタッチします。

1. [ポリシー] に、既存のポリシー名を入力します。新しいポリシーを作成するには、[ポリシーを作成] を選択します。
2. [次へ] を選択します。

ステップ 4: 確認して作成する

車両の構成を確認し、[車両を作成] を選択します。

> **Important**
>
> 車両が作成されたら、証明書とキーをダウンロードする必要があります。証明書とプライベートキーを使用して、 Edge Agent for AWS IoT FleetWise ソフトウェアで車両を接続します。

車両の作成 (AWS CLI)

車両を作成するときは、デコーダーマニフェストに関連付けられた車両モデルを使用する必要があります。CreateVehicle API オペレーションを使用すると、車両を作成できます。次の例では AWS CLI を使用しています。

車両を作成するには、次のコマンドを実行します。

file-name を、車両設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-vehicle --cli-input-json file://file-name.json
```

Example — 車両設定

- (オプション) `associationBehavior` の値には次のいずれかを指定できます。
  - `CreateIotThing` – 車両が作成されると、 AWS IoT FleetWise は車両の車両 ID の名前を持つ AWS IoT モノを自動的に作成します。
  - `ValidateIotThingExists` - 既存の AWS IoT モノを使用して車両を作成します。

AWS IoT モノを作成するには、次のコマンドを実行します。*thing-name* は、作成するモノの名前に置き換えます。

```
aws iot create-thing --thing-name thing-name
```

指定しない場合、 AWS IoT FleetWise は車両の AWS IoT モノを自動的に作成します。

> **Important**
> 車両の作成後に AWS IoT モノがプロビジョニングされていることを確認します。詳細については、「Provision AWS IoT FleetWise 車両」を参照してください。

- *vehicle-name* は、次のいずれかに置き換えます。
  - `associationBehavior` が に設定されている場合の AWS IoT モノの名前`ValidateIotThingExists`。
  - `associationBehavior` が `CreateIotThing` に設定されている場合は、作成する車両の ID。

    車両 ID は 1 ~ 100 文字で指定できます。有効な文字は、a ~ z、A ~ Z、0 ~ 9、ダッシュ (-)、アンダースコア (_)、コロン (:) です。
- *model-manifest-ARN* は、車両モデル (モデルマニフェスト) の ARN に置き換えます。
- *decoder-manifest-ARN* は、指定した車両モデルに関連付けられているデコーダーマニフェストの ARN に置き換えます。
- (オプション) 同じ車両モデルから作成された他の車両と区別するために、この車両に追加の属性を設定できます。例えば、電気自動車があるとすると、属性として `{"fuelType": "electric"}` という値を指定できます。

> **Important**
> 個々の車両に属性を追加できるようにするには、関連付けられている車両モデルで、それらの属性を事前に定義する必要があります。

```
{
    "associationBehavior": "associationBehavior",
    "vehicleName": "vehicle-name",
    "modelManifestArn": "model-manifest-ARN",
```

```
    "decoderManifestArn": "decoder-manifest-ARN",
    "attributes": {
        "key": "value"
    }
}
```

Example — 状態テンプレートを車両に関連付ける

状態テンプレートを車両に関連付けると、 stateTemplatesフィールドを使用して、クラウド内の車両から状態更新を収集できます。

この例では、 は次のいずれか*stateTemplateUpdateStrategy*になります。

- periodic: では、エッジエージェントソフトウェアがシグナル更新をクラウドに送信する固定レートを指定できます (エッジエージェントソフトウェアは、シグナル値が更新間で変更されていない場合でも更新を送信します) 。
- onChange: Edge Agent ソフトウェアは、シグナルが変更されるたびにシグナルの更新を送信します。

```
aws iotfleetwise create-vehicle --cli-input-json file://create-vehicle.json
```

create-vehicle.json ファイルに含まれる場所 (例 :

```
{
    "associationBehavior": "associationBehavior",
    "vehicleName": "vehicle-name",
    "modelManifestArn": "model-manifest-ARN",
    "decoderManifestArn": "decoder-manifest-ARN",
    "attributes": {
        "key": "value"
    },
    "stateTemplates": [
        {
            "identifier": "state-template-name",
            "stateTemplateUpdateStrategy": {
                "periodic": {
                    "stateTemplateUpdateRate": {
                        "unit": "SECOND",
                        "value": 10
                    }
                }
```

```
            }
        }
    ]
}
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateVehicle` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
{
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

複数の AWS IoT FleetWise 車両を作成する

BatchCreateVehicle API オペレーションを使用すると、複数の車両を一度に作成できます。次の例では AWS CLIを使用しています。

複数の車両を作成するには、次のコマンドを実行します。

file-name を、複数の車両の設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise batch-create-vehicle --cli-input-json file://file-name.json
```

Example — 車両設定

```
{
    "vehicles": [
        {
```

```
                "associationBehavior": "associationBehavior",
                "vehicleName": "vehicle-name",
                "modelManifestArn": "model-manifest-ARN",
                "decoderManifestArn": "decoder-manifest-ARN",
                "attributes": {
                    "key": "value"
                }
        },
        {
                "associationBehavior": "associationBehavior",
                "vehicleName": "vehicle-name",
                "modelManifestArn": "model-manifest-ARN",
                "decoderManifestArn": "decoder-manifest-ARN",
                "attributes": {
                    "key": "value"
                }
        }
    ]
}
```

1 回のバッチオペレーションで最大 10 台の車両を作成できます。車両の構成の詳細については、「AWS IoT FleetWise 車両を作成する」を参照してください。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `BatchCreateVehicle` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise 車両を更新する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

UpdateVehicle API オペレーションを使用すると、既存の車両を更新できます。次の例では AWS CLIを使用しています。

車両を更新するには、次のコマンドを実行します。

file-name を、車両の設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise update-vehicle --cli-input-json file://file-name.json
```

Example — 車両設定

- *vehicle-name* は、更新する車両の ID に置き換えます。
- (オプション) *model-manifest-ARN* は、使用中の車両モデルに代えて使用する車両モデル (モデルマニフェスト) の ARN に置き換えます。
- (オプション) *decoder-manifest-ARN* は、指定した新しい車両モデルに関連付けられているデコーダーマニフェストの ARN に置き換えます。
- (オプション) *attribute-update-mode* は、車両の属性に置き換えます。
  - `Merge` - 新しい属性を既存の属性にマージします。既存の属性は新しい値で更新され、存在しない属性は新しく追加されます。

    例えば、車両に `{"color": "black", "fuelType": "electric"}` という属性が設定されている場合、この車両を `{"color": "", "fuelType": "gasoline", "model": "x"}` という属性で更新すると、更新後の車両の属性は `{"fuelType": "gasoline", "model": "x"}` になります。
  - `Overwrite` - 既存の属性を新しい属性に置き換えます。

    例えば、車両に `{"color": "black", "fuelType": "electric"}` という属性が設定されている場合、この車両を `{"model": "x"}` という属性で更新すると、更新後の車両の属性は `{"model": "x"}` になります。

入力に属性が含まれている場合は必須です。

- (オプション) 新しい属性を追加したり、既存の属性を新しい値で更新したりするには、`attributes` を構成します。例えば、電気自動車があるとすると、属性として `{"fuelType": "electric"}` という値を指定できます。

  属性を削除するには、`attributeUpdateMode` を `Merge` に設定します。

> **Important**
>
> 個々の車両に属性を追加できるようにするには、関連付けられている車両モデルで、それらの属性を事前に定義する必要があります。

```
 {
         "vehicleName": "vehicle-name",
         "modelManifestArn": "model-manifest-arn",
         "decoderManifestArn": "decoder-manifest-arn",
         "attributeUpdateMode": "attribute-update-mode"
         }
}
```

Example — 車両に関連付けられた状態テンプレートを追加または削除します。

次のフィールドを使用して、追加の状態テンプレートを関連付けたり、車両から既存の関連付けを削除したりできます。

- `stateTemplatesToAdd`
- `stateTemplatesToRemove`

```
aws iotfleetwise update-vehicle --cli-input-json file://update-vehicle.json
```

update-vehicle.json ファイルに含まれる場所 (例:)

```
{
    "vehicleName": "vehicle-name",
    "modelManifestArn": "model-manifest-arn",
    "decoderManifestArn": "decoder-manifest-arn",
    "attributeUpdateMode": "attribute-update-mode",
```

```
    "stateTemplatesToAdd": [
        {
            "identifier": "state-template-name",
            "stateTemplateUpdateStrategy": {
                "onChange": {}
            }
        }
    ],
    "stateTemplatesToRemove": ["state-template-name"]
}
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `UpdateVehicle` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

multiple AWS IoT FleetWise 車両を更新する

BatchUpdateVehicle API オペレーションを使用すると、複数の既存の車両を一度に更新できます。次の例では AWS CLIを使用しています。

複数の車両を更新するには、次のコマンドを実行します。

file-name を、複数の車両の設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise batch-update-vehicle --cli-input-json file://file-name.json
```

Example — 車両設定

```
{
   "vehicles": [
      {
         "vehicleName": "vehicle-name",
         "modelManifestArn": "model-manifest-arn",
         "decoderManifestArn": "decoder-manifest-arn",
         "mergeAttributes": true,
         "attributes": {
         "key": "value"
         }
      },
      {
         "vehicleName": "vehicle-name",
         "modelManifestArn": "model-manifest-arn",
         "decoderManifestArn": "decoder-manifest-arn",
         "mergeAttributes": true,
         "attributes": {
         "key": "value"
         }
      }
   ]
}
```

1 回のバッチオペレーションで最大 10 台の車両を更新できます。各車両の構成の詳細については、「AWS IoT FleetWise 車両を更新する」を参照してください。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `BatchUpdateVehicle` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
```

```
        ]
      },
    ]
}
```

AWS IoT FleetWise 車両を削除する

AWS IoT FleetWise コンソールまたは API を使用して車両を削除できます。

> **Important**
>
> 車両が削除されると、 AWS IoT FleetWise は関連するフリートとキャンペーンから車両を自動的に削除します。詳細については、「AWS IoT FleetWise でフリートを管理する」および「キャンペーンを使用して AWS IoT FleetWise データを収集する」を参照してください。ただし、車両は引き続きモノとして存在するか、 内のモノに関連付けられています AWS IoT Core。モノを削除する手順については、「AWS IoT Core デベロッパーガイド」の「モノの削除」を参照してください。

車両の削除 (コンソール)

AWS IoT FleetWise コンソールを使用して車両を削除できます。

車両を削除するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両] を選択します。
3. [車両] ページで、削除する車両の横にあるボタンを選択します。
4. [削除] を選択します。
5. [削除]**vehicle-name** で、車両の名前を入力し、[削除] を選択します。

車両の削除 (AWS CLI)

DeleteVehicle API オペレーションを使用すると、車両を削除できます。次の例では、 を使用します AWS CLI。

車両を削除するには、次のコマンドを実行します。

vehicle-name は、削除する車両の ID に置き換えます。

```
aws iotfleetwise delete-vehicle --vehicle-name vehicle-name
```

車両の削除を確認する

ListVehicles API オペレーションを使用して、車両が削除されたかどうかを確認できます。次の例では AWS CLIを使用しています。

すべての車両の概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-vehicles
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListVehicles` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Get AWS IoT FleetWise 車両情報

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

GetVehicle API オペレーションを使用すると、車両情報を取得できます。次の例では AWS CLIを使用しています。

車両のメタデータを取得するには、次のコマンドを実行します。

vehicle-name は、取得する車両の ID に置き換えます。

```
aws iotfleetwise get-vehicle --vehicle-name vehicle-name
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、車両への変更はすぐには反映されない場合があります。

GetVehicleStatus API オペレーションを使用して、車両に関連付けられたリソースのステータスを取得できます。次の例では AWS CLIを使用しています。

車両に関連付けられたリソースのステータスを取得するには、次のコマンドを実行します。

- *vehicle-name* を、リソースが関連付けられている車両の ID に置き換えます。
- *type* は、ステータスを取得するリソースのタイプに置き換えます。type の有効値は、CAMPAIGN、STATE_TEMPLATE、および DECODER です。

```
aws iotfleetwise get-vehicle-status --vehicle-name vehicle-name --type type
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが GetVehicleまたは GetVehicleStatus API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
```

```
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise でフリートを管理する

フリートは、車両のグループを表します。車両が関連付けられていないフリートは空のエンティティです。フリートを使用して複数の車両を同時に管理するには、事前に車両をフリートに関連付ける必要があります。車両は複数のフリートに所属することができます。キャンペーンをデプロイすると、車両のフリートから収集するデータと、データを収集するタイミングを制御できます。詳細については、「キャンペーンを使用して AWS IoT FleetWise データを収集する」を参照してください。

フリートには、以下の情報が含まれています。

`fleetId`

フリートの ID。

(オプション) `description`

フリートを見つけるために役立つ説明。

`signalCatalogArn`

シグナルカタログの Amazon リソースネーム (ARN)。

AWS IoT FleetWise には、フリートの作成と管理に使用できる以下の API オペレーションが用意されています。

- CreateFleet - 同じシグナルのグループを含む車両のグループを作成します。
- AssociateVehicleFleet - 車両をフリートに関連付けます。
- DisassociateVehicleFleet - 車両とフリートの関連付けを解除します。
- UpdateFleet - 既存のフリートの説明を更新します。
- DeleteFleet - 既存のフリートを削除します。
- ListFleets - すべてのフリートの概要をページ分割されたリストとして取得します。
- ListFleetsForVehicle - 車両が所属しているすべてのフリートの ID をページ分割されたリストとして取得します。
- ListVehiclesInFleet - フリート内のすべての車両の概要をページ分割されたリストとして取得します。
- GetFleet - フリートに関する情報を取得します。

トピック

- AWS IoT FleetWise フリートを作成する
- AWS IoT FleetWise 車両をフリートに関連付ける
- AWS IoT FleetWise 車両とフリートの関連付けを解除する
- AWS IoT FleetWise フリートを更新する
- AWS IoT FleetWise フリートを削除する
- Get AWS IoT FleetWise フリート情報

AWS IoT FleetWise フリートを作成する

CreateFleet API オペレーションを使用すると、フリートを作成できます。次の例では、 を使用します AWS CLI。

> **Important**
>
> フリートを作成する前に、シグナルカタログを用意する必要があります。詳細については、「AWS IoT FleetWise シグナルカタログを作成する」を参照してください。

フリートを作成するには、次のコマンドを実行します。

- *fleet-id* は、作成するフリートの ID に置き換えます。

  フリート ID は一意でなければならず、1 ~ 100 文字にする必要があります。有効な文字は、英字 (A ~ Z と a ~ z)、数字 (0 ~ 9)、コロン (:)、ダッシュ (-)、アンダースコア (_) です。
- (オプション) *description* は、説明に置き換えます。

  説明は 1 ~ 2048 文字で入力できます。
- *signal-catalog-arn* は、シグナルカタログの ARN に置き換えます。

```
aws iotfleetwise create-fleet \
   --fleet-id fleet-id \
   --description description \
   --signal-catalog-arn signal-catalog-arn
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateFleet` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise 車両をフリートに関連付ける

AssociateVehicleFleet API オペレーションを使用すると、車両をフリートに関連付けることができます。次の例では、 を使用します AWS CLI。

> **Important**
>
> - 車両をフリートに関連付ける前に、車両とフリートを用意する必要があります。詳細については、「Manage AWS IoT FleetWise 車両」を参照してください。
> - キャンペーンのターゲットとなっているフリートに車両を関連付けると、 AWS IoT FleetWise によってキャンペーンが自動的に車両にデプロイされます。

車両をフリートに関連付けるには、次のコマンドを実行します。

- *`fleet-id`* は、フリートの ID に置き換えます。
- *`vehicle-name`* は、車両の ID に置き換えます。

```
aws iotfleetwise associate-vehicle-fleet --fleet-id fleet-id --vehicle-name vehicle-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが AssociateVehicleFleet API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise 車両とフリートの関連付けを解除する

DisassociateVehicleFleet API オペレーションを使用すると、車両とフリートの関連付けを解除できます。次の例では、 を使用します AWS CLI。

車両とフリートの関連付けを解除するには、次のコマンドを実行します。

- *fleet-id* は、フリートの ID に置き換えます。
- *vehicle-name* は、車両の ID に置き換えます。

```
aws iotfleetwise disassociate-vehicle-fleet --fleet-id fleet-id --vehicle-name vehicle-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが DisassociateVehicleFleet API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise フリートを更新する

UpdateFleet API オペレーションを使用すると、フリートの説明を更新できます。次の例では AWS CLIを使用しています。

フリートを更新するには、次のコマンドを実行します。

- *fleet-id* は、更新するフリートの ID に置き換えます。
- *description* は、新しい説明に置き換えます。

  説明は 1 ~ 2048 文字で入力できます。

```
aws iotfleetwise update-fleet --fleet-id fleet-id --description description
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが UpdateFleet API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

```
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise フリートを削除する

DeleteFleet API オペレーションを使用すると、フリートを削除できます。次の例では、 を使用します AWS CLI。

> **Important**
>
> フリートを削除する前に、関連付けられている車両がないことを確認してください。車両とフリートの関連付けを解除する方法については、「AWS IoT FleetWise 車両とフリートの関連付けを解除する」を参照してください。

フリートを削除するには、次のコマンドを実行します。

fleet-id は、削除するフリートの ID に置き換えます。

```
aws iotfleetwise delete-fleet --fleet-id fleet-id
```

フリートの削除を検証する

ListFleets API オペレーションを使用して、フリートが削除されたかどうかを確認できます。次の例では AWS CLIを使用しています。

すべてのフリートの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-fleets
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListFleets` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

Get AWS IoT FleetWise フリート情報

ListFleetsForVehicle API オペレーションを使用すると、車両が所属しているすべてのフリートの ID をページ分割されたリストとして取得できます。次の例では AWS CLIを使用しています。

車両が所属しているすべてのフリートの ID をページ分割されたリストとして取得するには、次のコマンドを実行します。

`vehicle-name` は、車両の ID に置き換えます。

```
aws iotfleetwise list-fleets-for-vehicle \
            --vehicle-name vehicle-name
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListFleetsForVehicle` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

```
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

ListVehiclesInFleet API オペレーションを使用すると、フリート内のすべての車両の概要をページ分割されたリストとして取得できます。次の例では AWS CLIを使用しています。

フリート内のすべての車両の概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

fleet-id は、フリートの ID に置き換えます。

```
aws iotfleetwise list-vehicles-in-fleet \
            --fleet-id fleet-id
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `ListVehiclesInFleet` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

GetFleet API オペレーションを使用すると、フリート情報を取得できます。次の例では AWS CLIを使用しています。

フリートのメタデータを取得するには、次のコマンドを実行します。

fleet-id は、フリートの ID に置き換えます。

```
aws iotfleetwise get-fleet \
            --fleet-id fleet-id
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、フリートへの変更はすぐには反映されない場合があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `GetFleet` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

キャンペーンを使用して AWS IoT FleetWise データを収集する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

キャンペーンとは、データ収集ルールのオーケストレーションです。キャンペーンは、エッジエージェント for AWS IoT FleetWise ソフトウェアに、データを選択、収集、クラウドに転送する方法に関する指示を与えます。

キャンペーンはクラウドで作成します。お客様またはお客様のチームがキャンペーンを承認すると、AWS IoT FleetWise はキャンペーンをデプロイする準備を整え、次の車両チェックインにデプロイします。キャンペーンを 1 台の車両にデプロイするか、車両のフリートにデプロイするかを選択できます。エッジエージェントソフトウェアは、実施中のキャンペーンが車両にデプロイされるまでデータの収集を開始しません。

> **Important**
>
> キャンペーンは、次の条件が満たされるまで機能しません。
>
> - エッジエージェントソフトウェアが車両内で実行されている。エッジエージェントソフトウェアを開発、インストール、使用する方法の詳細を確認するには、以下の操作を行います。
> 1. AWS IoT FleetWise コンソールを開きます。
> 2. サービスのホームページの「Get started with AWS IoT FleetWise」セクションで、「Explore Edge Agent」を選択します。
> - 車両をプロビジョニング AWS IoT Core するように をセットアップしました。詳細については、「Provision AWS IoT FleetWise 車両」を参照してください。

> **Note**
>
> また、「On Change」または「Periodic」更新戦略を使用してテレメトリデータをストリーミングできる状態テンプレートを使用して、ほぼリアルタイムで 車両の最終状態をモニタリングする (フリートではなく) することもできます。また、以前にデプロイされたテンプレートを有効または無効にしたり、現在の車両状態を 1 回リクエスト (フェッチ) したりする「オンデマンド」機能も提供します。
> 最後の既知の状態へのアクセスは、現在ゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

各キャンペーンには、以下の情報が含まれています。

`signalCatalogArn`

キャンペーンに関連付けられているシグナルカタログの Amazon リソースネーム (ARN)。

(オプション) `tags`

タグは、キャンペーンの管理に使用できるメタデータです。さまざまなサービスのリソースに同じタグを割り当てて、それらのリソースが関連していることを示すことができます。

`TargetArn`

キャンペーンのデプロイ先となる車両またはフリートの ARN。

`name`

キャンペーンを識別するために役立つ一意の名前。

`collectionScheme`

データ収集スキームは、収集するデータや収集するタイミングについて Edge Agent ソフトウェアに指示を与えます。 AWS IoT FleetWise は現在、条件ベースの収集スキームと時間ベースの収集スキームをサポートしています。

- `conditionBasedCollectionScheme` – 条件ベースのコレクションスキームは、論理式を使用して収集するデータを認識します。エッジエージェントソフトウェアは、条件が満たされたときにデータを収集します。
  - `expression` – 収集するデータを認識するために使用される論理式。例えば、`$variable.`myVehicle.InVehicleTemperature` > 50.0` という式を指定すると、エッジエージェントソフトウェアは 50.0 より大きい温度値を収集します。式の書き方の手順については、「AWS IoT FleetWise キャンペーンの論理式」を参照してください。

- (オプション) `conditionLanguageVersion` – 条件式言語のバージョン。
- (オプション) `minimumTriggerIntervalMs` – 2 つのデータ収集イベント間の最小時間をミリ秒単位で表します。シグナルが頻繁に変化する場合は、データの収集速度を遅くすることができます。
- (オプション) `triggerMode` – 次のいずれかの値を指定できます。
  - `RISING_EDGE` – Edge Agent ソフトウェアは、条件が初めて満たされた場合にのみデータを収集します。例えば、`$variable.`myVehicle.AirBagDeployed` == true`。
  - `ALWAYS` - エッジエージェントソフトウェアは、条件が満たされるたびにデータを収集します。

- `timeBasedCollectionScheme` – 時間ベースの収集スキームを定義する場合は、期間をミリ秒単位で指定します。エッジエージェントソフトウェアは、その時間間隔を使用してデータの収集頻度を決定します。例えば、時間間隔が 120,000 ミリ秒の場合、エッジエージェントソフトウェアはデータを 2 分ごとに 1 回収集します。
  - `periodMs` – データを収集する頻度を決定する期間 (ミリ秒単位) 。

(オプション) `compression`

ワイヤレス帯域幅を節約し、ネットワークトラフィックを減らすために、SNAPPY を指定して車両内のデータを圧縮できます。

デフォルト (`OFF`) では、エッジエージェントソフトウェアはデータを圧縮しません。

`dataDestinationConfigs`

キャンペーンが車両データを転送する 1 つの送信先を選択します。データを MQTT トピックに送信するか、Amazon S3 または Amazon Timestream に保存できます。

MQTT (Message Queuing Telemetry Transport) は、軽量で広く採用されているメッセージングプロトコルです。 AWS IoT ルールを使用して MQTT トピックにデータを発行し、独自のイベント駆動型アーキテクチャを立ち上げることができます。MQTT AWS IoT のサポートは、MQTT v3.1.1 仕様と MQTT v5.0 仕様に基づいていますが、いくつかの違いがあります。詳細については、「MQTT の違い」を参照してください。

S3 は、耐久性のあるデータ管理機能とダウンストリームデータサービスを提供する費用対効果の高いデータストレージメカニズムです。S3 は、運転動作や長期メンテナンスの分析に関連するデータに使用できます。

Timestream は、傾向やパターンをほぼリアルタイムで特定するために役立つデータ永続化メカニズムです。Timestream は、車両の速度やブレーキの履歴の傾向を分析する場合など、時系列データに使用できます。

> **Note**
>
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

(オプション) `dataExtraDimensions`

1 つ以上の属性を追加して、シグナルに追加情報を提供できます。

(オプション) `dataPartitions`

信号データを車両に一時的に保存するデータパーティションを作成します。データをクラウドに転送するタイミングと方法を設定します。

- 最大ストレージサイズ、最小有効期間、およびストレージの場所を定義して、 AWS IoT FleetWise が車両またはフリートにデータを保存する方法を指定します。
- キャンペーンは `spoolingMode`である必要があります`TO_DISK`。
- 設定のアップロードには、条件言語のバージョンと論理式の定義が含まれます。

(オプション) `description`

キャンペーンの目的を特定するのに役立つ説明を追加します。

(オプション) `diagnosticsMode`

診断モードを `SEND_ACTIVE_DTCS` に設定すると、キャンペーンは、保存された標準の故障診断コード (DTC) を送信するようになります。これは車両の問題を特定するために役立ちます。例えば、P0097 は、エンジンコントロールモジュール (ECM) によって、空気温度センサー 2 (IAT2) の入力が通常のセンサー範囲よりも低いと判断されたことを示します。

デフォルト (`OFF`) では、エッジエージェントソフトウェアは診断コードを送信しません。

(オプション) `expiryTime`

キャンペーンの有効期限を定義します。キャンペーンの有効期限が切れると、エッジエージェントソフトウェアはこのキャンペーンで指定されたデータの収集を停止します。車両に複数のキャ

ンペーンがデプロイされている場合、エッジエージェントソフトウェアは他のキャンペーンを使用してデータを収集します。

デフォルト値: `253402243200` (9999 年 12 月 31 日 00:00:00 UTC)

(オプション) `postTriggerCollectionDuration`

スキームが呼び出された後、エッジエージェントソフトウェアで一定期間データを収集し続けるように、トリガー後の収集期間を定義できます。例えば、`$variable.`myVehicle.Engine.RPM` > 7000.0` という式が指定された条件ベースの収集スキームが呼び出された場合に、エッジエージェントソフトウェアでエンジンの 1 分あたりの回転数 (RPM) 値を引き続き収集できます。RPM が一度 7000 を超えただけでも、機械的な問題を示している可能性があります。この場合、エッジエージェントソフトウェアでデータの収集を継続して状況をモニタリングできます。

デフォルト値: `0`

(オプション) `priority`

キャンペーンの優先度を示す整数を指定します。数値が小さいキャンペーンほど優先度が高くなります。1 つの車両に複数のキャンペーンをデプロイする場合、優先度の高いキャンペーンが最初に開始されます。

デフォルト値: `0`

(オプション) `signalsToCollect`

データ収集スキームが呼び出されたときにデータが収集されるシグナルのリスト。

- `name` – データ収集スキームが呼び出されたときにデータが収集されるシグナルの名前。
- `dataPartitionId` – シグナルで使用するデータパーティションの ID。ID は、 で指定された IDs のいずれかと一致する必要がありますdataPartitions。データパーティションの条件としてシグナルをアップロードする場合、それらの同じシグナルを に含める必要がありますsignalsToCollect。
- （オプション) `maxSampleCount` – データ収集スキームが呼び出されたときに Edge Agent ソフトウェアが収集してクラウドに転送するデータサンプルの最大数。
- （オプション) `minimumSamplingIntervalMs` — 2 つのデータサンプル収集イベント間の最小時間をミリ秒単位で表します。シグナルが頻繁に変化する場合は、このパラメータを使用してデータの収集速度を遅くすることができます。

  有効な範囲: 0 ~ 4294967295

(オプション) `spoolingMode`

`spoolingMode` が `TO_DISK` に設定されている場合、エッジエージェントソフトウェアは、車両がクラウドに接続されていないときにデータを一時的にローカルに保存します。接続が再確立されると、ローカルに保存されたデータが自動的にクラウドに転送されます。

デフォルト値: `OFF`

(オプション) `startTime`

承認されたキャンペーンは開始時刻に有効になります。

デフォルト値: `0`

キャンペーンのステータスは次のいずれかの値になります。

- `CREATING` – AWS IoT FleetWise はキャンペーンの作成リクエストを処理しています。
- `WAITING_FOR_APPROVAL` - 作成後のキャンペーンは `WAITING_FOR_APPROVAL` 状態になります。キャンペーンを承認するには、`UpdateCampaign` API オペレーションを使用します。キャンペーンが承認されると、 AWS IoT FleetWise によってキャンペーンが自動的にターゲットの車両またはフリートにデプロイされます。詳細については、「AWS IoT FleetWise キャンペーンを更新する」を参照してください。
- `RUNNING` - キャンペーンはアクティブです。
- `SUSPENDED` - キャンペーンは停止しています。キャンペーンを再開するには、`UpdateCampaign` API オペレーションを使用します。

AWS IoT FleetWise には、キャンペーンの作成と管理に使用できる以下の API オペレーションが用意されています。

- CreateCampaign - 新しいキャンペーンを作成します。
- UpdateCampaign - 既存のキャンペーンを更新します。キャンペーンを作成したら、この API オペレーションを使用してキャンペーンを承認する必要があります。
- DeleteCampaign - 既存のキャンペーンを削除します。
- ListCampaigns - すべてのキャンペーンの概要をページ分割されたリストとして取得します。
- GetCampaign - キャンペーンに関する情報を取得します。

チュートリアル

- AWS IoT FleetWise キャンペーンを作成する
- AWS IoT FleetWise キャンペーンを更新する
- AWS IoT FleetWise キャンペーンを削除する
- Get AWS IoT FleetWise キャンペーン情報
- キャンペーンデータの保存と転送
- AWS IoT FleetWise を使用して診断問題コードデータを収集する
- Visualize AWS IoT FleetWise 車両データ

AWS IoT FleetWise キャンペーンを作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise コンソールまたは API を使用して、車両データを収集するキャンペーンを作成できます。

> **Important**
>
> キャンペーンが機能するためには、次の条件が満たされている必要があります。
>
> - エッジエージェントソフトウェアが車両内で実行されている。エッジエージェントソフトウェアを開発、インストール、使用する方法の詳細を確認するには、以下の操作を行います。
> 1. AWS IoT FleetWise コンソールを開きます。
> 2. サービスのホームページの「Get started with AWS IoT FleetWise」セクションで、「Explore Edge Agent」を選択します。
> - 車両をプロビジョニング AWS IoT Core するように をセットアップしました。詳細については、「Provision AWS IoT FleetWise 車両」を参照してください。

トピック

- キャンペーンの作成 (コンソール)
- キャンペーンの作成 (AWS CLI)
- AWS IoT FleetWise キャンペーンの論理式

キャンペーンの作成 (コンソール)

AWS IoT FleetWise コンソールを使用して、車両データを選択、収集、クラウドに転送するキャンペーンを作成します。

キャンペーンを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[キャンペーン] を選択します。
3. [キャンペーン] ページで、[キャンペーンを作成] を選択し、以下のトピックの手順を完了します。

トピック

- ステップ 1: キャンペーンを構成する
- ステップ 2: ストレージとアップロード条件を指定する
- ステップ 3: データ送信先を設定する
- ステップ 4: 車両を追加する
- ステップ 5: 確認して作成する
- ステップ 6: キャンペーンをデプロイする

> **Important**
>
> - キャンペーンを作成する前に、シグナルカタログと車両を用意する必要があります。詳細については、「Manage AWS IoT FleetWise シグナルカタログ」および「Manage AWS IoT FleetWise 車両」を参照してください。
> - キャンペーンが作成されたら、そのキャンペーンを承認する必要があります。詳細については、「AWS IoT FleetWise キャンペーンを更新する」を参照してください。

ステップ 1: キャンペーンを構成する

[一般的な情報] セクションで、次の操作を行います。

1. キャンペーンの名前を入力します。
2. (オプション) 説明を入力します。

キャンペーンのデータ収集スキームを構成します。データ収集スキームは、どのようなデータをいつ収集するかに関する指示をエッジエージェントソフトウェアに与えます。 AWS IoT FleetWise コンソールでは、次の方法でデータ収集スキームを設定できます。

- データ収集スキームを手動で定義します。
- データ収集スキームを自動的に定義するためのファイルをアップロードします。

[設定オプション] で、次のいずれかを選択します。

- 手動でデータ収集スキームのタイプを指定し、オプションを定義してスキームをカスタマイズするには、[データ収集スキームを定義] を選択します。

  手動でデータ収集スキームのタイプを指定し、オプションを定義してスキームをカスタマイズします。

  1. [データ収集スキームの詳細] セクションで、このキャンペーンで使用するデータ収集スキームのタイプを選択します。収集する車両データを認識するために論理式を使用するには、[条件ベース] を選択します。特定の時間間隔を使用して車両データの収集頻度を決定するには、[時間ベース] を選択します。
  2. キャンペーンでデータを収集する期間を定義します。

     > **Note**
     >
     > デフォルトでは、承認されたキャンペーンはすぐにアクティブ化され、終了時間は設定されません。追加料金が発生しないようにするには、時間範囲を指定する必要があります。

  3. 条件ベースのデータ収集スキームを指定した場合は、収集するデータを認識する論理式を定義する必要があります。 AWS IoT FleetWise は論理式を使用して、条件ベースのスキーム用に収集するデータを認識します。この式では、シグナルの完全修飾名を表す変数、比較演算子、および比較値を指定する必要があります。

たとえば、`$variable.`myVehicle.InVehicleTemperature` > 50.0`式を指定すると、 AWS IoT FleetWise は 50.0 を超える温度値を収集します。式の書き方の手順については、「AWS IoT FleetWise キャンペーンの論理式」を参照してください。

収集するデータを認識するために使用される論理式を入力します。

4. (オプション) 条件式の言語バージョンを指定します。デフォルト値は 1 です。
5. (オプション) 最小トリガー間隔を指定します。これは、2 つのデータ収集イベント間の最小期間です。例えば、シグナルが頻繁に変化する場合は、データの収集速度を遅くすることができます。
6. エッジエージェントソフトウェアでデータを収集するための [トリガーモード] の条件を指定します。デフォルトでは、 Edge Agent for AWS IoT FleetWise ソフトウェアは、条件が満たされるたびに常にデータを収集します。または、[最初のトリガー時] を選択して、条件が初めて満たされたときにのみデータを収集することもできます。
7. 時間ベースのデータ収集スキームを指定した場合は、[期間] を 10,000 ~ 60,000 ミリ秒で指定する必要があります。エッジエージェントソフトウェアは、その時間間隔を使用してデータの収集頻度を決定します。
8. (オプション) スキームの高度なスキームオプションを編集します。
   a. データを圧縮することでワイヤレス帯域幅を節約し、ネットワークトラフィックを減らすには、SNAPPY を選択します。
   b. (オプション) データ収集イベントの後にデータを収集し続ける期間をミリ秒単位で定義するには、[トリガー後の収集期間] を指定します。
   c. (オプション) キャンペーンの優先度レベルを指定するには、キャンペーンの優先度を指定します。優先度の数値が小さいキャンペーンほど優先度が高いと見なされ、最初にデプロイされます。
   d. エッジエージェントソフトウェアは、車両がクラウドに接続されていないときにデータを一時的にローカルに保存できます。接続が再確立されると、ローカルに保存されたデータが自動的にクラウドに転送されます。[データのローカル保存] で、接続の切断時にエッジエージェントでデータをローカルに保存すかどうかを指定します。
   e. (オプション) シグナルの追加情報を提供するには、[追加のデータディメンション] として最大 5 個の属性を追加します。

- ファイルをアップロードしてデータ収集スキームを定義するには、ローカルデバイスから .json ファイルをアップロードを選択します。 AWS IoT FleetWise は、ファイルで定義できるオプションを自動的に定義します。選択されたオプションを確認して更新できます。

データ収集スキームに関する詳細が記述された .json ファイルをアップロードします。

1. データ収集スキームの情報をインポートするには、[ファイルを選択] を選択します。必要なファイル形式の詳細については、API ドキュメントの「CreateCampaign」を参照してください。

   > **Note**
   >
   > AWS IoT FleetWise は現在、.json ファイル形式の拡張子をサポートしています。

2. AWS IoT FleetWise は、ファイル内の情報に基づいてデータ収集スキームを自動的に定義します。 AWS IoT FleetWise が選択したオプションを確認します。必要に応じてオプションを更新できます。

ステップ 2: ストレージとアップロード条件を指定する

車両がクラウドに接続されていないときに Edge Agent ソフトウェアがデータを一時的にローカルに保存するかどうかを選択するには、スプーリングモードを指定します。

- データスプーリングモードで、次のいずれかを選択します。
  - 未保存 – エッジエージェントソフトウェアはデータを収集しますが、車両がオフラインのときに一時的にローカルに保存することはありません。エッジエージェントソフトウェアは、車両の再接続時にデータをクラウドに転送します。
  - ディスクに保存 – エッジエージェントソフトウェアは、車両がオフラインのときにデータを収集し、一時的にローカルに保存します。収集されたデータは、エッジエージェント設定ファイルの「永続性」セクションで定義された場所に一時的に保存されます。エッジエージェントは、車両の再接続時にデータをクラウドに転送します。
  - パーティションを含むディスクに格納 – 車両は常に指定されたデータパーティションの Edge に一時的にデータを保存します。保存したデータをクラウドに転送するタイミングを選択できます。
    1. (オプション) パーティション ID を入力して、特定のデータセットを指定します。
    2. データを保存する場所としてフォルダ名を入力します。ストレージの場所の絶対パスは です`{persistency_path} / {vehicle_name} / {campaign_name} / {storage_location}`。

3. パーティションに保存されているデータの最大ストレージサイズを入力します。パーティションが最大サイズに達すると、新しいデータは古いデータを上書きします。
4. このパーティション内のデータがディスクに保持される最小時間を入力します。
5. (オプション) パーティションのアップロード条件を入力します。

シグナルの指定

キャンペーン中に からデータを収集するシグナルを指定できます。

データを収集するシグナルを指定するには

1. シグナル名を選択します。
2. (オプション) 最大サンプル数には、キャンペーン中に Edge Agent ソフトウェアが収集してクラウドに転送するデータサンプルの最大数を入力します。
3. (オプション) [最小サンプリング間隔] に、2 つのデータサンプル収集イベント間の最小時間をミリ秒単位で入力します。シグナルが頻繁に変化する場合は、このパラメータを使用してデータの収集速度を遅くすることができます。
4. 別のシグナルを追加するには、[シグナルをさらに追加] を選択します。最大 999 個のシグナルを追加できます。
5. [次へ] を選択します。

ステップ 3: データ送信先を設定する

> **Note**
> キャンペーンにビジョンシステムデータシグナルが含まれている場合、車両データは Amazon S3 にのみ保存できます。Timestream に保存したり、MQTT トピックに送信したりすることはできません。
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

キャンペーンによって収集されたデータを送信または保存する送信先を選択します。車両データを MQTT トピックに送信するか、Amazon S3 または Amazon Timestream に保存できます。

[送信先の設定] で、次の操作を行います。

- ドロップダウンリストから Amazon S3、Amazon Timestream、または MQTT トピックを選択します。

Amazon S3

> **Important**
>
> AWS IoT FleetWise が S3 バケットに書き込むアクセス許可を持っている場合にのみ、S3 にデータを転送できます。アクセス許可の詳細については、AWS IoT FleetWise によるアクセスの制御」を参照してください。

車両データを S3 バケットに保存する場合は、[Amazon S3] を選択します。S3 は、データをオブジェクトとしてバケットに保存するオブジェクトストレージサービスです。詳細については、Amazon S3バケットの作成、設定、および操作」を参照してください。

S3 は、データストレージのコストを最適化し、データレイク、一元化されたデータストレージ、データ処理パイプライン、分析など、車両データを利用するための追加メカニズムを提供します。S3 を使用すると、データを保存してバッチ処理や分析を行うことができます。例えば、機械学習 (ML) モデル用に急ブレーキイベントのレポートを作成できます。受信した車両データは、配信前に 10 分間バッファリングされます。

[S3 destination settings] で、次の操作を行います。

1. [S3 bucket] で、 AWS IoT FleetWise にアクセス許可があるバケットを選択します。
2. (オプション) S3 バケットに保存されているデータを体系化するために使用できるカスタムプレフィックスを入力します。
3. 出力形式を選択します。これは、S3 バケットに保存されるファイルの形式です。
4. S3 バケットに保存されたデータを .gzip ファイルとして圧縮するかどうかを選択します。ストレージコストが最小限に抑えられるため、データを圧縮することをお勧めします。
5. [S3 送信先の設定] で選択したオプションに応じて、[S3 オブジェクト URI の例] が変更されます。これは、S3 に保存されるファイルの例を示すものです。

Amazon Timestream

> **Important**
>
> AWS IoT FleetWise に Timestream にデータを書き込むアクセス許可がある場合にのみ、テーブルにデータを転送できます。アクセス許可の詳細については、AWS IoT FleetWise によるアクセスの制御」を参照してください。
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

車両データを Timestream テーブルに保存するには、[Amazon Timestream] を選択します。Timestream を使用すると、車両データにクエリを実行して傾向やパターンを特定できます。例えば、Timestream を使用して車両の燃料レベルのアラームを作成できます。受信した車両データは、ほぼリアルタイムに Timestream に転送されます。詳細については、「Amazon Timestream デベロッパーガイド」の「Amazon Timestream とは」を参照してください。

[Timestream テーブルの設定] で、次の操作を行います。

1. [Timestream データベース名] で、ドロップダウンリストから Timestream データベースの名前を選択します。
2. [Timestream テーブル名] で、ドロップダウンリストから Timestream テーブルの名前を選択します。

[Timestream のサービスアクセス] で、次の操作を行います。

- ドロップダウンリストから IAM ロールを選択します。

MQTT トピック

> **Important**
>
> AWS IoT FleetWise がトピックへのアクセス許可を持っている場合にのみ、MQTT AWS IoT トピックにデータをルーティングできます。アクセス許可の詳細については、AWS IoT FleetWise によるアクセスの制御」を参照してください。

車両データを MQTT トピックに送信するには、MQTT トピックを選択します。

MQTT メッセージングによって送信される車両データはほぼリアルタイムで配信され、ルールを使用してアクションを実行したり、データを他の送信先にルーティングしたりできます。MQTT の使用の詳細については、「 AWS IoT Core デベロッパーガイド」の「 デバイス通信プロトコルと のルール AWS IoT」を参照してください。

1. MQTT トピックで、トピック名を入力します。
2. MQTT トピックのサービスアクセスで、 AWS IoT FleetWise に新しいサービスロールを作成して使用させるかどうかを選択します。既存のサービスロールを使用する場合は、「ロールの選択」のドロップダウンリストでロールを選択します。

- [次へ] を選択します。

ステップ 4: 車両を追加する

キャンペーンをデプロイする車両を選択するには、車両のリストで目的の車両を選択します。車両の作成時に追加した属性や値、または車両名で検索して、車両をフィルタリングします。

[車両をフィルタリング] で、次の操作を行います。

1. 検索ボックスで属性または車両名を検索し、リストから選択します。

> **Note**
> 各属性は 1 回だけ使用できます。

2. キャンペーンをデプロイする属性の値または車両名を入力します。例えば、属性の完全修飾名が `fuelType` の場合は、その値として `gasoline` を入力します。
3. 別の車両属性を検索するには、前のステップを繰り返します。車両属性は最大 5 つまで、車両名はいくつでも検索できます。
4. [車両名] に、検索条件に一致する車両のリストが表示されます。キャンペーンをデプロイする先の車両を選択します。

> **Note**
> 検索結果には最大 100 台の車両が表示されます。[すべて選択] を選択すると、すべての車両がキャンペーンに追加されます。

5. [次へ] を選択します。

ステップ 5: 確認して作成する

キャンペーンの構成を確認し、[キャンペーンを作成] を選択します。

> **Note**
> キャンペーンが作成されたら、ユーザーまたはユーザーのチームがキャンペーンを車両にデプロイする必要があります。

ステップ 6: キャンペーンをデプロイする

キャンペーンを作成したら、ユーザーまたはユーザーのチームがキャンペーンを車両にデプロイする必要があります。

キャンペーンをデプロイするには

1. [キャンペーンの概要] ページで、[デプロイ] を選択します。
2. デプロイを開始してキャンペーンに接続された車両からデータ収集を開始することを確認します。
3. [デプロイ] を選択します。

キャンペーンに接続されている車両からのデータ収集を一時停止する場合は、[キャンペーンの概要] ページで [停止] を選択します。キャンペーンに接続されている車両からのデータ収集を再開するには、[再開] を選択します。

キャンペーンの作成 (AWS CLI)

CreateCampaign API オペレーションを使用すると、キャンペーンを作成できます。次の例では AWS CLIを使用しています。

キャンペーンを作成すると、車両から収集されたデータを MQTT トピックに送信したり、Amazon S3 (S3) または Amazon Timestream に保存したりできます。ほぼリアルタイムの処理を必要とするデータを保存する場合など、高速でスケーラブルなサーバーレス時系列データベースが必要な場合は、Timestream を選択します。業界をリードするスケーラビリティ、データの可用性、セキュリ

ティ、パフォーマンスを備えたオブジェクトストレージに S3 を選択します。MQTT を選択すると、ほぼリアルタイムでデータを配信し、 ルール AWS IoTを使用して、定義したアクションを実行したり、他の送信先にルーティングしたりできます。

> **Important**
>
> 車両データを MQTT トピック、Amazon S3、または Amazon Timestream に転送できるのは、 AWS IoT FleetWise がユーザーに代わって MQTT メッセージを送信したり、S3 または Timestream にデータを書き込むアクセス許可を持っている場合のみです。アクセス許可の詳細については、AWS 「 IoT FleetWise によるアクセスの制御」を参照してください。Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

キャンペーンの作成

> **Important**
>
> - キャンペーンを作成する前に、シグナルカタログと車両またはフリートが必要です。詳細についてはManage AWS IoT FleetWise シグナルカタログ、Manage AWS IoT FleetWise 車両、およびAWS IoT FleetWise でフリートを管理するを参照してください。
> - キャンペーンが作成されたら、`UpdateCampaign` API オペレーションを使用してキャンペーンを承認する必要があります。詳細については、AWS IoT FleetWise キャンペーンを更新するを参照してください。

キャンペーンを作成するには、次のコマンドを実行します。

file-name を、キャンペーン設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-campaign --cli-input-json file://file-name.json
```

- *campaign-name* は、作成するキャンペーンの名前に置き換えます。
- *signal-catalog-arn* は、シグナルカタログの Amazon リソースネーム (ARN) に置き換えます。
- *target-arn* は、作成したフリートまたは車両の ARN に置き換えます。
- *bucket-arn* は、S3 バケットの ARN に置き換えます。

```
{
    "name": "campaign-name",
    "targetArn": "target-arn",
    "signalCatalogArn": "signal-catalog-arn",
    "collectionScheme": {
        "conditionBasedCollectionScheme": {
            "conditionLanguageVersion": 1,
            "expression": "$variable.`Vehicle.DemoBrakePedalPressure` > 7000",
            "minimumTriggerIntervalMs": 1000,
            "triggerMode": "ALWAYS"
        }
    },
    "compression": "SNAPPY",
    "diagnosticsMode": "OFF",
    "postTriggerCollectionDuration": 1000,
    "priority": 0,
    "signalsToCollect": [
        {
         "maxSampleCount": 100,
         "minimumSamplingIntervalMs": 0,
         "name": "Vehicle.DemoEngineTorque"
        },
        {
         "maxSampleCount": 100,
         "minimumSamplingIntervalMs": 0,
         "name": "Vehicle.DemoBrakePedalPressure"
        }
    ],
    "spoolingMode": "TO_DISK",
    "dataDestinationConfigs": [
        {
         "s3Config": {
             "bucketArn": "bucket-arn",
             "dataFormat": "PARQUET",
             "prefix": "campaign-name",
              "storageCompressionFormat": "GZIP"
      }
    }
  ],
     "dataPartitions": [
      { ...  }
  ]
}
```

> **Note**
>
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

- *campaign-name* は、作成するキャンペーンの名前に置き換えます。
- *signal-catalog-arn* は、シグナルカタログの ARN に置き換えます。
- *target-arn* は、作成したフリートまたは車両の ARN に置き換えます。
- *role-arn* を、Timestream テーブルにデータを配信するアクセス許可を AWS IoT FleetWise に付与するタスク実行ロールの ARN に置き換えます。
- *table-arn* は、Timestream テーブルの ARN に置き換えます。

```
{
  "name": "campaign-name",
  "targetArn": "target-arn",
  "signalCatalogArn": "signal-catalog-arn",
  "collectionScheme": {
    "conditionBasedCollectionScheme": {
      "conditionLanguageVersion": 1,
      "expression": "$variable.`Vehicle.DemoBrakePedalPressure` > 7000",
      "minimumTriggerIntervalMs": 1000,
      "triggerMode": "ALWAYS"
    }
  },
  "compression": "SNAPPY",
  "diagnosticsMode": "OFF",
  "postTriggerCollectionDuration": 1000,
  "priority": 0,
  "signalsToCollect": [
    {
      "maxSampleCount": 100,
      "minimumSamplingIntervalMs": 0,
      "name": "Vehicle.DemoEngineTorque"
    },
    {
      "maxSampleCount": 100,
      "minimumSamplingIntervalMs": 0,
      "name": "Vehicle.DemoBrakePedalPressure"
    }
```

```
  ],
  "spoolingMode": "TO_DISK",
  "dataDestinationConfigs": [
    {
      "timestreamConfig": {
        "executionRoleArn": "role-arn",
        "timestreamTableArn": "table-arn"
      }
    }
  ],
   "dataPartitions": [
      { ...  }
  ]
}
```

- *campaign-name* は、作成するキャンペーンの名前に置き換えます。
- *signal-catalog-arn* は、シグナルカタログの Amazon リソースネーム (ARN) に置き換えます。
- *target-arn* は、作成したフリートまたは車両の ARN に置き換えます。
- *topic-arn* を、車両データを含むメッセージの宛先として指定した MQTT トピックの ARN に置き換えます。
- *role-arn* を、指定した MQTT トピックのメッセージを送信、受信、およびアクションを実行するアクセス許可を AWS IoT FleetWise に付与するタスク実行ロールの ARN に置き換えます。

```
{
  "name": "campaign-name",
  "targetArn": "target-arn",
  "signalCatalogArn": "signal-catalog-arn",
  "collectionScheme": {
    "conditionBasedCollectionScheme": {
      "conditionLanguageVersion": 1,
      "expression": "$variable.`Vehicle.DemoBrakePedalPressure` > 7000",
      "minimumTriggerIntervalMs": 1000,
      "triggerMode": "ALWAYS"
    }
  },
  "compression": "SNAPPY",
  "diagnosticsMode": "OFF",
  "postTriggerCollectionDuration": 1000,
```

```
  "priority": 0,
  "signalsToCollect": [
    {
      "maxSampleCount": 100,
      "minimumSamplingIntervalMs": 0,
      "name": "Vehicle.DemoEngineTorque"
    },
    {
      "maxSampleCount": 100,
      "minimumSamplingIntervalMs": 0,
      "name": "Vehicle.DemoBrakePedalPressure"
    }
  ],
  "spoolingMode": "TO_DISK",
  "dataDestinationConfigs": [
      {
          "mqttTopicConfig": {
              "mqttTopicArn": "topic-arn",
              "executionRoleArn": "role-arn"
          }
      }
  ]
}
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `CreateCampaign` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
```

```
}
```

AWS IoT FleetWise キャンペーンの論理式

AWS IoT FleetWise は論理式を使用して、キャンペーンの一部として収集するデータを認識します。式の詳細については、「AWS IoT Events デベロッパーガイド」の「式」を参照してください。

式変数は、収集するデータの種類に関する規則に準拠するように構成する必要があります。テレメトリーシステムデータの場合、式変数はシグナルの完全修飾名でなければなりません。ビジョンシステムデータの場合、式はシグナルの完全修飾名と、シグナルのデータ型からそのプロパティの 1 つに至るパスを組み合わせたものになります。

シグナルカタログに次のノードが含まれている場合の例:

```
{
    myVehicle.ADAS.Camera:
    type: sensor
    datatype: Vehicle.ADAS.CameraStruct
    description: "A camera sensor"

    myVehicle.ADAS.CameraStruct:
    type: struct
    description: "An obstacle detection camera output struct"
}
```

ノードが ROS 2 の定義に従っている場合の例:

```
{
    Vehicle.ADAS.CameraStruct.msg:
    boolean obstaclesExists
    uint8[] image
    Obstacle[30] obstacles
}
{
    Vehicle.ADAS.Obstacle.msg:
    float32: probability
    uint8 o_type
    float32: distance
}
```

すべての可能なイベント式変数は以下のとおりです。

```
{
...
    $variable.`myVehicle.ADAS.Camera.obstaclesExists`
    $variable.`myVehicle.ADAS.Camera.Obstacle[0].probability`
    $variable.`myVehicle.ADAS.Camera.Obstacle[1].probability`
...
    $variable.`myVehicle.ADAS.Camera.Obstacle[29].probability`
    $variable.`myVehicle.ADAS.Camera.Obstacle[0].o_type`
    $variable.`myVehicle.ADAS.Camera.Obstacle[1].o_type`
...
    $variable.`myVehicle.ADAS.Camera.Obstacle[29].o_type`
    $variable.`myVehicle.ADAS.Camera.Obstacle[0].distance`
    $variable.`myVehicle.ADAS.Camera.Obstacle[1].distance`
...
    $variable.`myVehicle.ADAS.Camera.Obstacle[29].distance`
}
```

AWS IoT FleetWise キャンペーンを更新する

UpdateCampaign API オペレーションを使用すると、既存のキャンペーンを更新できます。次のコマンドは を使用します AWS CLI。

- *campaign-name* は、更新するキャンペーンの名前に置き換えます。
- *action* は、次のいずれかに置き換えます。
  - APPROVE — キャンペーンを承認して、 AWS IoT FleetWise が車両またはフリートにデプロイできるようにします。
  - SUSPEND - キャンペーンを停止します。キャンペーンが車両から削除され、停止中のキャンペーン内のすべての車両でデータ送信が停止されます。
  - RESUME - SUSPEND で停止したキャンペーンを再開します。キャンペーンは次のチェックイン時にすべての車両に再デプロイされるように設定され、車両はデータの送信を再開します。
  - UPDATE – 属性を定義し、キャンペーンに関連付けることで、キャンペーンを更新します。
- *description* は、新しい説明に置き換えます。

  説明には最大 2,048 文字を使用できます。
- *data-extra-dimensions* を指定された車両属性に置き換えて、キャンペーン中に収集されたデータを強化します。たとえば、車両メーカーとモデルをキャンペーンに追加できます。 AWS IoT FleetWise はデータを Amazon Timestream のディメンションとしてそれらの属性に関連付けます。その後、車両のメーカーとモデルに対してデータをクエリできます。

```
aws iotfleetwise update-campaign \
            --name campaign-name \
            --action action \
            --description description \
            --data-extra-dimensions data-extra-dimensions
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが UpdateCampaign API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

AWS IoT FleetWise キャンペーンを削除する

IoT FleetWise AWS IoT コンソールまたは API を使用してキャンペーンを削除できます。

キャンペーンの削除 (コンソール)

キャンペーンを削除するには、 AWS IoT FleetWise コンソールを使用します。

キャンペーンを削除するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[キャンペーン] を選択します。
3. [キャンペーン] ページで、ターゲットキャンペーンを選択します。

4. [削除] を選択します。
5. [**campaign-name** を削除しますか?] で、削除するキャンペーンの名前を入力し、[確認] を選択します。

キャンペーンの削除 (AWS CLI)

DeleteCampaign API オペレーションを使用すると、キャンペーンを削除できます。次の例では、 を使用します AWS CLI。

キャンペーンを削除するには、次のコマンドを実行します。

campaign-name は、削除する車両の名前に置き換えます。

```
aws iotfleetwise delete-campaign --name campaign-name
```

> **削除されたデータパーティションは復元できません**
>
> キャンペーンを削除すると、デバイスからすべてのデータが削除され、パーティション内のデータはクラウドにアップロードされません。

キャンペーンの削除を確認する

ListCampaigns API オペレーションを使用すると、キャンペーンが削除されたかどうかを確認できます。次の例では AWS CLIを使用しています。

すべてのキャンペーンの概要をページ分割されたリストとして取得するには、次のコマンドを実行します。

```
aws iotfleetwise list-campaigns
```

Get AWS IoT FleetWise キャンペーン情報

GetCampaign API オペレーションを使用すると、車両情報を取得できます。次の例では AWS CLIを使用しています。

キャンペーンのメタデータを取得するには、次のコマンドを実行します。

campaign-name は、取得するキャンペーンの名前に置き換えます。

```
aws iotfleetwise get-campaign --name campaign-name
```

> **Note**
>
> このオペレーションは結果整合性があります。言い換えると、キャンペーンへの変更はすぐには反映されない場合があります。

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが GetCampaign API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
    },
  ]
}
```

キャンペーンデータの保存と転送

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

キャンペーン内のデータパーティションを使用して、車両とフリートの信号データを Edge に一時的に保存します。データパーティションのアップロードオプションとストレージオプションを設定する

ことで、指定したデータ送信先 (Amazon S3 バケットなど) へのデータ転送に最適な条件を最適化できます。例えば、Wi-Fi に接続するまで車両にデータを保存するようにデータパーティションを設定できます。次に、車両が接続すると、キャンペーンはその特定のパーティション内のデータをクラウドに送信するようトリガーします。または、 AWS IoT ジョブを使用してデータを収集することもできます。

トピック

- データパーティションを作成する
- キャンペーンデータをアップロードする
- ジョブを使用して AWS IoT データをアップロードする

データパーティションを作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

キャンペーンのデータパーティションは、シグナルデータを一時的に保存します。データをクラウドに転送するタイミングと方法を設定します。

データパーティションは、まずキャンペーン`dataPartitionId`の を使用して特定のデータセットを指定することで機能します。次に、最大サイズ、データパーティションをライブ (ディスク上) に維持する最小時間、データを Edge に保存する場所などのパーティションストレージオプションをさらに定義できます。を使用して、車両のストレージの場所を特定できます`storageLocation`。ストレージの場所によって、キャンペーンストレージフォルダのデータパーティションのフォルダ名が決まります。キャンペーンストレージフォルダは、 Edge 設定ファイルで定義された永続性パスの車両名の後に名前が付けられたフォルダにあります。これはストレージの場所の絶対パスです: `{persistency_path} / {vehicle_name} / {campaign_name} / {storage_location}`。

に設定されたスプーリングモードは、パーティション化されたデータを車両のディスクに保存することと`TO_DISK`を指定します。データパーティションのデータストレージは、FIFO (先入れ先出し) ベースで動作します。キャンペーンを削除すると、関連するデータパーティションのデータも削除されます。接続のオン/オフのユースケースにデータパーティションを指定しない場合でも、 AWS IoT FleetWise は、接続がない場合でもデータを車両のリングバッファに保存します。接続が再開される

と、 AWS IoT FleetWise はデータをクラウドにアップロードします。この動作は、 Edge Agent for AWS IoT FleetWise ソフトウェアで設定できます。

> **Important**
>
> データパーティションが設定された最大ストレージ制限を超えると、パーティションが最大サイズに達すると、新しいデータによって古いデータが上書きされます。Edge で失われたデータは復元できません。ストレージサイズは、 Edge ストレージの制限によって決まります。
>
> データがクラウドにアップロードされると、最小有効期限が経過した後に削除できます。意図しない削除を避けるために、適切な有効期限を設定します。

アップロードオプションは、変数式と条件言語を決定します。アップロードオプションが指定されている場合は、ストレージオプションも指定する必要があります。データパーティション内のシグナルをクラウドにアップロードするようにリクエストすることもできます。詳細については、「キャンペーンデータをアップロードする」を参照してください。

データパーティション条件が定義された後、 はデータパーティションで考慮するシグナルを指定する`signalsToCollect`のに役立ちます。データパーティションIDs を指定するか、`dataPartitionId`を に設定`default`して、確立されたデフォルトのデータパーティションを使用できます。が指定されていないシグナル`dataPartitionId`は、デフォルトの に関連付けられます`dataPartition`。

データパーティションを作成するには

次の例を使用して、データパーティションストレージ条件でキャンペーンを作成します。このサンプルキャンペーンは、車両データを Amazon Timestream に保存するように設定されています。

1. *`campaign-name`* は、作成するキャンペーンの名前に置き換えます。
2. (オプション) 説明を入力します。
3. *`role-arn`* を、Timestream テーブルにデータを配信する許可を AWS IoT FleetWise に付与するタスク実行ロールの Amazon リソースネーム (ARN) に置き換えます。
4. *`table-arn`* は、Timestream テーブルの ARN に置き換えます。
5. *`signal-catalog-arn`* は、シグナルカタログの ARN に置き換えます。
6. *`data-partition-id`* は、`dataPartitions`ID と の両方を に関連付ける ID に置き換えます`signalsToCollect`。まず、シグナルで使用するデータパーティションの ID を置き換えま

す。の場合signalsToCollect、ID は で指定された IDs のいずれかと一致する必要がありますdataPartitions。

> **Note**
>
> を ID defaultとして使用して、キャンペーンのデフォルトのデータパーティションを確立します。

7. *target-arn* は、作成したフリートまたは車両の ARN に置き換えます。

```
{
    "name": "campaign-name",
    "description": "Measurement of SOC, SOH, thermal, and power optimization for Fleet
 2704",
    "targetArn": "target-arn",
    "collectionScheme": {
        "conditionBasedCollectionScheme": {
            "conditionLanguageVersion": 1,
            "expression": "$variable.`Vehicle.BMS` > 50",
            "minimumTriggerIntervalMs": 1000,
            "triggerMode": "ALWAYS"
        }
    },
    "compression": "SNAPPY",
    "dataDestinationConfigs": [{
        "timestreamConfig": {
            "executionRoleArn": "role-arn",
            "timestreamTableArn": "table-arn"
        }
    }],
    "dataPartitions": [{
        "id": "data-partition-id",
        "storageOptions": {
            "maximumSize": {
                "unit": "GB",
                "value": 1024
            },
            "minimumTimeToLive": {
                "unit": "WEEKS",
                "value": 6
            },
```

```
            "storageLocation": "string"
        },
        "uploadOptions": {
            "conditionLanguageVersion": 1,
            "expression": "$variable.`Vehicle.BMS.PowerOptimization` > 90"
        }
    }],
    "signalCatalogArn": "signal-catalog-arn",
    "signalsToCollect": [{
        "dataPartitionId": "data-partition-id",
        "maxSampleCount": 50000,
        "minimumSamplingIntervalMs": 100,
        "name": "Below-90-percent"
    }],
    "spoolingMode": "TO_DISK",
    "tags": [{
        "Key": "BMS",
        "Value": "Under-90"
    }]
}
```

指定されたすべての条件を満たすと、パーティション化されたデータはクラウドに転送され、新しいパーティション化されたシグナルの収集と保存が可能になります。

次に、 `UpdateCampaign` API を呼び出して、それを Edge Agent for AWS IoT FleetWise ソフトウェアにデプロイします。詳細については、「キャンペーンデータをアップロードする」を参照してください。

キャンペーンデータをアップロードする

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

Edge にキャンペーンデータをアップロードするには、次の 2 つの方法があります。

- アップロード条件を満たすキャンペーンは、承認後にデータを自動的にクラウドにアップロードします。キャンペーンを承認するには、 `updateCampaign` API オペレーションを使用します。

- AWS IoT ジョブを使用すると、指定した条件が満たされない場合でも、データを強制的にアップロードできます。詳細については、「ジョブを使用して AWS IoT データをアップロードする」を参照してください。

UpdateCampaign API オペレーションを使用してキャンペーンデータをアップロードするには

キャンペーンを作成すると、 を に変更WAITING_FOR_APPROVALするまで、キャンペーンのステータスは action として表示されますAPPROVED。

- 次のサンプルを使用して、UpdateCampaign API オペレーションで を呼び出しactionてキャンペーンを更新します。

```
{
   "action": "APPROVED",
   "dataExtraDimensions": [ "string" ],
   "description": "string",
   "name": "string"
}
```

ジョブを使用して AWS IoT データをアップロードする

> **Important**
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT ジョブを使用すると、保存されている車両データを必要なときにクラウドにアップロードするようにキャンペーンを設定できます。

キャンペーンのジョブドキュメントを作成するには

- 次の例を使用して、キャンペーンのジョブドキュメントを作成します。ジョブドキュメントは、ジョブの実行に必要な車両またはフリートに関する情報を含む .json ファイルです。ジョブドキュメントの作成の詳細については、「 デベロッパーガイド」の「 を使用してジョブを作成および管理する AWS CLI」を参照してください。 AWS IoT

1 つの車両のみがデータをアップロードするようにリクエストするには、ジョブターゲットを車両に関連付けられている AWS IoT モノに設定します。複数の車両 (同じキャンペーン内) にデータのアップロードをリクエストするには、車両に対応するすべてのモノのモノのグループを作成し、ジョブターゲットをモノのグループに設定します。

```
{
  "version": "1.0",
  "parameters": {
     "campaignArn": ${aws:iot:parameter:campaignArn},
     "endTime": ${aws:iot:parameter:endTime}
  }
}
```

a. を同じリージョンとアカウントのキャンペーンの Amazon リソースネーム (ARN) `CampaignArn`に置き換えます。キャンペーン ARN が必要です。

b. (オプション) を、ISO 8601 UTC 形式 (ミリ秒なし) で車両で収集されたデータのタイムスタンプ`endTime`に置き換えます。例えば、`2024-03-05T23:00:00Z` と指定します。タイムスタンプは排他的であり、アップロードする最後のデータポイントを決定します。を省略すると`endTime`、キャンペーンに保存されたデータがすべてアップロードされるまで、エッジエージェントソフトウェアはアップロードを続行します。すべてのデータがアップロードされると、ジョブの実行ステータスが に更新されます`SUCCEEDED`。ジョブの状態がに更新されます`COMPLETED`。

マネージドジョブテンプレートを使用してジョブを作成するには

1. マネージドテンプレートのリストから IoT-IoTFleetWise-CollectCampaignData を選択します。詳細については、「 デベロッパーガイド」の AWS 「マネージドテンプレートからジョブを作成する」を参照してください。 AWS IoT
2. マネージドテンプレートには、 `CampaignArn`および `endTime`パラメータがあります。

   a. を同じリージョンとアカウントのキャンペーンの Amazon リソースネーム (ARN) `CampaignArn`に置き換えます。キャンペーン ARN が必要です。

   b. (オプション) を、ISO 8601 UTC 形式 (ミリ秒なし) で車両で収集されたデータのタイムスタンプ`endTime`に置き換えます。例えば、`2024-03-05T23:00:00Z` と指定します。タイムスタンプは排他的であり、アップロードする最後のデータポイントを決定します。を省略すると`endTime`、キャンペーンに保存されたデータがすべてアップロードされるまで、

エッジエージェントソフトウェアはアップロードを続行します。すべてのデータがアップロードされると、ジョブの実行ステータスが に更新されますSUCCEEDED。ジョブの状態が に更新されますCOMPLETED。

関連するトラブルシューティングのトピックについては、「」を参照してください問題の保存と転送。

AWS IoT ジョブの詳細については、「 AWS IoT デベロッパーガイド」の「ジョブ」を参照してください。

AWS IoT FleetWise を使用して診断問題コードデータを収集する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

車両がエラーを検出すると、診断問題コード (DTC) が生成され、影響を受けたセンサーまたはアクチュエータのスナップショットが記録されます。DTC は、エラーについてほぼリアルタイムで学習し、原因を理解し、修正アクションを実行するのに役立ちます。 AWS IoT FleetWise は、対応する DTCs スナップショットやデータ収集キャンペーンを通じた拡張データを含む DTC の収集をサポートしています。このトピックでは、例で示すように、DTC データ収集を容易にする概念、ワークフロー、キーワードについて説明します。

以下に、DTC を使用するための主要な概念を示します。

カスタム定義関数

カスタム定義関数は、エッジエージェントで事前定義された独自の関数を呼び出して実行し、カスタムデコードの概念を拡張する機能です。これらの関数は、 AWS IoT FleetWise エージェントと連携して使用されます。Edge Agent for AWS IoT FleetWise ソフトウェアは、最小値、最大値、平均値などのシグナル統計を計算するための組み込み関数を提供します。カスタム定義の 関数は、特定のユースケースに合わせてカスタマイズされたロジックを作成できるようにすることで、この機能を拡張します。診断問題コード (DTC) データ収集の場合、デベロッパーはカスタム関数を活用して、Unified Diagnostic Services (UDS) または代替診断インターフェイスを介して車両の Edge から直接 DTC コード、スナップショット、拡張データを取得するなどの高度なデータ取り出しメカニズムを実装できます。

詳細については、「カスタム関数ガイド」および「Edge Agent デベロッパーガイド」の「DTC データ収集リファレンス実装」を参照してください。

シグナルフェッチ

データ収集キャンペーンでは、通常、信号はデバイスから継続的に収集され、エッジエージェントソフトウェアにバッファされます。その後、シグナルは時間ベースのキャンペーンで定期的にアップロードまたは保存されるか、条件ベースのキャンペーンの特定の条件によってトリガーされます。ただし、デバイストラフィックの輻輳が懸念されるため、デバイスから DTC 信号を収集して継続的にバッファリングすることはできません。これに対処するために、 AWS IoT FleetWise はシグナルフェッチを提供します。これにより、ターゲットシグナルがデバイスから不連続にフェッチされます。

シグナルフェッチは、定期的なアクションと条件駆動型のアクションの両方をサポートします。デバイスから継続的に収集すべきではないシグナルごとにカスタム定義の関数を使用して、フェッチ駆動型メソッド、条件、正確なアクションを定義できます。シグナルフェッチメカニズムによって管理されるシグナルの場合、ローカルストレージまたはクラウドアップロードのトリガータイプと条件は`CollectionScheme`引き続き によって管理されます。`timeBasedCollectionScheme`と の両方`conditionBasedCollectionScheme`がサポートされ、通常のシグナルと同じです。

以下のトピックでは、DTCs を作成して使用する方法について説明します。

トピック

- 診断問題コードキーワード
- 診断問題コードのデータ収集キャンペーンを作成する
- 診断問題コードのユースケース

診断問題コードキーワード

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

signalsToFetch キャンペーンを作成するための パラメータ

signalsToFetch 構文を使用して、 Edge でシグナル情報を取得する方法を設定します。標準シグナルフェッチは、デコーダーマニフェストで明示的に定義されたルール、または Edge First Modeling で定義されたカスタムルールとしてモデリングすることによって制御されます。フェッチするシグナルを使用すると、キャンペーン中にデータを取得するタイミングと方法を定義できます。

取得するシグナルにより、DTC 情報を収集できます。例えば、すべてのエンジンコントロールユニット (ECU) の DTC 情報を含むことができる `DTC_Info` という名前の文字列タイプのシグナルを作成できます。または、特定の ECU をフィルタリングすることもできます。

- `SignalFetchInformation` 構造とパラメータの定義。

```
structure SignalFetchInformation {
    @required
    fullyQualifiedName: NodePath,
    @required
    signalFetchConfig: SignalFetchConfig,
    // Conditional language version for this config
    conditionLanguageVersion: languageVersion,
    @required
    actions: EventExpressionList,
}
```

  - `fullyQualifiedName`: カスタムフェッチを使用するシグナルの完全修飾名 (FQDN)。
  - `signalFetchConfig`: 上記の定義されたシグナルを取得する方法に関するルールを定義します。時間ベースおよび条件ベースのフェッチをサポートしています。
  - `conditionLanguageVersion`: 設定で式を解析するために使用される条件言語バージョン。
  - `actions`: Edge で評価されたすべてのアクション式のリスト。Edge は、定義されたシグナルの値を取得します。

> **Important**
>
> アクションは のみを使用できます`custom_function`。

キャンペーン式のキーワード

次の式は、車両でサポートされているシグナルの完全修飾名を取得し、 Edge のシグナルバッファにデータがない場合に true を返します。また、false を返します。

```
isNull(signalFqdn:String): Boolean
```

Example 使用

```
isNull($variable.`Vehicle.ECU1.DTC_INFO`) == false

We want to make sure DTC_Info signal is being generated
on edge.
```

この式は、次の入力を受け取ります。

functionName:文字列

Edge でサポートされているカスタム関数の名前

params: varargs*Expression*

のパラメータfunctionName。これは、任意の式のリストにすることができます。

パラメータはリテラルタイプをサポートします。文字列、整数、ブール値、または倍精度。

```
custom_function(functionName:String, params: varargsExpression): Void
```

Example 使用

```
{
       "fullyQualifiedName":"Vehicle.ECU1.DTC_INFO",
       "signalFetchConfig":{
          "timeBased":{
             "executionFrequencyMs":2000
          }
       },
       "actions":"custom_function(“DTC_QUERY”, -1, 2, -1)"
    }
```

診断問題コードのデータ収集キャンペーンを作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

このトピックでは、診断問題コード (DTC) のデータ収集キャンペーンを作成する方法について説明します。

1. Edge でカスタムシグナルを定義します。Edge の DTC 信号のデコードルールをカスタムデコード信号として定義する必要があります。詳細については、「チュートリアル: カスタムデコードインターフェイスを使用してネットワークに依存しないデータ収集を設定する」を参照してください。
2. Edge でカスタム関数を定義します。Edge でコンパイル時に DTC シグナルを収集するためのカスタム関数を定義する必要があります。

   詳細については、「 カスタム関数ガイド」および「 Edge Agent デベロッパーガイド」の「DTC データ収集リファレンス実装」を参照してください。

   > **Note**
   >
   > カスタム定義関数の例は、デモスクリプトに示されているDTC_QUERYとおりです。

3. DTC シグナルを文字列タイプとしてモデル化するシグナルカタログを作成します。

```
[
 {
    "branch": {
        "fullyQualifiedName": "Vehicle",
        "description": "Vehicle"
        }
      },
      {
    "branch": {
        "fullyQualifiedName": "Vehicle.ECU1",
        "description": "Vehicle.ECU1"
        }
      },
```

```
      {
    "sensor": {
        "fullyQualifiedName": "Vehicle.ECU1.DTC_INFO",
        "description": "Vehicle.ECU1.DTC_INFO",
        "dataType": "STRING"
      }
   }
 ]
```

4. DTC シグナルを追加して車両モデルを作成してアクティブ化します。
5. DTC シグナルを追加したデコーダーマニフェストを作成してアクティブ化します。DTC シグナルは、CUSTOM_DECODING_INTERFACEネットワークインターフェイスタイプのCUSTOM_DECODING_SIGNALシグナルデコーダータイプである必要があります。

   Example シグナルデコーダー

```
[
  {
    "fullyQualifiedName": "Vehicle.ECU1.DTC_INFO",
    "interfaceId": "UDS_DTC",
    "type": "CUSTOM_DECODING_SIGNAL",
    "customDecodingSignal": {
      "id": "Vehicle.ECU1.DTC_INFO"
    }
  }
 ]
```

   Example ネットワークインターフェイス

```
[
  {
    "interfaceId": "UDS_DTC",
    "type": "CUSTOM_DECODING_INTERFACE",
    "customDecodingInterface": {
      "name": "NamedSignalInterface"
    }
  }
]
```

> **Note**
> コントローラーエリアネットワーク (CAN) シグナルは、文字列データ型をサポートしていません。

6. 車両をプロビジョニングして作成します。車両は、前のステップでアクティブ化された車両モデル (モデルマニフェスト) とデコーダーマニフェストを使用する必要があります。
7. キャンペーンを作成して承認します。DTC シグナル (オプションでテレメトリシグナルを使用) を定義してキャンペーンを作成し、車両にデプロイする必要があります。
8. 定義された送信先のデータにアクセスします。DTC データには`DTCCode`、キャンペーンで定義されたデータ送信先の raw 文字列`DTCExtendedDatastrings`として `DTCSnapshot`、、 が含まれます。

診断問題コードのユースケース

> **Important**
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

次のユースケースでは、 `DTC_QUERY`関数がデモスクリプトで定義されていることを前提としています。

定期的なフェッチ

設定された間隔で DTC コレクションを取得します。

次の例は、すべての ECU のステータスマスクを持つすべての DTCs`Vehicle.DTC_INFO`に対しての定期的なシグナルフェッチを行うキャンペーンです。 ECUs 用に収集されたデータには条件があります`Vehicle.DTC_INFO`。

```
{
  "compression": "SNAPPY",
  "spoolingMode": "TO_DISK",
  "signalsToFetch": [
    {
      "fullyQualifiedName": "Vehicle.ECU1.DTC_INFO",
```

```
      "signalFetchConfig": {
        "timeBased": {
        // The FleetWise Edge Agent will query the UDS module for all DTCs every five
 seconds.
          "executionFrequencyMs": 5000
        }
      },
      "actions": [
      // Every five seconds, this action is called and its output is stored in the
      // signal history buffer of Vehicle.DTC_INFO
        "custom_function(\"DTC_QUERY\", -1, 2, -1)"
      ]
    }
  ],
  "signalsToCollect": [
    {
      "name": "Vehicle.ECU1.DTC_INFO"
    }
  ],
  "collectionScheme": {
    "conditionBasedCollectionScheme": {
      "conditionLanguageVersion": 1,
      // Whenever a new DTC is filled into the signal, the data is ingested.
      "expression": "!isNull($variable.`Vehicle.ECU1.DTC_INFO`)",
      "minimumTriggerIntervalMs": 1000,
      // Make sure that data is ingested only when there are new DTCs.
      "triggerMode": "RISING_EDGE"
    }
  },
  "dataDestinationConfigs": [
    {
      "s3Config":
        {
          "bucketArn": "bucket-arn",
          "dataFormat": "PARQUET",
          "prefix": "campaign-name",
          "storageCompressionFormat": "GZIP"
        }
    }
  ]
}
```

条件駆動型フェッチ

条件が満たされたときに DTC コレクションを取得します。例えば、CAN シグナルが の場合`Vehicle.Ignition == 1`、DTC データを取得してアップロードします。

次のキャンペーン例では、条件駆動型の シグナルフェッチ`Vehicle.ECU1.DTC_INFO`を使用して、ECU-1 の recordNumber 1 で DTC ("AAA123") が保留になっているかどうかを確認します。recordNumber このキャンペーンには、時間ベースのデータ収集とアップロードがあります。

```
{
  "compression": "SNAPPY",
  "spoolingMode": "TO_DISK",
  "signalsToFetch": [
    {
      "fullyQualifiedName": "Vehicle.ECU1.DTC_INFO",
      "signalFetchConfig": {
        "conditionBased": {
        // The action will only run when the ignition is on.
          "conditionExpression": "$variable.`Vehicle.Ignition` == 1",
          "triggerMode": "ALWAYS"
        }
      },
      // The UDS module is only requested for the specific ECU address and the specific
 DTC Number/Status.
      "actions": ["custom_function(\"DTC_QUERY\", 1, 2, 8, \"0xAAA123\")"]
    }
  ],
  "signalsToCollect": [
    {
      "name": "Vehicle.ECU1.DTC_INFO"
    },
    {
      "name": "Vehicle.Ignition"
    }
  ],
  "collectionScheme": {
    "timeBasedCollectionScheme": {
      "periodMs": 10000
    }
  },
  "dataDestinationConfigs": [
    {
      "s3Config":
```

```
        {
          "bucketArn": "bucket-arn",
          "dataFormat": "PARQUET",
          "prefix": "campaign-name",
          "storageCompressionFormat": "GZIP"
        }
    }
  ]
}
```

オンデマンドフェッチ

フリートの特定の DTC を取得します。

オンデマンドのユースケースでは、定期的なフェッチで定義されているのと同じキャンペーンを使用できます。オンデマンド効果は、 AWS IoT FleetWise コンソールを使用してキャンペーンをデプロイした直後にキャンペーンを停止するか、次の CLI コマンドを実行することで実現されます。

- *command-name* をコマンド名に置き換えます。

```
aws iotfleetwise update-campaign \
    --name campaign-name \
    --action APPROVE
```

次に、DTC データが到着したらキャンペーンを停止します。

```
aws iotfleetwise update-campaign \
    --name campaign-name \
    --action SUSPEND
```

キャンペーンを再開して、DTC データフェッチを行うことができます。

```
aws iotfleetwise update-campaign \
    --name campaign-name \
    --action RESUME
```

Visualize AWS IoT FleetWise 車両データ

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

Edge Agent for AWS IoT FleetWise ソフトウェアは、選択した車両データを MQTT トピックに送信するか、Amazon Timestream または Amazon Simple Storage Service (Amazon S3) に転送します。データがデータ送信先に到着したら、他の AWS サービスを使用してデータを処理、再ルーティング、視覚化、共有できます。

> **Note**
>
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

MQTT トピックに送信される車両データの処理

MQTT メッセージングによって送信される車両データはほぼリアルタイムで配信され、ルールを使用してアクションを実行したり、データを他の送信先にルーティングしたりできます。MQTT の使用の詳細については、「 AWS IoT Core デベロッパーガイド」の「 デバイス通信プロトコルと のルール AWS IoT」を参照してください。

MQTT メッセージで送信されるデータのデフォルトのスキーマには、次のフィールドが含まれます。

フィールド名	データ型	説明
`eventId`	varchar	データ収集イベントの ID。
`vehicleName`	varchar	データが収集された車両の ID。
`name`	varchar	エッジエージェントソフトウェアがデー

フィールド名	データ型	説明
		タ収集に使用したキャンペーンの名前。
`time`	timestamp	データポイントのタイムスタンプ。
`measure_name`	varchar	シグナルの名前。
`measure_value::bigint`	bigint	Integer 型のシグナル値。
`measure_value::double`	double	Double 型のシグナル値。
`measure_value::boolean`	boolean	Boolean 型のシグナル値。
`measure_value::varchar`	varchar	varchar 型のシグナル値。

Timestream で車両データを処理する

Timestream は、1 日あたりに何兆もの時系列データポイントを保存して分析できる、フルマネージド型の時系列データベースです。データはカスタマー管理の Timestream テーブルに保存されます。Timestream を使用すると、車両データにクエリを実行して、車両に関するインサイトを得ることができます。詳細については、「What is Amazon Timestream?」を参照してください。

Timestream に転送されるデータのデフォルトのスキーマには、次のフィールドが含まれています。

フィールド名	データ型	説明
`eventId`	varchar	データ収集イベントの ID。
`vehicleName`	varchar	データが収集された車両の ID。

フィールド名	データ型	説明
`name`	varchar	エッジエージェントソフトウェアがデータ収集に使用したキャンペーンの名前。
`time`	timestamp	データポイントのタイムスタンプ。
`measure_name`	varchar	シグナルの名前。
`measure_value::bigint`	bigint	Integer 型のシグナル値。
`measure_value::double`	double	Double 型のシグナル値。
`measure_value::boolean`	boolean	Boolean 型のシグナル値。
`measure_value::varchar`	varchar	varchar 型のシグナル値。

Timestream に保存されている車両データを視覚化する

車両データが Timestream に転送されたら、次の AWS のサービスを使用して、データの視覚化、モニタリング、分析、共有を行うことができます。

- Grafana または Amazon Managed Grafana を使用して、ダッシュボードでデータを視覚化してモニタリングします。1 つの Grafana ダッシュボードで、複数の AWS ソース (Amazon CloudWatch や Timestream など) やその他のデータソースからのデータを視覚化できます。
- QuickSight を使用してダッシュボード内のデータを分析および視覚化します。

Amazon S3 で車両データを処理する

Amazon S3 は、任意の量のデータを保存して保護するオブジェクトストレージサービスです。S3 は、データレイク、バックアップと復元、アーカイブ、エンタープライズアプリケーション、 AWS

IoT デバイス、ビッグデータ分析など、さまざまなユースケースに使用できます。データは、バケット内のオブジェクトとして S3 に保存されます。詳細については、「Amazon S3 とは」を参照してください。

Amazon S3 に転送されるデータのデフォルトのスキーマには、次のフィールドが含まれています。

フィールド名	データ型	説明
`eventId`	varchar	データ収集イベントの ID。
`vehicleName`	varchar	データが収集された車両の ID。
`name`	varchar	エッジエージェントソフトウェアがデータ収集に使用したキャンペーンの名前。
`time`	timestamp	データポイントのタイムスタンプ。
`measure_name`	varchar	シグナルの名前。
`measure_value_BIGINT`	bigint	Integer 型のシグナル値。
`measure_value_DOUBLE`	double	Double 型のシグナル値。
`measure_value_BOOLEAN`	boolean	Boolean 型のシグナル値。
`measure_value_STRUCT`	struct	Struct 型のシグナル値。
`measure_value_VARCHAR`	varchar	varchar 型のシグナル値。

Amazon S3 オブジェクト形式

AWS IoT FleetWise は車両データを S3 に転送し、そこでオブジェクトとして保存されます。データを一意に識別するオブジェクト URI を使用して、キャンペーンのデータを検索できます。S3 オブジェクト URI 形式は、収集データが非構造化データか処理済みデータかによって異なります。

Unstructured data (非構造化データ)

非構造化データは、事前に定義されていない方法で S3 に保存されます。画像や動画など、さまざまな形式で保存できます。

Amazon Ion ファイルからのシグナルデータを使用して AWS IoT FleetWise に渡される車両メッセージはデコードされ、オブジェクトとして S3 に転送されます。S3 オブジェクトは各シグナルを表し、バイナリエンコーディングされます。

非構造化データの S3 オブジェクト URI は、次の形式を使用します。

```
s3://bucket-name/prefix/unstructured-data/random-ID-yyyy-MM-dd-HH-mm-ss-SSS-
vehicleName-signalName-fieldName
```

処理済みデータ

処理済みデータは S3 に保存され、メッセージを検証、強化、変換する処理ステップを経ます。処理済みデータの例としては、オブジェクトリストや速度があります。

S3 に転送されたデータは、約 10 分間バッファリングされたレコードを表すオブジェクトとして保存されます。デフォルトでは、 AWS IoT FleetWise はオブジェクトを S3 に書き込む`year=YYYY/month=MM/date=DD/hour=HH`前に 形式の UTC 時間プレフィックスを追加します。このプレフィックスにより、バケットに論理階層が作成されます。各スラッシュ (/) は階層のレベルを形成します。処理済みデータには、非構造化データへの S3 オブジェクト URI も含まれます。

処理済みデータの S3 オブジェクト URI は、次の形式を使用します。

```
s3://bucket-name/prefix/processed-data/year=YYYY/month=MM/day=DD/hour=HH/
part-0000-random-ID.gz.parquet
```

raw データ

raw データは、プライマリデータとも呼ばれ、Amazon Ion ファイルから収集されたデータです。raw データを使用して、問題のトラブルシューティングを行ったり、エラーの根本原因を特定したりできます。

raw データの S3 オブジェクト URI は、次の形式を使用します。

```
s3://bucket-name/prefix/raw-data/vehicle-name/eventID-timestamp.10n
```

Amazon S3 に保存されている車両データを分析する

車両データを S3 に転送したら、以下の AWS のサービスを使用して、データのモニタリング、分析、共有を行うことができます。

Amazon SageMaker AI を使用して、ダウンストリームのラベル付けと機械学習 (ML) ワークフロー用にデータを抽出して分析します。

詳細については、Amazon SageMaker AI デベロッパーガイドの以下のトピックを参照してください。

- データを処理する
- 機械学習モデルをトレーニングする
- イメージにラベル付けする

を使用してデータをカタログ化し AWS Glue クローラー 、Amazon Athena で分析します。デフォルトでは、S3 に書き込まれたオブジェクトは Apache Hive スタイルのタイムパーティションに分割され、データパスには等号で接続されたキーと値のペアが含まれます。

詳細については、「Amazon Athena ユーザーガイド」の次のトピックを参照してください。

- Athena でのデータのパーティション化
- AWS Glue を使用して Amazon S3 のデータソースに接続する
- で Athena を使用する場合のベストプラクティス AWS Glue

QuickSight を使用してデータを視覚化するには、Athena テーブルまたは S3 バケットを直接読み取ります。

> **Tip**
>
> S3 から直接読み取る場合は、QuickSight が Apache Parquet 形式をサポートしていないため、車両データが JSON 形式であることを確認します。

詳細については、「Amazon QuickSight ユーザーガイド」の次のトピックを参照してください。

- サポートされているデータソース
- データソースの作成

コマンド

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。
> このドキュメントでは、AWS IoT FleetWise のコマンド機能を使用する方法について説明します。でコマンド機能を使用する方法については AWS IoT Device Management、「コマンド」を参照してください。
> お客様は、安全かつ適用法に準拠した方法でコマンドをデプロイする責任を単独で負います。責任の詳細については、AWS 「サービスのサービス条件 AWS IoT」を参照してください。

コマンド機能を使用して、クラウドから車両でコマンドを実行します。コマンドは一度に 1 つのデバイスをターゲットとし、デバイス側のログの取得やデバイスの状態変更の開始など、低レイテンシーで高スループットのアプリケーションに使用できます。

コマンドは、 によって管理されるリソースです AWS IoT Device Management。これには、車両にコマンド実行を送信するときに適用される再利用可能な設定が含まれています。特定のユースケースの一連のコマンドを事前定義することも、それらを使用して繰り返しユースケースの再利用可能な設定を作成することもできます。例えば、アプリで使用できるコマンドを設定して、車両のドアをロックしたり、温度をリモートで変更したりできます。

AWS IoT コマンド機能を使用すると、次のことができます。

- コマンドリソースを作成し、設定を再利用して複数のコマンドをターゲットデバイスに送信し、デバイスで実行します。
- 各コマンドをデバイスで実行する粒度を制御します。たとえば、車両を AWS IoT モノとしてプロビジョニングし、車両のドアをロックまたはロック解除するコマンドを送信できます。
- 前のコマンドが完了するのを待たずに、ターゲットデバイスで複数のコマンドを同時に実行します。
- コマンドイベントの通知を有効にし、コマンドの実行時と完了時にデバイスからステータスと結果情報を取得します。

以下のトピックでは、コマンドを作成、送信、受信、管理する方法について説明します。

トピック

- コマンドの概念
- 車両とコマンド
- コマンドの作成と管理
- コマンド実行の開始とモニタリング
- 例: コマンドを使用して車両のステアリングモードを制御する (AWS CLI)
- コマンドの使用シナリオ

コマンドの概念

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

コマンドは、クラウドからターゲットデバイスに送信される手順です。ターゲットデバイスは車両にすることができ、AWS IoT モノレジストリにモノとして登録する必要があります。コマンドには、車両のアクチュエータが実行する必要があるアクションを定義するパラメータを含めることができます。その後、車両はコマンドとそのパラメータを解析し、それらを処理して対応するアクションを実行します。その後、コマンド実行のステータスでクラウドアプリケーションに応答します。

詳細なワークフローについては、「」を参照してください車両とコマンド。

トピック

- コマンドの主な概念
- コマンド実行ステータス

コマンドの主な概念

コマンド機能を使用するためのいくつかの重要な概念と、それが最後の既知の状態 (LKS) 状態テンプレートとどのように機能するかを以下に示します。

コマンド

コマンドは、エンジンをオンにしたり、ウィンドウの位置を変更したりするなどのアクションを実行するために、物理的な車両に指示を送信するために使用できるエンティティです。特定のユースケースの一連のコマンドを事前定義することも、それらを使用して繰り返しユースケースの再利用可能な設定を作成することもできます。例えば、アプリで使用できるコマンドを設定して、車両のドアをロックしたり、温度をリモートで変更したりできます。

名前空間

コマンド機能を使用する場合は、コマンドの名前空間を指定する必要があります。 AWS IoT FleetWise でコマンドを作成するときは、名前空間`AWS-IoT-FleetWise`として を選択する必要があります。この名前空間を使用する場合は、車両でコマンドを実行するために使用されるパラメータを指定する必要があります。 AWS IoT Device Management 代わりに でコマンドを作成する場合は、代わりに `AWS-IoT`名前空間を使用する必要があります。詳細については、「 デAWS IoT Device Management ベロッパーガイド」の「 コマンド」を参照してください。

コマンドの状態

作成するコマンドは使用可能な状態になります。つまり、車両でコマンド実行を開始するために使用できます。コマンドが古くなった場合は、そのコマンドを非推奨にすることができます。非推奨状態のコマンドの場合、既存のコマンドの実行は完了するまで実行されます。コマンドを更新したり、新しい実行を実行したりすることはできません。新しい実行を送信するには、 コマンドを復元して使用可能にする必要があります。

コマンドが不要になった場合は削除することもできます。コマンドを削除対象としてマークすると、コマンドが最大タイムアウトの 24 時間より長い期間非推奨になっている場合、コマンドはすぐに削除されます。コマンドが非推奨になっていない場合、または最大タイムアウトより短い期間非推奨になっている場合、コマンドは保留中の削除状態になります。コマンドは 24 時間後にアカウントから自動的に削除されます。

パラメータ

コマンドを作成するときは、オプションで、コマンドの実行時にターゲット車両が実行するパラメータを指定できます。作成するコマンドは再利用可能な設定であり、複数のコマンド実行を車両に送信して同時に実行するために使用できます。または、実行時にのみパラメータを指定し、コマンドを作成して車両に送信するワンタイムオペレーションを実行することもできます。

ターゲット車両

コマンドを実行する場合は、コマンドを受信して特定のアクションを実行するターゲット車両を指定する必要があります。ターゲット車両はすでにモノとして登録されている必要があります

AWS IoT。コマンドを車両に送信すると、指定したパラメータと値に基づいてコマンドのインスタンスの実行が開始されます。

アクチュエータ

コマンドを実行する場合は、コマンドを受信する車両のアクチュエータと、実行するアクションを決定する値を指定する必要があります。オプションでアクチュエータのデフォルト値を設定して、不正確なコマンドを送信しないようにできます。例えば、コマンドが誤ってドアのロックを解除しないように、ドアロックアクチュエータ`LockDoor`にデフォルト値の を使用できます。アクチュエータの一般的な情報については、「」を参照してください主要なコンセプト。

データ型サポート

コマンド機能に使用されるアクチュエータでは、次のデータ型がサポートされています。

> **Note**
> 配列は、テレマティクスデータ、コマンド、または最後の既知の状態 (LKS) ではサポートされていません。配列データ型は、ビジョンシステムデータにのみ使用できます。

- 浮動小数点タイプ。次のタイプがサポートされます。
  - 浮動小数点数 (32 ビット)
  - ダブル (64 ビット)
- 整数 (署名付きと署名なしの両方) 。次の整数型がサポートされています。
  - int8 および uint8
  - int16 および uint16
  - int32 および uint32
- ロング。次のロングタイプがサポートされています。
  - ロング (int64)
  - 符号なしロング (uint64)
- String
- ブール値

コマンドの実行

コマンド実行は、ターゲットデバイスで実行されるコマンドのインスタンスです。車両は、コマンドの作成時またはコマンド実行の開始時に指定したパラメータを使用してコマンドを実行します。その後、車両は指定されたオペレーションを実行し、実行のステータスを返します。

> **Note**
>
> 特定の車両に対して、複数のコマンドを同時に実行できます。車両ごとに実行できる同時実行の最大数については、AWS IoT Device Management 「コマンドクォータ」を参照してください。

Last known state (LKS) 状態テンプレート

状態テンプレートは、車両所有者が車両の状態を追跡するメカニズムを提供します。車両の最後の既知の状態 (LKS) をほぼリアルタイムでモニタリングするには、状態テンプレートを作成して車両に関連付けることができます。

コマンド機能を使用すると、状態データの収集と処理に使用できる「オンデマンド」オペレーションを実行できます。たとえば、現在の車両状態を 1 回リクエスト (フェッチ) したり、以前にデプロイされた LKS 状態テンプレートをアクティブ化または非アクティブ化して、車両データのレポートを開始または停止したりできます。状態テンプレートでコマンドを使用する方法を示す例については、「」を参照してくださいコマンドの使用シナリオ。

コマンド実行ステータス

コマンド実行を開始すると、車両は実行のステータスを発行し、実行に関する追加情報としてステータスの理由を指定できます。以下のセクションでは、さまざまなコマンド実行ステータスとステータスコードについて説明します。

トピック

- コマンド実行ステータスの理由コードと説明
- コマンド実行ステータスとステータスコード
- コマンド実行のタイムアウトステータス

コマンド実行ステータスの理由コードと説明

コマンド実行ステータスの更新を報告するには、 AWS IoT Core デベロッパーガイドで説明されている コマンド予約トピックを使用して、車両は `UpdateCommandExecution` API を使用して更新されたステータス情報をクラウドに発行できます。ステータス情報をレポートする場合、デバイスは、 `StatusReason` オブジェクトを使用して各コマンド実行のステータス、および オブジェク

トreasonDescriptionに含まれるフィールドreasonCodeと に関する追加のコンテキストを提供できます。

コマンド実行ステータスとステータスコード

次の表は、さまざまなコマンド実行ステータスコードと、コマンド実行が移行できる許可されたステータスを示しています。また、コマンド実行が「ターミナル」かどうか (つまり、これ以上のステータスの更新は予定されていない) 、変更が車両またはクラウドによって開始されたかどうか、さまざまな事前定義されたステータスコード、およびそれらがクラウドによって報告されたステータスにどのようにマッピングされるかも表示されます。

- が事前定義されたステータスコードと statusReason オブジェクト AWS IoT FleetWise を使用する方法については、「 Edge Agent for AWS IoT FleetWise ソフトウェアドキュメント」の「コマンドステータス」を参照してください。
- ターミナル実行と非ターミナル実行、およびステータス間の遷移の詳細については、「 デAWS IoT Core ベロッパーガイド」の「コマンド実行ステータス」を参照してください。

コマンドの実行ステータスとソース

コマンド実行ステータス	説明	デバイス/クラウドによって開始されますか？	ターミナル実行？	許可されたステータス遷移	事前定義されたステータスコード
CREATED	コマンドの実行を開始する API リクエスト (StartCommandExecution API) が成功すると、コマンドの実行ステータスは に変わりますCREATED。	Cloud	いいえ	• IN_PROGRESS • SUCCEEDED • FAILED • REJECTED • TIMED_OUT	なし

コマンド実行ステータス	説明	デバイス/クラウドによって開始されますか？	ターミナル実行？	許可されたステータス遷移	事前定義されたステータスコード
IN_PROGRESS	車両がコマンドの実行を開始すると、応答トピックにメッセージを発行してステータスを に更新できますIN_PROGRESS 。	デバイス	いいえ	• IN_PROGRESS • 成功 • FAILED • 拒否 • TIMED_OUT	COMMAND_STATUS_COMMAND_IN_PROGRESS
SUCCEEDED	車両がコマンドを正常に処理し、実行を完了すると、レスポンストピックにメッセージを発行してステータスをに更新できますSUCCEEDED 。	デバイス	はい	該当しない	COMMAND_STATUS_SUCCEEDED

コマンド実行ステータス	説明	デバイス/クラウドによって開始されますか？	ターミナル実行？	許可されたステータス遷移	事前定義されたステータスコード
FAILED	車両がコマンドの実行に失敗すると、レスポンストピックにメッセージを発行してステータスをに更新できますFAILED。	デバイス	はい	該当しない	COMMAND_STATUS_EXECUTION_FAILED
REJECTED	車両がコマンドを受け入れない場合、レスポンストピックにメッセージを発行してステータスをに更新できますREJECTED。	デバイス	はい	該当しない	なし

コマンド実行ステータス	説明	デバイス/クラウドによって開始されますか？	ターミナル実行？	許可されたステータス遷移	事前定義されたステータスコード
TIMED_OUT	コマンドの実行ステータスは、次のいずれかTIMED_OUT の理由で に変わる可能性があります。 • コマンド実行の結果は受信されず、クラウドは自動的にTIMED_OUT ステータスを報告します。 • 車両は、コマンドを実行しようとしたときにタイムアウトが発生したことを報告します。この場合、コマンドの実行はターミナルになります。	デバイスとクラウド	いいえ	• 成功 • FAILED • 拒否 • TIMED_OUT	COMMAND_STATUS_EXECUTION_TIMEOUT

コマンド実行ステータス	説明	デバイス/クラウドによって開始されますか？	ターミナル実行？	許可されたステータス遷移	事前定義されたステータスコード
	このステータスの詳細については、「」を参照してください[コマンド実行のタイムアウトステータス](#)。				

コマンド実行のタイムアウトステータス

コマンド実行タイムアウトは、クラウドとデバイスの両方で報告できます。コマンドがデバイスに送信されると、タイマーが開始されます。指定された期間内にデバイスから応答を受信しなかった場合、クラウドは`TIMED_OUT`ステータスを報告します。この場合、 `TIMED_OUT`ステータスのコマンド実行は非ターミナルです。

デバイスは、このステータスを 、、 `SUCCEEDED` `FAILED`などのターミナルステータスに上書きできます`REJECTED`。コマンドの実行時にタイムアウトが発生したことを報告することもできます。この場合、コマンドの実行ステータスは のまま`TIMED_OUT`ですが、`StatusReason`オブジェクトのフィールドはデバイスによって報告された情報に基づいて更新されます。`TIMED_OUT` ステータスのコマンド実行がターミナルになりました。

詳細については、 デAWS IoT Core ベロッパーガイドの「コマンド実行タイムアウトに関する考慮事項」を参照してください。

車両とコマンド

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

お客様は、適用法に準拠し、安全かつ安全な方法でコマンドをデプロイする全責任を負います。

コマンド機能を使用するには：

1. まず、コマンドリソースを作成します。必要に応じて、コマンドの実行に必要な情報を含むパラメータを指定します。
2. コマンドを受け取り、指定されたアクションを実行するターゲット車両を指定します。
3. これで、ターゲットデバイスで コマンドを実行し、コマンド実行の詳細を確認してステータスを取得し、CloudWatch Logs を使用して問題のトラブルシューティングをさらに行うことができます。

以下のセクションでは、車両とコマンド間のワークフローについて説明します。

トピック

- ワークフローの概要
- 車両ワークフロー
- コマンドワークフロー
- (オプション) コマンド通知

ワークフローの概要

次の手順では、車両とコマンド間のコマンドワークフローの概要を示します。HTTP API オペレーションのいずれかのコマンドを使用すると、リクエストは Sigv4 認証情報を使用して署名されます。

> **Note**
>
> `StartCommandExecution` API オペレーションを除き、HTTP プロトコルで実行されるすべてのオペレーションはコントロールプレーンエンドポイントを使用します。

1. MQTT 接続を確立し、コマンドトピックをサブスクライブする

   コマンドワークフローを準備するには、デバイスは`iot:Data-ATS`エンドポイントとの MQTT 接続を確立し、上記のコマンドリクエストトピックをサブスクライブする必要があります。オプションで、デバイスは、承諾および拒否された応答トピックをサブスクライブすることもできます。

2. 車両モデルとコマンドリソースを作成する

   および `CreateCommand`コントロールプレーン API オペレーションを使用して、車両`CreateVehicle`とコマンドリソースを作成できるようになりました。コマンドリソースには、車両でコマンドが実行されたときに適用される設定が含まれています。

3. ターゲットデバイスでコマンド実行を開始する

   アカウント固有の`iot:Jobs`エンドポイントで`StartCommandExecution`データプレーン API を使用して、車両でコマンド実行を開始します。API は、protobuf でエンコードされたペイロードメッセージを コマンドリクエストトピックに発行します。

4. コマンド実行の結果を更新する

   車両はコマンドと受信したペイロードを処理し、 `UpdateCommandExecution` API を使用してコマンド実行の結果をレスポンストピックに発行します。車両が応答のトピックを受け入れたコマンドと拒否したコマンドをサブスクライブしている場合、応答がクラウドサービスによって受け入れられたか拒否されたかを示すメッセージが表示されます。

5. (オプション) コマンド実行結果を取得する

   コマンド実行の結果を取得するには、`GetCommandExecution`コントロールプレーン API オペレーションを使用できます。車両がコマンド実行結果をレスポンストピックに発行すると、この API は更新された情報を返します。

6. (オプション) コマンドイベントのサブスクライブと管理

   コマンド実行ステータスの更新に関する通知を受け取るには、 コマンドイベントトピックをサブスクライブします。その後、`CreateTopicRule`コントロールプレーン API を使用して、コマンドイベントデータを AWS Lambda 関数や Amazon SQS などの他のアプリケーションにルーティングし、その上にアプリケーションを構築できます。

車両ワークフロー

次の手順では、 コマンド機能を使用する際の車両のワークフローについて詳しく説明します。

> **Note**
> このセクションで説明するオペレーションでは、MQTT プロトコルを使用します。

1. MQTT 接続を確立する

   コマンド機能を使用するように車両を準備するには、まず AWS IoT Core メッセージブローカーに接続する必要があります。車両は、 メッセージブローカーに接続 AWS IoT Core して MQTT 接続を確立する `iot:Connect`アクションを実行できる必要があります。のデータプレーンエンドポイントを検索するには AWS アカウント、次に示すように `DescribeEndpoint` API または `describe-endpoint` CLI コマンドを使用します。

   ```
   aws iot describe-endpoint --endpoint-type iot:Data-ATS
   ```

   このコマンドを実行すると、次に示すように、アカウント固有のデータプレーンエンドポイントが返されます。

   ```
   account-specific-prefix.iot.region.amazonaws.com
   ```

2. Susbcribe to commands リクエストトピック

   接続が確立されると、デバイスは AWS IoT コマンド MQTT リクエストトピックにサブスクライブできます。コマンドを作成してターゲットデバイスでコマンド実行を開始すると、protobuf でエンコードされたペイロードメッセージがメッセージブローカーによってリクエストトピックに発行されます。その後、デバイスはペイロードメッセージを受信し、コマンドを処理できます。この例では、 をターゲット車両の一意の識別子*<DeviceID>*に置き換えます。この ID は、車両の一意の識別子またはモノの名前にすることができます。

   > **Note**
   > デバイスに送信されるペイロードメッセージは、protobuf 形式を使用する必要があります。

   ```
   $aws/commands/things/<DeviceID>/executions/+/request/protobuf
   ```

3. (オプション) コマンドレスポンストピックをサブスクライブする

   オプションで、これらのコマンドレスポンストピックをサブスクライブして、クラウドサービスがデバイスからのレスポンスを承諾したか拒否したかを示すメッセージを受信できます。

   > **Note**
   >
   > 車両が /acceptedおよび /rejectedレスポンストピックにサブスクライブすることはオプションです。車両は、これらのトピックに明示的にサブスクライブしていない場合でも、これらのレスポンスメッセージを自動的に受信します。

   ```
   $aws/commands/things/<DeviceID>/executions/<ExecutionId>/response/protobuf/accepted
   $aws/commands/things/<DeviceID>/executions/<ExecutionId>/response/protobuf/rejected
   ```

4. コマンド実行の結果を更新する

   その後、ターゲット車両はコマンドを処理します。次に、 UpdateCommandExecution API を使用して、実行の結果を次の MQTT レスポンストピックに発行します。

   > **Note**
   >
   > 特定の車両とコマンドの実行では、*<DeviceID>* は、デバイスがサブスクライブしたリクエストトピックの対応するフィールドと一致する必要があります。

   ```
   $aws/commands/things/<DeviceID>/executions/<ExecutionId>/response/protobuf
   ```

   UpdateCommandExecution API は、TLS で認証された MQTT に対するデータプレーン API オペレーションです。

   - クラウドサービスがコマンド実行結果を正常に処理すると、MQTT が受け入れたトピックにメッセージが発行されます。受け入れられるトピックは次の形式を使用します。

     ```
     $aws/commands/things/<DeviceID>/executions/<ExecutionId>/response/protobuf/
     accepted
     ```

   - クラウドサービスがコマンド実行結果を処理できなかった場合、MQTT 拒否トピックにレスポンスが発行されます。拒否されたトピックは次の形式を使用します。

```
$aws/commands/things/<DeviceID>/executions/<ExecutionId>/response/protobuf/
rejected
```

この API の詳細と例については、「」を参照してください[コマンド実行結果を更新する](#)。

コマンドワークフロー

次の手順では、コマンドワークフローについて詳しく説明します。

> **Note**
>
> このセクションで説明するオペレーションでは、HTTP プロトコルを使用します。

1. 車両を登録する

   これで、 コマンド機能を使用するように車両を準備できたので、車両を登録し、車両に送信されるコマンドを作成することで、アプリケーションを準備できます。車両を登録するには、`CreateVehicle`コントロールプレーン API オペレーションを使用して車両モデル (モデルマニフェスト) のインスタンスを作成します。詳細と例については、「車両の作成」を参照してください。

2. コマンドを作成する

   HTTP コントロールプレーン API `CreateCommand` オペレーションを使用して、ターゲットとする車両に適用されるコマンドをモデル化します。コマンドの実行時に使用するパラメータとデフォルト値を指定し、 `AWS-IoT-FleetWise`名前空間を使用していることを確認します。この API の使用に関する詳細と例については、「」を参照してください[コマンドリソースを作成する](#)。

3. コマンドの実行を開始する

   `StartCommandExecution` データプレーン API オペレーションを使用して、車両で作成したコマンドを実行できるようになりました。 AWS IoT Device Management はコマンドとコマンドパラメータを取得し、受信リクエストを検証します。次に、必要なパラメータを使用して AWS IoT FleetWise API を呼び出し、車両固有のペイロードを生成します。その後、ペイロードは MQTT AWS IoT Device Management を介して、デバイスがサブスクライブしたコマンドリクエ

ストトピックにデバイスに送信されます。この API の使用に関する詳細と例については、「」を参照してください[コマンドを送信する (AWS CLI)](#)。

```
$aws/commands/things/<DeviceID>/executions/+/request/protobuf
```

> **Note**
>
> コマンドがクラウドから送信され、MQTT 永続セッションが使用中のときにデバイスがオフラインだった場合、コマンドはメッセージブローカーで待機します。デバイスがタイムアウト時間前にオンラインに戻り、コマンドリクエストトピックをサブスクライブしている場合、デバイスはコマンドを処理して結果をレスポンストピックに発行できます。タイムアウト時間より前にデバイスがオンラインに戻らない場合、コマンドの実行はタイムアウトし、ペイロードメッセージは期限切れになります。

4. コマンド実行を取得する

   デバイスで コマンドを実行したら、`GetCommandExecution`コントロールプレーン API オペレーションを使用して、コマンド実行の結果を取得してモニタリングします。API を使用して、最後に更新された日時、実行が完了した日時、指定されたパラメータなど、実行データに関する追加情報を取得することもできます。

   > **Note**
   >
   > 最新のステータス情報を取得するには、デバイスがコマンド実行結果をレスポンストピックに発行している必要があります。

   この API の使用に関する詳細と例については、「」を参照してください[コマンド実行の取得](#)。

(オプション) コマンド通知

コマンドイベントをサブスクライブして、コマンド実行のステータスが変更されたときに通知を受け取ることができます。次の手順では、コマンドイベントをサブスクライブして処理する方法を示します。

1. トピックルールを作成する

   コマンドイベントトピックをサブスクライブし、コマンド実行のステータスが変更されたときに通知を受け取ることができます。トピックルールを作成して、車両によって処理されたデータを AWS Lambda 関数などの他のアプリケーションにルーティングすることもできます。トピックルールは、 AWS IoT コンソールまたは`CreateTopicRule` AWS IoT Core コントロールプレーン API オペレーションを使用して作成できます。詳細については、「 および AWS IoT ルールの作成」を参照してください。

   この例では、 *<CommandID>*を通知を受信するコマンドの識別子*<CommandExecutionStatus>*に置き換え、 をコマンド実行のステータスに置き換えます。

```
$aws/events/commandExecution/<CommandID>/<CommandExecutionStatus>
```

   > **Note**
   > すべてのコマンドとコマンド実行ステータスの通知を受け取るには、ワイルドカード文字を使用して次のトピックにサブスクライブします。

```
$aws/events/commandExecution/+/#
```

2. コマンドイベントを受信して処理する

   前のステップでコマンドイベントをサブスクライブするトピックルールを作成した場合は、受信したコマンドプッシュ通知を管理できます。オプションで、作成したトピックルールを使用して、Amazon SQS AWS Lambda、Amazon SNS、 AWS Step Functions などのアプリケーションを構築することもできます。

次のコードは、受け取るコマンドイベント通知のサンプルペイロードを示しています。

```
{
    "executionId": "2bd65c51-4cfd-49e4-9310-d5cbfdbc8554",
    "status":"FAILED",
    "statusReason": {
         "reasonCode": "4",
         "reasonDescription": ""
    },
    "eventType": "COMMAND_EXECUTION",
```

```
    "commandArn":"arn:aws:iot:us-east-1:123456789012:command/0b9d9ddf-
e873-43a9-8e2c-9fe004a90086",
    "targetArn":"arn:aws:iot:us-east-1:123456789012:thing/5006c3fc-
de96-4def-8427-7eee36c6f2bd",
    "timestamp":1717708862107
}
```

コマンドの作成と管理

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

再利用可能なリモートアクションを設定するか、デバイスに 1 回限りの即時の指示を送信できます。この機能を使用すると、デバイスがほぼリアルタイムで実行できる手順を指定できます。コマンドを使用すると、ターゲット車両の再利用可能なリモートアクションを設定できます。コマンドを作成したら、特定の車両をターゲットとするコマンド実行を開始できます。

このトピックでは、 AWS IoT Core API または を使用してコマンドリソースを作成および管理する方法を示します AWS CLI。コマンドリソースで次のアクションを実行する方法を示します。

トピック

- コマンドリソースを作成する
- コマンドに関する情報を取得する
- アカウントのコマンドを一覧表示する
- コマンドリソースを更新または廃止する
- コマンドリソースを削除する

コマンドリソースを作成する

`CreateCommand` AWS IoT Core コントロールプレーン API オペレーションまたは AWS IoT FleetWise コンソールを使用して、コマンドを作成できます。

コマンドを作成する (コンソール)

AWS IoT FleetWise コンソールを使用してコマンドを作成できます。

コマンドを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、 コマンドを選択します。
3. コマンドの作成を選択します。
4. 車両で実行するコマンドを識別するのに役立つ一意のコマンド ID を指定します。
5. (オプション) オプションの表示名と説明を指定します。
6. (オプション) アクチュエータとデフォルトのパラメータ値を選択します。パラメータは、ターゲット車両がコマンドを受信したときに実行できるアクションを指定します。パラメータを追加しない場合は、 コマンドの実行時にパラメータを指定する必要があります。
7. コマンドのペイロードを生成するアクセス許可を付与する IAM ロールを選択します。「アクセスの制御」を参照してください。
8. コマンドの作成を選択します。

コマンドを作成する (AWS CLI)

次の例は、 パラメータを使用してコマンドを作成する方法を示しています。

コマンドを作成する際の考慮事項

でコマンドを作成する場合 AWS IoT FleetWise：

- 車両でコマンドを作成および実行するアクセス許可を付与`roleArn`する を指定する必要があります。KMS キーが有効な場合など、ポリシーの例の詳細については、「」を参照してください[を使用してコマンドのペイロードを生成する AWS IoT Device Management アクセス許可を付与する AWS IoT FleetWise](#)。
- 名前空間`AWS-IoT-FleetWise`として を指定する必要があります。
- 代わりに、 `mandatory-parameters`フィールドをスキップして実行時に指定できます。または、パラメータを使用してコマンドを作成し、オプションでデフォルト値を指定することもできます。デフォルト値を指定した場合、実行時にこれらの値を使用するか、独自の値を指定して上書きできます。これらのその他の例については、「」を参照してください[コマンドの使用シナリオ](#)。
- `mandatory-parameters` フィールドに最大 3 つの名前と値のペアを指定できます。ただし、車両で コマンドを実行する場合、1 つの名前と値のペアのみが受け入れられ、 `name`フィールドは`$actuatorPath.`プレフィックスで完全修飾名を使用する必要があります。

- *command-id* をコマンドの一意の識別子に置き換えます。UUID、英数字、「-」、「_」を使用できます。
- *role-arn* を、 などのコマンドを作成および実行するアクセス許可を付与する IAM ロールに置き換えます"arn:aws:iam:*accountId*:role/*FwCommandExecutionRole*"。
- （オプション）*display-name* をコマンドのわかりやすい名前に置き換え、 *description* をコマンドのわかりやすい説明に置き換えます。
- mandatory-parameters オブジェクト*###*と*##*、作成するコマンドの必要な情報に置き換えます。name フィールドは、 をプレフィックス$actuatorPath.とするシグナルカタログで定義されている完全修飾名です。たとえば、 nameは *$actuatorPath.Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringMode* にすることができ、*{"B": false}* のようなステアリングモードのステータスを示すブール値valueにすることができます。

```
aws iot create-command --command-id command-id \
    --role-arn role-arn \
    --description description \
    --display-name display-name \
    --namespace "AWS-IoT-FleetWise" \
    --mandatory-parameters '[
        {
            "name": name,
            "value": value
        }
   ]'
```

CreateCommand API オペレーションは、 コマンドの ID と ARN (Amazon リソースネーム) を含むレスポンスを返します。

```
{
    "commandId": "HandsOffSteeringMode",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/HandsOffSteeringMode"
}
```

コマンドに関する情報を取得する

GetCommand AWS IoT Core コントロールプレーン API オペレーションを使用して、コマンドリソースに関する情報を取得できます。

コマンドリソースに関する情報を取得するには、次のコマンドを実行します。*command-id* を、コマンドの作成時に使用された識別子に置き換えます。

```
aws iot get-command --command-id command-id
```

GetCommand API オペレーションは、次の情報を含むレスポンスを返します。

- コマンドの ID と ARN (Amazon リソースネーム) 。
- コマンドが作成され、最後に更新された日時。
- 車両で実行できるかどうかを示すコマンド状態。
- コマンドの作成時に指定したパラメータ。

```
{
    "commandId": "HandsOffSteeringMode",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/HandsOffSteeringMode"",
    "namespace": "AWS-IoT-FleetWise",
    "mandatoryParameters":[
        {
            "name":
 "$actuatorPath.Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringMode",
            "value": {"B": false }
        }
    ],
    "createdAt": "2024-03-23T11:24:14.919000-07:00",
    "lastUpdatedAt": "2024-03-23T11:24:14.919000-07:00",
    "deprecated": false,
    "pendingDeletion": false
}
```

アカウントのコマンドを一覧表示する

ListCommands AWS IoT Core コントロールプレーン API オペレーションを使用して、作成したアカウント内のすべてのコマンドを一覧表示できます。

アカウントのコマンドを一覧表示するには、次のコマンドを実行します。デフォルトでは、API は両方の名前空間用に作成されたコマンドを返します。リストをフィルタリングして、作成されたコマンドのみを表示するには AWS IoT FleetWise、次のコマンドを実行します。

> **Note**
> リストを昇順または降順にソートしたり、特定のコマンドパラメータ名を持つコマンドのみを表示するようにリストをフィルタリングしたりすることもできます。

```
aws iot list-commands --namespace "AWS-IoT-FleetWise"
```

`ListCommands` API オペレーションは、次の情報を含むレスポンスを返します。

- コマンドの ID と ARN (Amazon リソースネーム) 。
- コマンドが作成され、最後に更新された日時。
- コマンドを車両で実行できるかどうかを示すコマンド状態。

コマンドリソースを更新または廃止する

`UpdateCommand` AWS IoT Core コントロールプレーン API オペレーションまたは AWS IoT FleetWise コンソールを使用して、コマンドリソースを更新できます。コマンドの表示名と説明を更新できます。コマンドが現在使用されていない場合は、そのコマンドを非推奨にすることもできます。

> **Note**
> コマンドの実行時に使用する名前空間情報またはパラメータを変更することはできません。

コマンドを更新する (コンソール)

コマンドを更新する

コンソールからコマンドを更新するには、 AWS IoT FleetWise コンソールのコマンドページに移動し、次の手順を実行します。

1. 更新するコマンドを選択し、編集を選択します。
2. コマンドの詳細を編集し、変更の保存を選択します。

コマンドを非推奨にする

コンソールからコマンドを非推奨にするには、 AWS IoT FleetWise コンソールのコマンドページに移動し、次の手順を実行します。

1. 非推奨にするコマンドを選択し、非推奨を選択します。
2. 非推奨を確認し、非推奨を選択します。

コマンドを更新する (AWS CLI)

コマンドを更新する

コマンドリソースを更新するには、次のコマンドを実行します。*command-id* を更新したいコマンドの識別子に置き換え、更新された *display-name* と*##*を指定します。

```
aws iot update-command \
    --command-id command-id \
    --display-name display-name \
    --description description
```

`UpdateCommand` API オペレーションは次のレスポンスを返します。

```
{
    "commandId": "HandsOffSteeringMode",
    "deprecated": false,
    "lastUpdatedAt": "2024-05-09T23:16:51.370000-07:00"
}
```

コマンドを非推奨にする

コマンドを廃止するのは、デバイスへの使用を停止する場合や、古い場合です。次の例は、コマンドを非推奨にする方法を示しています。

```
aws iot update-command \
    --command-id command-id \
    --deprecated
```

`UpdateCommand` API オペレーションは、 コマンドの ID と ARN (Amazon リソースネーム) を含むレスポンスを返します。

```
{
    "commandId": "HandsOffSteeringMode",
```

```
    "deprecated": true,
    "lastUpdatedAt": "2024-05-09T23:16:51.370000-07:00"
}
```

コマンドが廃止されると、既存のコマンド実行は、終了するまで車両で実行され続けます。新しいコマンド実行を実行するには、 UpdateCommand API を使用してコマンドを復元し、使用可能にする必要があります。コマンドの廃止と復元に関する追加情報と考慮事項については、「 AWS IoT Core デベロッパーガイド」の「コマンドリソースの廃止」を参照してください。

コマンドリソースを削除する

DeleteCommand AWS IoT Core コントロールプレーン API オペレーションまたは AWS IoT FleetWise コンソールを使用して、コマンドリソースを削除できます。

> **Note**
>
> 削除の操作は永続的で、元には戻せません。コマンドはアカウントから完全に削除されます。

コマンドを削除する (コンソール)

コンソールからコマンドを削除するには、 AWS IoT FleetWise コンソールのコマンドページに移動し、次の手順を実行します。

1. 削除するコマンドを選択し、削除を選択します。
2. コマンドを削除することを確認し、削除を選択します。

コマンドを削除する (AWS CLI)

コマンドリソースを削除するには、次のコマンドを実行します。*command-id* を削除するコマンドの識別子に置き換えます。次の例は、コマンドリソースを削除する方法を示しています。

```
aws iot delete-command --command-id command-id
```

削除リクエストが成功した場合：

- コマンドが最大タイムアウトの 24 時間より長い期間廃止された場合、コマンドはすぐに削除され、HTTP statusCodeは 204 になります。

- コマンドが非推奨になっていないか、最大タイムアウトより短い期間非推奨になっている場合、コマンドは `pending deletion`状態になり、HTTP は 202 `statusCode` になります。コマンドは、最大タイムアウトの 24 時間後にアカウントから自動的に削除されます。

コマンド実行の開始とモニタリング

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

コマンドリソースを作成したら、ターゲット車両でコマンド実行を開始できます。車両がコマンドの実行を開始すると、コマンド実行の結果の更新を開始し、ステータスの更新と結果情報を MQTT 予約済みトピックに発行できます。その後、コマンド実行のステータスを取得し、アカウントの実行のステータスをモニタリングできます。

このトピックでは、 AWS CLI または AWS IoT FleetWise コンソールを使用して車両にコマンドを送信する方法について説明します。また、コマンド実行のステータスをモニタリングおよび更新する方法も示します。

トピック

- コマンド実行結果を更新する
- コマンド実行の取得
- アカウントのコマンド実行を一覧表示する
- コマンド実行を削除する

コマンドを送信する (コンソール)

コンソールからコマンドを送信するには、 AWS IoT FleetWise コンソールの車両ページに移動し、次の手順を実行します。

1. コマンドを送信する車両を選択します。
2. [Run command] を選択してください。
3. コマンド ID を選択します。
4. コマンド実行タイムアウトを指定し、コマンドの実行を選択します。

コマンドを送信する (AWS CLI)

StartCommandExecution AWS IoT データプレーン API オペレーションを使用して、車両にコマンドを送信できます。その後、車両はコマンドを自動車ミドルウェアサービス (SOME/IP (IP 経由のスケーラブルなサービス指向ミドルウェア) など) に転送するか、車両ネットワーク (コントローラーエリアネットワーク (CAN) デバイスインターフェイスなど) に発行します。次の例では AWS CLIを使用しています。

トピック

- コマンド送信時の考慮事項
- アカウント固有のデータプレーンエンドポイントを取得する
- コマンドの例を送信する

コマンド送信時の考慮事項

でコマンド実行を開始する場合 AWS IoT FleetWise：

- 車両に AWS IoT モノをプロビジョニングする必要があります。詳細については、「Provision AWS IoT FleetWise 車両」を参照してください。
- 名前空間AWS-IoT-FleetWiseとして を使用してコマンドを作成し、 AWS IoT FleetWise でコマンドを作成および実行するアクセス許可を付与role-Arnする を指定する必要があります。詳細については、「コマンドリソースを作成する」を参照してください。
- コマンドの作成時にパラメータに指定されたデフォルト値を使用する場合は、parametersフィールドをスキップできます。が作成時に指定mandatory-parametersされていない場合、またはパラメータに独自の値を指定してデフォルト値を上書きする場合は、parametersフィールドを指定する必要があります。これらのその他の例については、「」を参照してくださいコマンドの使用シナリオ。
- mandatory-parameters フィールドに最大 3 つの名前と値のペアを指定できます。ただし、車両で コマンドを実行する場合、1 つの名前と値のペアのみが受け入れられ、 nameフィールドは$actuatorPath.プレフィックスで完全修飾名を使用する必要があります。

アカウント固有のデータプレーンエンドポイントを取得する

API コマンドを実行する前に、エンドポイントのアカウント固有のiot:Jobsエンドポイント URL を取得する必要があります。たとえば、次のコマンドを実行するとします。

```
aws iot describe-endpoint --endpoint-type iot:Jobs
```

以下のレスポンスの例に示すように、アカウント固有のエンドポイント URL が返されます。

```
{
    "endpointAddress": "<account-specific-prefix>.jobs.iot.<region>.amazonaws.com"
}
```

コマンドの例を送信する

車両にコマンドを送信するには、次のコマンドを実行します。

- *command-arn* を、実行するコマンドの ARN に置き換えます。この情報は、 `create-command`CLI コマンドのレスポンスから取得できます。
- *target-arn* を、コマンドを実行するターゲットデバイスの ARN または AWS IoT モノに置き換えます。

> **Note**
>
> AWS IoT モノ (AWS IoT FleetWise 車両) のターゲット ARN を指定できます。モノのグループとフリートは現在サポートされていません。

- *endpoint-url* を、 で取得したアカウント固有のエンドポイントに置き換えます。`https://`たとえばアカウント固有のデータプレーンエンドポイントを取得する、 というプレフィックスが付きます`https://`*`123456789012abcd`*`.jobs.iot.`*`ap-south-1`*`.amazonaws.com`。
- name と *value* を、 CLI `create-command` を使用してコマンドを作成したときに指定した `mandatory-parameters`フィールドに置き換えます。

  name フィールドは、 をプレフィックス`$actuatorPath.`とするシグナルカタログで定義されている完全修飾名です。たとえば、 nameは *`$actuatorPath.Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringMode`* にすることができ、*`{"B": false}`* のようなステアリングモードのステータスを示すブール値`value`にすることができます。
- (オプション) 追加のパラメータ を指定することもできます`executionTimeoutSeconds`。このオプションのフィールドは、デバイスが実行結果で応答する必要がある時間を秒単位で指定します。タイムアウトは 24 時間の最大値に設定できます。

コマンド実行が作成されると、タイマーが開始されます。タイマーの有効期限が切れる前に、コマンドの実行ステータスが SUCCEEDEDや などの終了ステータスに変わらない場合FAILED、ステータスは自動的に に変わりますTIMED_OUT。

> **Note**
>
> デバイスはTIMED_OUTステータスを報告したり、このステータスを SUCCEEDED、、FAILEDなどのステータスに上書きしたりすることもできREJECTED、コマンドの実行はターミナルになります。詳細については、「コマンド実行のタイムアウトステータス」を参照してください。

```
aws iot-jobs-data start-command-execution \
    --command-arn command-arn \
    --target-arn target-arn \
    --execution-timeout-seconds 30 \
    --endpoint-url endpoint-url \
    --parameters '[
        {
            "name": name,
            "value": value
        }
   ]'
```

StartCommandExecution API オペレーションは、コマンド実行 ID を返します。この ID を使用して、コマンド実行ステータス、詳細、およびコマンド実行履歴をクエリできます。

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542"
 }
```

コマンドを実行すると、デバイスは以下の情報を含む通知を受け取ります。issued_timestamp_ms フィールドは、StartCommandExecutionAPI が呼び出された時刻に対応します。は、 StartCommandExecution API を呼び出すときに executionTimeoutSecondsパラメータを使用して設定されたタイムアウト値timeout_msに対応します。

```
timeout_ms: 9000000
```

```
issued_timestamp_ms: 1723847831317
```

コマンド実行結果を更新する

コマンド実行のステータスを更新するには、デバイスが MQTT 接続を確立し、次のコマンドリクエストトピックをサブスクライブしている必要があります。

この例では、 をターゲットデバイスの一意の識別子<device-id>、 VehicleIdまたはモノの名前、 をコマンド実行の識別子<execution-id>に置き換えます。

> **Note**
>
> - ペイロードは protobuf 形式を使用する必要があります。
> - デバイスが /acceptedおよび /rejectedレスポンストピックをサブスクライブすることはオプションです。デバイスが明示的にサブスクライブしていない場合でも、これらのレスポンスメッセージを受信します。

```
// Request topic
$aws/devices/<DeviceID>/command_executions/+/request/protobuf

// Response topics (Optional)
$aws/devices/<DeviceID>/command_executions/<ExecutionId>/response/accepted/protobuf
$aws/devices/<DeviceID>/command_executions/<ExecutionId>/response/rejected/protobuf
```

デバイスは、コマンドレスポンストピックにメッセージを発行できます。コマンドを処理すると、protobuf でエンコードされたレスポンスがこのトピックに送信されます。<DeviceID> フィールドは、リクエストトピックの対応するフィールドと一致する必要があります。

```
$aws/devices/<DeviceID>/command_executions/<ExecutionId>/response/<PayloadFormat>
```

デバイスがこのトピックへのレスポンスを発行したら、 GetCommandExecution API を使用して更新されたステータス情報を取得できます。コマンド実行のステータスは、ここにリストされているもののいずれかになります。

- IN_PROGRESS
- SUCCEEDED

- FAILED
- REJECTED
- TIMED_OUT

ステータス SUCCEEDED、、 FAILEDのいずれかのコマンド実行REJECTEDはターミナルであり、ステータスはデバイスによって報告されることに注意してください。コマンド実行がターミナルの場合、ステータスや関連フィールドはそれ以上更新されません。TIMED_OUT ステータスは、デバイスまたはクラウドによって報告される場合があります。クラウドから報告された場合、後でデバイスによってステータス理由フィールドの更新が行われることがあります。

例えば、デバイスが発行する MQTT メッセージの例を次に示します。

> **Note**
>
> コマンド実行ステータスについて、デバイスが statusReason オブジェクトを使用してステータス情報を公開する場合は、以下を確認する必要があります。
>
> - はパターン reasonCodeを使用し[A-Z0-9_-]+、64 文字を超えないようにします。
> - の長さreasonDescriptionは 1,024 文字以下です。新しい行などのコントロール文字を除く任意の文字を使用できます。

```
{
    "deviceId": "",
    "executionId": "",
    "status": "CREATED",
    "statusReason": {
        "reasonCode": "",
        "reasonDescription": ""
    }
}
```

AWS IoT Core MQTT テストクライアントを使用してトピックをサブスクライブし、コマンド実行メッセージを表示する方法を示す例については、 デAWS IoT Core ベロッパーガイドの「MQTT テストクライアントを使用したコマンドの更新の表示」を参照してください。

コマンド実行の取得

GetCommandExecution AWS IoT コントロールプレーン API オペレーションを使用して、コマンド実行に関する情報を取得できます。StartCommandExecution API オペレーションを使用してこのコマンドをすでに実行している必要があります。

実行されたコマンドのメタデータを取得するには、次のコマンドを実行します。

- *execution-id* を コマンドの ID に置き換えます。この情報は、 start-command-executionCLI コマンドのレスポンスから取得できます。
- *target-arn* を、コマンドを実行するターゲット車両の ARN または AWS IoT モノに置き換えます。

```
aws iot get-command-execution --execution-id execution-id \
    --target-arn target-arn
```

GetCommandExecution API オペレーションは、コマンド実行の ARN、実行ステータス、コマンドの実行開始時刻と完了時刻に関する情報を含むレスポンスを返します。次のコードは、API リクエストからのレスポンスの例を示しています。

各コマンド実行のステータスに関する追加のコンテキストを提供するために、 コマンド機能は statusReason オブジェクトを提供します。オブジェクトには、 reasonCodeと の 2 つのフィールドが含まれていますreasonDescription。これらのフィールドを使用すると、デバイスはコマンド実行のステータスに関する追加情報を提供できます。この情報は、クラウドから報告されたデフォルトの reasonDescription reasonCodeと を上書きします。

この情報を報告するために、デバイスは更新されたステータス情報をクラウドに発行できます。次に、 GetCommandExecution API を使用してコマンド実行ステータスを取得すると、最新のステータスコードが表示されます。

> **Note**
>
> 実行レスポンスの completedAtフィールドは、デバイスがターミナルステータスをクラウドにレポートする時間に対応します。TIMED_OUT ステータスの場合、このフィールドはデバイスがタイムアウトを報告したときにのみ設定されます。TIMED_OUT ステータスがクラウドによって設定されている場合、TIMED_OUTステータスは更新されません。タイムアウト動作の詳細については、「」を参照してくださいコマンド実行のタイムアウトステータス。

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/LockDoor",
    "targetArn": "arn:aws:iot:ap-south-1:123456789012:thing/myFrontDoor",
    "status": "SUCCEEDED",
    "statusReason": {
        "reasonCode": "65536",
        "reasonDescription": "SUCCESS"
    },
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "completedAt": "2024-03-23T00:50:10.095000-07:00",
    "Parameters": '{
         "$actuatorPath.Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringMode":

         { "B": true }
    }'
}
```

アカウントのコマンド実行を一覧表示する

ListCommandExecutions AWS IoT Core コントロールプレーンの HTTP API オペレーションを使用して、アカウント内のすべてのコマンド実行を一覧表示します。この例では、 AWS CLIを使用します。

トピック

- コマンド実行を一覧表示する際の考慮事項
- コマンド実行を一覧表示する例

コマンド実行を一覧表示する際の考慮事項

ListCommandExecutions API を使用する際の考慮事項を以下に示します。

- 特定のコマンドtargetArnまたはターゲット車両の実行を一覧表示するかどうかcommandArnに応じて、少なくとも または を指定する必要があります。API リクエストを空にしたり、同じリクエストに両方のフィールドを含めることはできません。
- startedTimeFilter または completedTimeFilter情報のみを指定する必要があります。API リクエストを空にしたり、同じリクエストに両方のフィールドを含めることはできません。オブジェクトの beforeおよび afterフィールドを使用して、特定の期間内に作成または完了したコマンド実行を一覧表示できます。

- フィールドbeforeと afterフィールドの両方を現在の時刻より大きくすることはできません。デフォルトでは、値を指定しない場合、 beforeフィールドは現在の時刻、 afterフィールドは現在の時刻 - 6 か月です。つまり、使用するフィルターに応じて、API は過去 6 か月以内に作成または完了したすべての実行を一覧表示します。
- sort-order パラメータを使用して、実行を昇順で一覧表示するかどうかを指定できます。デフォルトでは、このフィールドを指定しない場合、実行は降順で表示されます。
- コマンド ARN のコマンド実行を一覧表示するときに、ステータスに基づいてコマンド実行をフィルタリングすることはできません。

コマンド実行を一覧表示する例

次の例は、 でコマンド実行を一覧表示する方法を示しています AWS アカウント。

コマンドを実行するときは、リストをフィルタリングして、 を使用して特定のデバイス用に作成されたコマンド実行のみを表示するかtargetArn、 を使用して指定された特定のコマンドの実行のみを表示するかを指定する必要がありますcommandArn。

この例では、次のように置き換えます。

- *<target-arn>* は、 など、実行をターゲットとするデバイスの Amazon リソースナンバー (ARN) を使用しますarn:aws:iot:*us-east-1*:*123456789012*:thing/*b8e4157c98f332cffb37627f*。
- *<target-arn>* は、 など、実行をターゲットとするデバイスの Amazon リソースナンバー (ARN) を使用しますarn:aws:iot:*us-east-1*:*123456789012*:thing/*b8e4157c98f332cffb37627f*。
- *<after>* は、作成された実行を一覧表示する時間です。たとえば、 ですAssert 2024-11-01T03:00。

```
aws iot list-command-executions \
--target-arn <target-arn> \
--started-time-filter '{after=<after>}' \
--sort-order "ASCENDING"
```

このコマンドを実行すると、作成したコマンド実行のリスト、実行の開始時刻、完了時刻を含むレスポンスが生成されます。また、ステータス情報と、ステータスに関する追加情報を含む statusReason オブジェクトも提供します。

```
{
```

```
    "commandExecutions": [
        {
            "commandArn": "arn:aws:iot:us-east-1:123456789012:command/TestMe002",
            "executionId": "b2b654ca-1a71-427f-9669-e74ae9d92d24",
            "targetArn": "arn:aws:iot:us-east-1:123456789012:thing/
b8e4157c98f332cffb37627f",
            "status": "TIMED_OUT",
            "createdAt": "2024-11-24T14:39:25.791000-08:00",
            "startedAt": "2024-11-24T14:39:25.791000-08:00"
        },
        {
            "commandArn": "arn:aws:iot:us-east-1:123456789012:command/TestMe002",
            "executionId": "34bf015f-ef0f-4453-acd0-9cca2d42a48f",
            "targetArn": "arn:aws:iot:us-east-1:123456789012:thing/
b8e4157c98f332cffb37627f",
            "status": "IN_PROGRESS",
            "createdAt": "2024-11-24T14:05:36.021000-08:00",
            "startedAt": "2024-11-24T14:05:36.021000-08:00"
        }
    ]
}
```

コマンド実行を削除する

コマンド実行が不要になった場合は、アカウントから完全に削除できます。

> **Note**
>
> コマンド実行は、、、 SUCCEEDED FAILEDなどのターミナルステータスになった場合にのみ削除できますREJECTED。

次の例は、 コマンドを使用してdelete-command-execution AWS CLI コマンド実行を削除する方法を示しています。を削除するコマンド実行の識別子*<execution-id>*に置き換えます。

```
aws iot delete-command-execution --execution-id <execution-id>
```

API リクエストが成功すると、コマンド実行は 200 のステータスコードを生成します。GetCommandExecution API を使用して、コマンド実行がアカウントに存在しなくなったことを確認できます。

例: コマンドを使用して車両のステアリングモードを制御する (AWS CLI)

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

次の例は、 を使用して コマンド機能を使用する方法を示しています AWS CLI。この例では、 AWS IoT FleetWise 車両をターゲットデバイスとして使用して、ステアリングモードをリモートで制御するコマンドを送信する方法を示します。

トピック

- 車両ステアリングモードの概要の例
- 前提条件
- リモートコマンドを使用するための IAM ポリシー
- AWS IoT コマンドを実行する (AWS CLI)
- クリーンアップ

車両ステアリングモードの概要の例

この例では、次の操作を行います。

1. を使用して オペレーションのコマンドリソースを作成し`create-command` AWS CLI 、車両のステアリングモードを変更します。
2. を使用して、コマンドが作成された時刻や最後に更新された時刻など、コマンドに関する情報を取得します`get-command` AWS CLI。
3. `start-command-execution` AWS CLI ステアリングモードを必須パラメータとする を使用して、 コマンドを車両に送信します。このパラメータはデバイスで実行されます。
4. を使用してコマンド実行の結果を取得します`get-command-execution` AWS CLI。実行が完了した日時を確認し、実行結果やコマンドの実行完了にかかった時間などの追加の詳細を取得できます。
5. 使用しなくなったコマンドとコマンド実行を削除して、クリーンアップアクティビティを実行します。

前提条件

この例を実行する前に、以下を実行します。

- 車両を AWS IoT レジストリの AWS IoT モノ AWS IoT FleetWise としてプロビジョニングします。また、モノに証明書を追加してアクティブ化し、モノにポリシーをアタッチする必要があります。その後、デバイスはクラウドに接続し、コマンドを実行できます。詳細については、「車両のプロビジョニング」を参照してください。
- 「」に示すように、 コマンドを使用して API オペレーションを実行するアクセス許可を付与する IAM ユーザーと IAM ポリシーを作成しますリモートコマンドを使用するための IAM ポリシー。

リモートコマンドを使用するための IAM ポリシー

次の表は、 コマンド機能のすべてのコントロールプレーンおよびデータプレーン API オペレーションへのアクセスを許可する IAM ポリシーの例を示しています。アプリケーションのユーザーは、表に示すように、すべてのリモートコマンド API オペレーションを実行するアクセス許可を持ちます。

API オペレーション

API アクション	コントロール/データプレーン	プロトコル	説明	リソース
`CreateCommand`	コントロールプレーン	HTTP	コマンドリソースを作成します。	• コマンド
`GetCommand`	コントロールプレーン	HTTP	コマンドに関する情報を取得します。	• コマンド
`UpdateCommand`	コントロールプレーン	HTTP	コマンドまたは に関する情報を更新して非推奨にします	• コマンド
`ListCommands`	コントロールプレーン	HTTP	アカウントのコマンドを一覧表示します	• コマンド
`DeleteCommand`	コントロールプレーン	HTTP	コマンドを削除します。	• コマンド

API アクション	コントロール/データプレーン	プロトコル	説明	リソース
`StartCommandExecution`	データプレーン	HTTP	コマンドの実行を開始します	• コマンド • thing
`UpdateCommandExecution`	データプレーン	MQTT	コマンド実行を更新する	• コマンド • thing
`GetCommandExecution`	コントロールプレーン	HTTP	コマンド実行に関する情報を取得します。	• コマンド • thing
`ListCommandExecutions`	コントロールプレーン	HTTP	アカウントのコマンド実行を一覧表示します	• コマンド • thing
`DeleteCommandExecution`	コントロールプレーン	HTTP	コマンド実行を削除します。	• コマンド • thing

この例では、次のように置き換えます。

- *region* など AWS リージョン、 で を使用します`ap-south-1`。
- *account-id* は、 などの 番号に置き換えます AWS アカウント `57EXAMPLE833`。
- *command-id*、*command-id1*、 など、一意のコマンド識別子*command-id2*を持つ `LockDoor` `TurnOffAC`。
- *thing-name* などの AWS IoT モノの名前を指定します`my_car`。

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

```
            "iot:CreateCommand",
            "iot:GetCommand",
            "iot:ListCommands",
            "iot:UpdateCommand",
            "iot:DeleteCommand"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:iot:<region>:<account-id>:command/command-id1",
            "arn:aws:iot:<region>:<account-id>:command/command-id2",
        ]
    },
    {
        "Action": [
            "iot:GetCommandExecution",
            "iot:ListCommandExecutions",
            "iot:DeleteCommandExecution"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:iot:<region>:<account-id>:command/command-id",
            "arn:aws:iot:<region>:<account-id>:thing/thing-name",
        ]
    },
    {
        "Action": "iot:StartCommandExecution",
        "Effect": "Allow",
        "Resource": [
            "arn:aws:iot:<region>:<account-id>:command/command-id",
            "arn:aws:iot:<region>:<account-id>:thing/thing-name",
        ]
    }
  ]
}
```

AWS IoT コマンドを実行する (AWS CLI)

以下は、 を使用してコマンドオペレーション AWS CLI を実行し、車両のステアリングモードを変更する方法を示しています。

1. ステアリングモードオペレーションのコマンドリソースを作成する

   create-command CLI を使用して、デバイスに送信するコマンドを作成します。この例では、以下を指定します。

   - *TurnOffSteeringMode* としての command-id
   - role-arn として "arn:aws:iam:*accountId*:role/*FwCommandExecutionRole*" を指定role-arnする必要があります。これは、車両でコマンドを作成および実行するアクセス許可を付与する IAM ロールであるためです。詳細については、「を使用してコマンドのペイロードを生成する AWS IoT Device Management アクセス許可を付与する AWS IoT FleetWise」を参照してください。
   - display-name *Turn off steering mode*「」として
   - namespace は である必要があります AWS-IoT-FleetWise
   - mandatory-parameters を「$actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringModename」とし、defaultValue を「$actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringMode」とする名前と値のペア*actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringMode*
     { "S": "true" }

   > **Note**
   > 必須パラメータを指定せずにコマンドを作成することもできます。次に、start-command-executionCLI を使用してコマンドを実行するときに使用するパラメータを指定する必要があります。例については、コマンドの使用シナリオを参照してください。

   > **Important**
   > AWS-IoT-FleetWise 名前空間を使用する場合は、 の一部として指定された Nameフィールドが $actuatorPath. プレフィックスmandatory-parametersを使用し、 Valueフィールドが文字列データ型を使用していることを確認する必要があります。

```
aws iot create-command \
    --command-id TurnOffSteeringMode \
    --role-arn "arn:aws:iam:accountId:role/FwCommandExecutionRole" \
    --display-name "Turn off steering mode" \
    --namespace AWS-IoT-FleetWise \
    --mandatory-parameters '[
      {
        "name": "$actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringMode",
        "defaultValue": { "S": "true" }
      }
    ]'
```

次の出力は、 CLI からのレスポンスの例を示しています。ここで、 `ap-south-1` と `123456789012`は AWS リージョン および AWS アカウント ID の例です。

```
{
    "commandId": "TurnOffSteeringMode",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/TurnOffSteeringMode"
}
```

このコマンドを使用するその他の例については、「」を参照してください[コマンドリソースを作成する](#)。

2. コマンドに関する情報を取得する

次のコマンドを実行して、コマンドに関する情報を取得します。ここで、 `command-id`は、上記の `create-command`オペレーションの出力のコマンド ID です。

> **Note**
>
> 複数のコマンドを作成する場合は、 `ListCommands` API を使用してアカウント内のすべてのコマンドを一覧表示し、 `GetCommand` API を使用して特定のコマンドに関する追加情報を取得できます。詳細については、「[アカウントのコマンドを一覧表示する](#)」を参照してください。

```
aws iot get-command --command-id TurnOffSteeringMode
```

このコマンドを実行すると、次のレスポンスが生成されます。コマンドが作成された時刻と最後に更新された時刻、指定したパラメータ、およびコマンドがデバイスで実行できるかどうかが表示されます。

```
{
    "commandId": "TurnOffSteeringMode",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/
TurnOffSteeringMode",
    "namespace": "AWS-IoT-FleetWise",
    "mandatoryParameters":[
        {
            "name":
 "$actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringMode",
            "defaultValue": {"S": "true" }
        }
    ],
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "lastUpdatedAt": "2024-03-23T00:50:10.095000-07:00",
    "deprecated": false
}
```

このコマンドを使用するその他の例については、「」を参照してください[コマンドに関する情報を取得する](#)。

3. コマンド実行を開始する

次のコマンドを実行してコマンドの実行を開始します。ここで、 `command-arn`は上記の `get-command`オペレーションの出力のコマンド ARN です。`target-arn` は、 コマンドを実行するターゲットデバイスの ARN です。たとえば、 です*`myVehicle`*。

この例では、コマンドの作成時にパラメータにデフォルト値を指定しているため、CLI `start-command-execution` はコマンドの実行時にこれらの値を使用できます。CLI の使用時にパラメータに別の値を指定することで、デフォルト値を上書きすることもできます。

```
aws iot-data start-command-execution \
    --command-arn arn:aws:iot:ap-south-1:123456789012:command/TurnOffSteeringMode \
    --target-arn arn:aws:iot:ap-south-1:123456789012:thing/myVehicle
```

このコマンドを実行すると、コマンド実行 ID が返されます。この ID を使用して、コマンド実行ステータス、詳細、およびコマンド実行履歴をクエリできます。

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542"
}
```

CLI の使用に関するその他の例については、「」を参照してください[コマンドを送信する (AWS CLI)](#)。

4. コマンド実行に関する情報を取得する

次のコマンドを実行して、ターゲットデバイスで実行したコマンドに関する情報を取得します。上から`start-command-execution`操作の出力として`execution-id`取得した と、ターゲットとするデバイスの ARN `target-arn`である を指定します。

> **Note**
>
> - 最新のステータス情報を取得するには、デバイスが MQTT API を使用するコマンドの `UpdateCommandExecution` MQTT 予約レスポンストピックに更新されたステータス情報を公開している必要があります。詳細については、「[コマンド実行結果を更新する](#)」を参照してください。
> - 複数のコマンド実行を開始する場合は、 `ListCommandExecutions` API を使用してアカウント内のすべてのコマンド実行を一覧表示し、 `GetCommandExecution` API を使用して特定の実行に関する追加情報を取得できます。詳細については、「[アカウントのコマンド実行を一覧表示する](#)」を参照してください。

```
aws iot get-command-execution \
    --execution-id <"07e4b780-7eca-4ffd-b772-b76358da5542"> \
    --target-arn arn:aws:iot:<region>:<account>:thing/myVehicle
```

このコマンドを実行すると、コマンドの実行、実行ステータス、実行を開始した時刻、完了時刻に関する情報が返されます。たとえば、次のレスポンスは、ターゲットデバイスでコマンドの実行が成功し、ステアリングモードがオフになったことを示しています。

```
{
    "executionId": "07e4b780-7eca-4ffd-b772-b76358da5542",
    "commandArn": "arn:aws:iot:ap-south-1:123456789012:command/
TurnOffSteeringMode",
```

```
    "targetArn": "arn:aws:iot:ap-south-1:123456789012:thing/myVehicle",
    "result": "SUCCEEDED",
     "statusReason": {
        "reasonCode": "65536",
        "reasonDescription": "SUCCESS"
    },
    "result": {
        "KeyName": {
            "S": "",
            "B": true,
            "BIN": null
        }
    },
    "createdAt": "2024-03-23T00:50:10.095000-07:00",
    "completedAt": "2024-03-23T00:50:10.095000-07:00",
    "parameters": '{
         "$actuatorPath.Vehicle.Chassis.SteeringWheel.TurnOffSteeringMode":
         { "S": "true" }
    }'
}
```

クリーンアップ

コマンドを作成してデバイスで実行したので、このコマンドを使用する予定がない場合は、削除できます。進行中の保留中のコマンド実行は、削除リクエストの影響を受けずに引き続き実行されます。

> **Note**
>
> または、コマンドが古く、後でターゲットデバイスで実行する必要がある場合は、そのコマンドを非推奨にすることもできます。

1. (オプション) コマンドリソースを非推奨にする

   次のコマンドを実行してコマンドを非推奨にします。ここで、 `command-id`は、上記の `get-command`オペレーションの出力のコマンド ID です。

```
aws iot update-command \
   --command-id TurnOffSteeringMode \
   --deprecated
```

このコマンドを実行すると、コマンドが廃止されたことを示す出力が返されます。CLI を使用してコマンドを復元することもできます。

> **Note**
>
> update-command CLI を使用して、コマンドの表示名と説明を更新することもできます。詳細については、「コマンドリソースを更新または廃止する」を参照してください。

```
{
    "commandId": "TurnOffSteeringMode",
    "deprecated": true,
    "lastUpdatedAt": "2024-05-09T23:16:51.370000-07:00"
}
```

2. コマンドを削除する

   次のコマンドを実行して、 で指定されたコマンドを削除しますcommand-id。

   > **Note**
   >
   > 削除アクションは永続的であり、元に戻すことはできません。

   ```
   aws iot delete-command --command-id TurnOffSteeringMode
   ```

   削除リクエストが成功すると、コマンドを非推奨にしたか、いつ非推奨にしたかに応じて、HTTP statusCodeが 202 または 204 になります。詳細と例については、「コマンドリソースを削除する」を参照してください。

   get-command CLI を使用して、コマンドがアカウントから削除されたことを確認できます。

3. (オプション) コマンド実行を削除する

   デフォルトでは、すべてのコマンド実行は、作成日から 6 か月以内に削除されます。この情報は、 GetCommandExecution API の timeToLiveパラメータを使用して表示できます。

または、実行ステータスが 、、または のいずれかである場合などSUCCEEDEDFAILED、コマンド実行がターミナルになった場合はREJECTED、コマンド実行を削除できます。次のコマンドを実行して実行を削除します。ここで、 execution-idは上記の get-command-executionオペレーションの出力にある実行 ID です。

```
aws iot delete-command-execution \
            --execution-id "07e4b780-7eca-4ffd-b772-b76358da5542"
```

get-command-execution CLI を使用して、コマンド実行がアカウントから削除されたことを確認できます。

コマンドの使用シナリオ

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

コマンド機能を使用する場合、以下のシナリオでコマンドを作成して実行できます。

- 作成時にパラメータを省略し、コマンド ID のみを指定できます。この場合、ターゲットデバイスで コマンドを実行するときに使用するパラメータを指定する必要があります。
- 1 つ以上のパラメータを指定し、コマンドの作成時にデフォルト値を設定できます。デフォルト値を指定すると、不正確なコマンドの送信を防ぐことができます。
- 1 つ以上のパラメータを指定し、コマンドの作成時にそれらの値を設定できます。複数のパラメータを指定できますが、そのうちの 1 つのみが実行されます。このパラメータの Nameフィールドは $actuatorPathプレフィックスを使用する必要があります。

このセクションでは、 CreateCommandおよび StartCommandExecution API の使用シナリオと、 パラメータの使用シナリオについて説明します。また、状態テンプレートでコマンドを使用する例をいくつか示します。

トピック

- パラメータなしでコマンドを作成する

- パラメータのデフォルト値を使用したコマンドの作成
- パラメータ値を使用したコマンドの作成
- 状態テンプレートでのコマンドの使用

パラメータなしでコマンドを作成する

次のユースケースは、 `CreateCommand` API または CLI `create-command` を使用してパラメータなしでコマンドを作成する方法を示しています。コマンドを作成するときは、コマンド ID とロール ARN のみを指定する必要があります。

このユースケースは、同じコマンドを車両に複数回送信する場合など、繰り返し発生するユースケースで特に役立ちます。この場合、コマンドは特定のアクチュエータに関連付けられておらず、任意のアクチュエータでコマンドを柔軟に実行できます。`StartCommandExecution` API または CLI `start-command-execution` を使用してコマンドを実行する場合は、代わりに実行時にパラメータを指定する必要があります。これには、アクチュエータと物理信号値が含まれます。

`mandatory-parameters` 入力なしでコマンドを作成する

このユースケースは、必須パラメータを入力せずにコマンドを作成する方法を示しています。

```
aws iot create-command \
    --command-id "UserJourney1" \
    --role-arn "arn:aws:iam:accountId:role/FwCommandExecutionRole" \
    --description "UserJourney1 - No mandatory parameters" \
    --namespace "AWS-IoT-FleetWise"
```

`mandatory-parameters` 入力なしで作成されたコマンドの実行

この最初の例では、上記のコマンドを使用して、制限なしで任意のアクチュエータでコマンドを実行できます。を 10 の値`actuator1`に設定するには、以下を実行します。

```
aws iot-jobs-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/UserJourney1 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/target-vehicle \
    --parameters '{
        "$actuatorPath.Vehicle.actuator1": {"S": "10"}
    }'
```

同様に、 を の値`actuator3`に設定するコマンドを実行できます`true`。

```
aws iot-jobs-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/UserJourney1 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/target-vehicle \
    --parameters '{
        "$actuatorPath.Vehicle.actuator3": {"S": "true"}
    }'
```

パラメータのデフォルト値を使用したコマンドの作成

このコマンドでは、指定されたアクチュエータに対してのみコマンドを実行できます。デフォルト値を指定すると、不正確なコマンドの送信を防ぐことができます。たとえば、ドアをロックおよびロック解除するLockDoorコマンドをデフォルト値で設定して、コマンドが誤ってドアをロック解除しないようにできます。

このユースケースは、同じコマンドを複数回送信し、車両のドアのロックやロック解除など、同じアクチュエータに対して異なるアクションを実行する場合に特に便利です。アクチュエータをデフォルト値に設定する場合は、qny を `start-command-execution` CLI `parameters`に渡す必要はありません。`start-command-execution` CLI `parameters`で に別の値を指定すると、デフォルト値が上書きされます。

のデフォルト値を使用したコマンドの作成 **mandatory-parameters**

次のコマンドは、アクチュエータ 1 のデフォルト値を指定する方法を示しています。

```
aws iot create-command \
    --command-id "UserJourney2" \
    --namespace "AWS-IoT-FleetWise" \
    --role-arn "arn:aws:iam:accountId:role/FwCommandExecutionRole" \
    --mandatory-parameters '[
        {
            "name": "$actuatorPath.Vehicle.actuator1",
            "defaultValue": {"S": "0"}
        }
    ]'
```

のデフォルト値で作成されたコマンドの実行 **mandatory-parameters**

コマンドUserJourney2を使用すると、実行時に入力値を渡すことなくコマンドを実行できます。この場合、実行時の実行では、作成時に指定されたデフォルト値が使用されます。

```
aws iot-data start-command-execution \
```

```
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/UserJourney3 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/target-vehicle
```

ランタイム中に同じアクチュエーターであるアクチュエーター 1 に別の値を渡すこともできます。これにより、デフォルト値が上書きされます。

```
aws iot-jobs-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/UserJourney3 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/target-vehicle \
    --parameters '{
        "$actuatorPath.Vehicle.actuator1": {"S": "139"}
    }'
```

パラメータ値を使用したコマンドの作成

このコマンドでは、指定されたアクチュエータに対してのみコマンドを実行できます。また、ランタイム中にアクチュエータの値を設定する必要もあります。

このユースケースは、エンドユーザーが車両でアクチュエータを実行するときに、一部のアクチュエータに対して特定の指定されたアクションのみを実行できるようにする場合に特に便利です。

> **Note**
>
> `mandatory-parameters` 入力には 個以上の名前と値のペアがあり、一部またはすべてのデフォルト値を使用できます。実行時に、アクチュエータでの実行時に使用するパラメータを決定できます。ただし、アクチュエータ名に `$actuatorPath.`プレフィックスが付いた完全修飾名が使用されている場合です。

のデフォルト値を使用しないコマンドの作成 **mandatory-parameters**

このコマンドでは、指定されたアクチュエータに対してのみコマンドを実行できます。また、ランタイム中にアクチュエータの値を設定する必要もあります。

```
aws iot create-command \
    --command-id "UserJourney2" \
    --namespace "AWS-IoT-FleetWise" \
    --role-arn "arn:aws:iam:accountId:role/FwCommandExecutionRole" \
    --mandatory-parameters '[
        {
```

```
            "name": "$actuatorPath.Vehicle.actuator1"
        }
    ]'
```

のデフォルト値なしで作成されたコマンドの実行 **mandatory-parameters**

コマンドを実行する場合、この場合は actuator1 の値を指定する必要があります。以下に示すコマンドを実行すると、 の値が `actuator1`に正常に設定されます`10`。

```
aws iot-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/UserJourney2 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/target-vehicle \
    --parameters '{
        "$actuatorPath.Vehicle.actuator1": {"S": "10"}
    }'
```

状態テンプレートでのコマンドの使用

コマンド API オペレーションを使用して、状態データの収集と処理を行うこともできます。たとえば、ワンタイム状態スナップショットを取得したり、状態テンプレートをアクティブ化または非アクティブ化して、車両状態データの収集を開始または停止したりできます。次の例は、 状態テンプレートで コマンド機能を使用する方法を示しています。詳細については、データ収集と処理のためのステートテンプレートオペレーションを参照してください。

> **Note**
>
> `mandatory-parameters` 入力の一部として指定する名前フィールドには、`$stateTemplate` プレフィックスを使用する必要があります。

例 1: デフォルト値を使用して状態テンプレートのコマンドを作成する

この例では、 CLI `create-command` を使用して状態テンプレートをアクティブ化する方法を示します。

```
aws iot create-command \
    --command-id <COMMAND_ID> \
    --display-name "Activate State Template" \
    --namespace AWS-IoT-FleetWise \
    --mandatory-parameters '[
```

```
      {
          "name": "$stateTemplate.name"
      },
      {
          "name": "$stateTemplate.operation",
          "defaultValue": {"S": "activate"}
      }
    ]'
```

同様に、次のコマンドは、状態テンプレートに `start-command-execution` CLI を使用する方法の例を示しています。

```
aws iot-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/<COMMAND_ID> \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME> \
    --parameters '{
       "$stateTemplate.name": {"S": "ST345"}
    }'
```

例 2: デフォルト値なしで状態テンプレートのコマンドを作成する

次のコマンドは、パラメータのデフォルト値なしで複数の状態テンプレートを作成します。これにより、これらのパラメータとその値を使用して コマンドを強制的に実行できます。

```
aws iot create-command \
    --command-id <COMMAND_ID> \
    --display-name "Activate State Template" \
    --namespace AWS-IoT-FleetWise \
    --mandatory-parameters '[
      {
          "name": "$stateTemplate.name",
          "defaultValue": {"S": "ST123"}
      },
      {
          "name": "$stateTemplate.operation",
          "defaultValue": {"S": "activate"}
      },
      {
          "name": "$stateTemplate.deactivateAfterSeconds",
          "defaultValue": {"L": "120"}
      }
    ]'
```

次のコマンドは、上記の例で `start-command-execution` CLI を使用する方法を示しています。

```
aws iot-data start-command-execution \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/<COMMAND_ID> \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME> \
    --parameters '{
        "$stateTemplate.name": {"S": "ST345"},
        "$stateTemplate.operation": {"S": "activate"},
        "$stateTemplate.deactivateAfterSeconds" : {"L": "120"}
```

車両の最終状態をモニタリングする

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

状態テンプレートを作成し、車両に関連付けることで、車両の最終状態をほぼリアルタイムでモニタリングできます。状態テンプレートに関連付けられた車両は、 `onChange`または `periodic` 更新戦略を使用してテレメトリデータをストリーミングします。変更時の更新戦略では、関連する車両は変更があったときにテレメトリデータをストリーミングします。定期的な更新戦略中、関連付けられた車両は指定された期間中にテレメトリデータをストリーミングします。

オンデマンドオペレーションでは、現在の車両状態を一度にリクエストできます (フェッチ) 。以前にデプロイした状態テンプレートを有効または無効にして、車両状態データのレポートを開始または停止することもできます。最後の既知の状態オペレーションは、 AWS IoT コマンド APIsを使用して実行されます。

各状態テンプレートには、次の情報が含まれています。

`name`

状態テンプレートの一意のエイリアス。

`signalCatalogArn`

状態テンプレートに関連付けられたシグナルカタログの Amazon リソースネーム (ARN)。

`stateTemplateProperties`

データが収集されるシグナルのリスト。状態テンプレートのプロパティは、車両がクラウドに送信する特定のシグナル更新を決定します。

`dataExtraDimensions`

プロトコルバッファ (Protobuf) でエンコードされた処理済みデータに含まれる車両属性のリスト。

`metadataExtraDimensions`

処理されたデータを MQTT 5 ユーザープロパティとして公開する車両属性のリスト。

`id`

サービスによって生成された一意の識別子。

Edge Agent for AWS IoT FleetWise ソフトウェアを使用する車両によって送信されるデータを収集する方法については、「」を参照してくださいMQTT メッセージングを使用して最後の既知の状態車両データを処理する。状態テンプレートを車両に関連付ける方法の詳細については、「」を参照してくださいAWS IoT FleetWise 車両を作成する。

トピック

- AWS IoT FleetWise 状態テンプレートを作成する
- AWS IoT FleetWise 状態テンプレートを更新する
- AWS IoT FleetWise 状態テンプレートを削除する
- Get AWS IoT FleetWise 状態テンプレート情報
- データ収集と処理のためのステートテンプレートオペレーション

AWS IoT FleetWise 状態テンプレートを作成する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise API またはコンソールを使用して、状態テンプレートを作成できます。状態テンプレートは、車両の状態を追跡するメカニズムを提供します。車両で実行される Edge Agent for AWS IoT FleetWise ソフトウェアは、シグナル更新を収集してクラウドに送信します。

状態テンプレートを作成する (コンソール)

AWS IoT FleetWise コンソールを使用して、状態テンプレートを作成できます。

状態テンプレートを作成するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、状態テンプレートを選択します。

3. 状態テンプレートページで、状態テンプレートの作成を選択します。
4. 状態テンプレートの詳細で、状態テンプレートの名前を入力し、オプションで説明を入力します。
5. 「シグナルの選択」で、車両ステータス情報を取得するシグナルを追加します。
6. 状態テンプレートの作成 を選択します。

状態テンプレートを正常に作成すると、状態テンプレートページに表示されます。車両に関連付けることができるようになりました。

状態テンプレートを作成する (AWS CLI)

CreateStateTemplate API オペレーションを使用して、状態テンプレートを作成できます。次の例では AWS CLIを使用しています。

状態テンプレートを作成するには、次のコマンドを実行します。

create-state-template を、状態テンプレート設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise create-state-template \
    --cli-input-json file://create-state-template.json
```

Example 状態テンプレートの設定

`stateTemplateProperties` には、シグナルの完全修飾名を含める必要があります。

`dataExtraDimensions` および には、車両属性の完全修飾名を含める`metadataExtraDimensions`必要があります。指定されたディメンションは、状態テンプレート内の既存のディメンション値を置き換えます。

```
{
    "name": "state-template-name",
    "signalCatalogArn": "arn:aws:iotfleetwise:region:account:signal-catalog/catalog-name",
    "stateTemplateProperties": [
        "Vehicle.Signal.One",
        "Vehicle.Signal.Two"
    ],
    "dataExtraDimensions": [
```

```
        "Vehicle.Attribute.One",
        "Vehicle.Attribute.Two"
    ],
    "metadataExtraDimensions": [
        "Vehicle.Attribute.Three",
        "Vehicle.Attribute.Four"
    ]
}
```

AWS IoT FleetWise 状態テンプレートを車両に関連付ける

状態テンプレートを車両に関連付ける (コンソール)

AWS IoT FleetWise コンソールを使用して、関連する状態テンプレートを車両に追加できます。

状態テンプレートを関連付けるには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両] を選択します。
3. リストから車両を選択して、詳細ページを開きます。
4. 状態テンプレートタブで、状態テンプレートの管理を選択します。
5. 状態の追加テンプレートを選択します。
6. 状態テンプレートを選択し、そのレポート方法を選択します。
   a. 変更時 – 状態テンプレートは車両の状態への変更を報告します。
   b. 定期的 – 状態テンプレートは、指定された時間間隔の更新を報告します。
7. [Save changes] (変更の保存) をクリックします。

AWS IoT FleetWise 状態テンプレートを車両に関連付ける (AWS CLI)

作成した状態テンプレートを車両に関連付けて、車両からクラウドへの状態更新の収集を許可します。これを行うには、以下を使用します。

- 車両を作成するときは、 `create-vehicle` コマンドの `stateTemplates`フィールドを使用します。詳細については、「AWS IoT FleetWise 車両を作成する」を参照してください。
- 車両を更新するときは、 `update-vehicle` コマンドの `stateTemplatesToAdd`または `stateTemplatesToRemove`フィールドを使用します。詳細については、「AWS IoT FleetWise 車両を更新する」を参照してください。

AWS IoT FleetWise 状態テンプレートを更新する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

UpdateStateTemplate API オペレーションまたは AWS IoT FleetWise コンソールを使用して、既存の状態テンプレートを更新できます。

状態テンプレートを更新する (コンソール)

コンソールから状態テンプレートを更新するには、 AWS IoT FleetWise コンソールのステートテンプレートページに移動し、次の手順を実行します。

1. 更新する状態テンプレートを選択し、編集を選択します。
2. 状態テンプレートの詳細を編集し、変更の保存を選択します。

状態テンプレートを更新する (AWS CLI)

状態テンプレートを更新するには、次のコマンドを実行します。

update-state-template を、状態テンプレートの設定を含む .json ファイルの名前に置き換えます。

```
aws iotfleetwise update-state-template \
    --cli-input-json file://update-state-template.json
```

Example 状態テンプレートの設定

には、シグナルの完全修飾名が含まれている`stateTemplateProperties`必要があります。

`dataExtraDimensions` および には、車両属性の完全修飾名が含まれている`metadataExtraDimensions`必要があります。

```
{
    "identifier": "state-template-name",
    "stateTemplatePropertiesToAdd": [
        "Vehicle.Signal.Three"
```

```
    ],
    "stateTemplatePropertiesToRemove": [
        "Vehicle.Signal.One"
    ],
    "dataExtraDimensions": [
        "Vehicle.Attribute.One",
        "Vehicle.Attribute.Two"
    ],
    "metadataExtraDimensions": [
        "Vehicle.Attribute.Three",
        "Vehicle.Attribute.Four"
    ]
}
```

AWS IoT FleetWise 状態テンプレートを削除する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

DeleteStateTemplate API オペレーションまたは AWS IoT FleetWise コンソールを使用して、状態テンプレートを削除できます。

状態テンプレートを削除する (コンソール)

コンソールから状態テンプレートを削除するには、 AWS IoT FleetWise コンソールの 状態テンプレート ページに移動し、次の手順を実行します。

1. 削除する状態テンプレートを選択し、削除を選択します。
2. 状態テンプレートを削除することを確認し、削除を選択します。

状態テンプレートを削除する (AWS CLI)

状態テンプレートを削除するには、次のコマンドを実行します。

identifier を状態テンプレートの名前または ID に置き換えます。

```
aws iotfleetwise delete-state-template \
```

```
    --identifier idenitfier
```

Get AWS IoT FleetWise 状態テンプレート情報

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

GetStateTemplate API オペレーションを使用して、状態テンプレートに関する情報を取得できます。次の例では AWS CLIを使用しています。

identifier を状態テンプレートの名前に置き換えます。

```
aws iotfleetwise get-state-template \
    --identifier idenitfier
```

ListStateTemplates API オペレーションを使用して、作成した状態テンプレートのリストを取得できます。次の例では AWS CLIを使用しています。

```
aws iotfleetwise list-state-templates
```

カスタマーマネージド AWS KMS キーを使用して暗号化を有効にした場合は、ロールが `GetStateTemplate`または `ListStateTemplates` API オペレーションを呼び出すことができるように、次のポリシーステートメントを含めます。

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

    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:KMS_KEY_REGION:KMS_KEY_ACCOUNT_ID:key/KMS_KEY_ID"
      ]
```

```
    },
  ]
}
```

データ収集と処理のためのステートテンプレートオペレーション

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

以下のセクションでは、状態テンプレートを使用してデータ収集の有効化と無効化、フェッチオペレーションの実行、車両からの状態データの処理を行う方法について説明します。

トピック

- 状態テンプレートを使用して状態データ収集をアクティブ化または非アクティブ化する
- 状態テンプレートを使用して車両状態スナップショットを取得する
- MQTT メッセージングを使用して最後の既知の状態車両データを処理する

状態テンプレートを使用して状態データ収集をアクティブ化または非アクティブ化する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

以下のセクションでは、 を使用して状態テンプレートによるデータ取り込みをアクティブ化および非アクティブ化する方法について説明します AWS CLI。

> **Important**
>
> 開始する前に、状態テンプレートを既に作成し、そのテンプレートとその更新戦略を車両に関連付けていることを確認してください。

エッジエージェントがクラウドにシグナル更新を送信できるように、状態テンプレートをアクティブ化する必要があります。

状態テンプレートを使用してこれらのオペレーションを実行するには、まずコマンドリソースを作成し、次に車両でコマンド実行を開始します。次のセクションでは、この API を使用する方法と、データインジェストをアクティブ化および非アクティブ化する方法について説明します。

トピック

- CreateCommand API を使用する場合
- 例: 状態テンプレートをアクティブ化する
- 例: 状態テンプレートを非アクティブ化する

`CreateCommand` API を使用する場合

`AWS-IoTFleetwise`「」名前空間にコマンドリソースを作成し、状態テンプレートのコマンドリソースを作成または送信するときに、次のパラメータを使用します。

- `$stateTemplate.name` – オペレーションを実行するステートテンプレートの名前。オペレーションを実行する前に、状態テンプレートを車両に適用する必要があります。詳細については、「AWS IoT FleetWise 状態テンプレートを車両に関連付ける」を参照してください。
- `$stateTemplate.operation` – 状態テンプレートで実行されるオペレーション。このパラメータには、次のいずれかの値を使用します。
  - `activate` – エッジエージェントは、状態テンプレートを車両に適用したときに、`stateTemplateUpdateStrategy`指定した (変更時または定期的な) に基づいて、クラウドへのシグナル更新の送信を開始します。詳細については、「AWS IoT FleetWise 状態テンプレートを車両に関連付ける」を参照してください。

    また、自動状態テンプレートの非アクティブ化時間を定義して、指定した期間後に更新を停止することもできます。自動非アクティブ化時間が指定されていない場合、状態テンプレートは非アクティブ化呼び出しが発行されるまで更新を送信し続けます。

    `activate` コマンドを受信するとすぐに、デバイスは更新戦略に従って状態テンプレートで指定されたシグナルを送信する必要があります。 AWS IoT FleetWise では、デバイスがアクティブ化コマンドを受信すると、送信する最初のメッセージに状態テンプレート内のすべてのシグナルのスナップショットを含めることをお勧めします。後続のメッセージは、更新戦略に従って送信する必要があります。
  - `deactivate` – エッジエージェントは、クラウドへのシグナル更新の送信を停止します。

- `fetchSnapshot` – エッジエージェントは、状態テンプレートを車両に適用したときに`stateTemplateUpdateStrategy`指定した に関係なく、状態テンプレートで定義されたシグナルの 1 回限りのスナップショットを送信します。

- （オプション）`$stateTemplate.deactivateAfterSeconds` – 状態テンプレートは、指定された時間後に自動的に非アクティブ化されます。このパラメータは、 パラメータの値が`$stateTemplate.operation`「アクティブ」の場合にのみ使用できます。このパラメータが指定されていない場合、またはこのパラメータの値が 0 の場合、エッジエージェントは状態テンプレートの「非アクティブ化」オペレーションを受信するまで、シグナル更新をクラウドに送信し続けます。状態テンプレートは自動的に非アクティブ化されることはありません。

  最小値: 0、最大値: 4294967295。

> **Note**
>
> - API は、既にアクティブな状態にあるテンプレートのアクティベーションリクエストに応答して成功を返します。
> - API は、すでに非アクティブ化状態にあるテンプレートの非アクティブ化リクエストに応答して成功を返します。
> - 状態テンプレートに対して行った最新のリクエストは、有効になるリクエストです。たとえば、状態テンプレートを 1 時間以内に非アクティブ化するようにリクエストし、同じテンプレートを 4 時間以内に非アクティブ化するように 2 回目のリクエストを行うと、4 時間の非アクティブ化は最新のリクエストであるために有効になります。

> **Important**
>
> 検証例外は、次のいずれかのシナリオで発生する可能性があります。
>
> - 車両`ASSOCIATED`に付属していない状態テンプレートが提供されます。
> - 状態テンプレートをアクティブ化するリクエストは行われますが、車両`DEPLOYED`にはありません。
> - 状態テンプレートに対するリクエストは行われますが、車両`DELETED`上にあります。

例: 状態テンプレートをアクティブ化する

状態テンプレートをアクティブ化するには、まずコマンドリソースを作成します。その後、状態テンプレートをアクティブ化する車両に次のコマンドを送信できます。この例では、コマンドの作成時にパラメータのデフォルト値を指定する方法を示します。これらのパラメータとその値は、コマンド実行を開始して状態テンプレートをアクティブ化するときに使用されます。

1. コマンドリソースを作成する

   車両にコマンドを送信する前に、コマンドリソースを作成する必要があります。コマンドを車両に送信するときに、必須パラメータの代替値を指定できます。詳細については、「コマンドリソースを作成する」を参照してください。

   > **Important**
   >
   > `$stateTemplate.name` および `$stateTemplate.operation`パラメータは文字列データ型として指定する必要があります。他のデータ型が指定されている場合、またはこれら 2 つのパラメータのいずれかが欠落している場合、コマンドの実行は検証例外で失敗します。`$stateTemplate.deactivateAfterSeconds` パラメータはLongデータ型として指定する必要があります。

```
aws iot create-command \
    --description "This command activates a state template on a vehicle"
    --command-id ActivateStateTemplate \
    --display-name "Activate State Template" \
    --namespace AWS-IoTFleetWise \
    --mandatory-parameters '[
    {
        "name": "$stateTemplate.name",
        "defaultValue": {"S": "ST123"}
    },
    {
        "name": "$stateTemplate.operation",
        "defaultValue": {"S": "activate"}
    },
    {
        "name": "$stateTemplate.deactivateAfterSeconds",
        "defaultValue": {"L": "120"}
    }
```

```
]'
```

2. 車両でコマンド実行を開始する

   コマンドを作成したら、コマンドを車両に送信します。コマンドリソースの作成時に必須パラメータの値を指定しなかった場合は、今すぐ指定する必要があります。詳細については、「コマンドを送信する (AWS CLI)」を参照してください。

   > **Important**
   > API オペレーションには、アカウント固有の AWS IoT ジョブデータプレーン API エンドポイントを使用していることを確認してください。

```
aws iot-jobs-data start-command-execution \
    --endpoint-url <endpoint-url> \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/ActivateStateTemplate \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>
```

3. 状態テンプレートオペレーションのステータスを取得する

   コマンドの実行を開始したら、 `GetCommandExecution` API を使用して状態テンプレートを取得できます。

```
aws iot get-command-execution --execution-id <EXECUTION_ID>
```

例: 状態テンプレートを非アクティブ化する

状態テンプレートを非アクティブ化するには、まずコマンドリソースを作成します。その後、状態テンプレートを非アクティブ化する車両に次のコマンドを送信できます。この例では、コマンドの作成時にパラメータのデフォルト値を指定する方法を示します。これらのパラメータとその値は、コマンド実行を開始して状態テンプレートを非アクティブ化するときに使用されます。

1. コマンドリソースを作成する

   車両にコマンドを送信する前に、コマンドリソースを作成する必要があります。コマンドを車両に送信するときに、必須パラメータの代替値を指定できます。詳細については、「コマンドリソースを作成する」を参照してください。

```
aws iot create-command \
    --description "This command deactivates a state template on a vehicle"
    --command-id DeactivateStateTemplate \
    --display-name "Deactivate State Template" \
    --namespace AWS-IoTFleetWise \
    --mandatory-parameters '[
    {
        "name": "$stateTemplate.name",
        "defaultValue": {"S": "ST123"}
    },
    {
        "name": "$stateTemplate.operation",
        "defaultValue": {"S": "deactivate"}
    }
]'
```

2. 車両でコマンド実行を開始する

   コマンドを作成したら、コマンドを車両に送信します。コマンドリソースの作成時に必須パラメータの値を指定しなかった場合は、今すぐ指定する必要があります。詳細については、「コマンドを送信する (AWS CLI)」を参照してください。

```
aws iot-jobs-data start-command-execution \
    --endpoint-url <endpoint-url> \
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/DeactivateStateTemplate
 \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>
```

3. 状態テンプレートオペレーションのステータスを取得する

   コマンドの実行を開始したら、 `GetCommandExecution` API を使用して状態テンプレートを取得できます。

```
aws iot get-command-execution  --execution-id <EXECUTION_ID>
```

状態テンプレートを使用して車両状態スナップショットを取得する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

`CreateCommand` AWS IoT Core コントロールプレーン API オペレーションまたは AWS IoT FleetWise コンソールを使用して、車両の最後の既知の状態を取得できます。

> **Important**
>
> 検証例外は、次のいずれかのシナリオで発生する可能性があります。
>
> - 車両`ASSOCIATED`に付属していない状態テンプレートが提供されます。
> - 状態テンプレートをアクティブ化するリクエストは行われますが、車両`DEPLOYED`にはありません。
> - 状態テンプレートに対するリクエストは行われますが、車両`DELETED`上にあります。

車両状態のスナップショットを取得する (コンソール)

AWS IoT FleetWise コンソールを使用して、車両の最後の既知の状態を取得できます。 AWS IoT FleetWise は、データを取得するためのコマンドを作成します。

車両の状態を取得するには

1. AWS IoT FleetWise コンソールを開きます。
2. ナビゲーションペインで、[車両] を選択します。
3. リストから車両を選択して、詳細ページを開きます。
4. 状態テンプレートタブで、データの取得を選択します。
5. コマンドを送信してデータを取得するアクセス許可を AWS IoT FleetWise に付与する IAM ロールを選択します。「アクセスの制御」を参照してください。
6. 取得状態を選択します。

車両状態のスナップショットを取得する (AWS CLI)

状態スナップショットを取得するには、まずコマンドリソースを作成します。その後、状態スナップショットを取得する車両に次のコマンドを送信できます。CreateCommand API とそのパラメータの使用の詳細については、「」を参照してください[CreateCommand API を使用する場合](#)。

1. コマンドリソースを作成する

   次の例は、フェッチオペレーションを実行するコマンドリソースを作成する方法を示しています。コマンドを車両に送信するときに、必須パラメータの代替値を指定できます。詳細については、「[コマンドリソースを作成する](#)」を参照してください。

```
aws iot create-command \
    --command-id <COMMAND_ID> \
    --display-name "FetchSnapshot State Template" \
    --namespace AWS-IoTFleetWise \
    --mandatory-parameters '[
      {
          "name": "$stateTemplate.name",
          "defaultValue": {"S": "ST123"}
      },
      {
          "name": "$stateTemplate.operation",
          "defaultValue": {"S": "fetchSnapshot"}
      }
    ]'
```

   レスポンス:

```
{
    "commandId": "<COMMAND_ID>",
    "commandArn": "arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/<COMMAND_ID>"
}
```

2. コマンド実行を開始して状態スナップショットを取得する

   コマンドを作成したら、コマンドを車両に送信します。コマンドリソースの作成時に必須パラメータの値を指定しなかった場合は、今すぐ指定する必要があります。詳細については、「[コマンドを送信する (AWS CLI)](#)」を参照してください。

```
aws iot-jobs-data start-command-execution \
```

```
    --command-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:command/<COMMAND_ID> \
    --target-arn arn:aws:iot:<REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>
```

レスポンス:

```
{
    "executionId": "<UNIQUE_UUID>"
}
```

3. 状態テンプレートオペレーションのステータスを取得する

   コマンドの実行を開始したら、 `GetCommandExecution` API を使用して状態テンプレートを取得できます。

```
aws iot get-command-execution --execution-id <EXECUTION_ID>
```

MQTT メッセージングを使用して最後の既知の状態車両データを処理する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

車両から更新を受け取り、そのデータを処理するには、次の MQTT トピックにサブスクライブします。詳細については、「AWS IoT Core デベロッパーガイド」の「MQTT トピック」を参照してください。

```
$aws/iotfleetwise/vehicles/$vehicle_name/last_known_state/$state_template_name/data
```

MQTT は注文を保証しないため、最後の既知の状態シグナル更新メッセージが順序どおりに受信されない可能性があります。MQTT を使用して車両データを受信および処理するクライアントは、これを処理する必要があります。最後の既知の状態シグナル更新メッセージは、MQTT 5 メッセージングプロトコルに従います。

各 MQTT メッセージのメッセージヘッダーには、次のユーザープロパティがあります。

- vehicleName – 車両の一意の識別子。

- stateTemplateName – 最後の既知の状態テンプレートの一意の識別子。

さらに、状態テンプレートを更新または作成するときにmetadataExtraDimensionsリクエストパラメータを指定することで、MQTT メッセージヘッダーに含める車両属性を指定できます。（「状態テンプレート」を参照してください。）

MQTT メッセージヘッダーのユーザープロパティは、ペイロードを検査せずにメッセージを異なる宛先にルーティングするのに役立ちます。

MQTT メッセージペイロードには、車両から収集されたデータが含まれます。状態テンプレートを作成または更新するときにextraDimensionsリクエストパラメータを指定することで、MQTT メッセージペイロードに含める車両属性を指定できます (「」を参照AWS IoT FleetWise 状態テンプレートを作成する）。追加のディメンションは、追加のディメンションを関連付けることで、車両から収集されたデータを強化します。

MQTT メッセージペイロードはプロトコルバッファ (Protobuf) でエンコードされ、MQTT メッセージヘッダーには application/octet-stream として定義されたコンテンツタイプインジケータが含まれています。Protobuf エンコーディングスキーマは次のとおりです。

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

syntax = "proto3";

option java_package = "com.amazonaws.iot.autobahn.schemas.lastknownstate";
package Aws.IoTFleetWise.Schemas.CustomerMessage;

message LastKnownState {

  /*
   * The absolute timestamp in milliseconds since Unix Epoch of when the event was
 triggered in vehicle.
   */
  uint64 time_ms = 1;

  /*
   * This field is deprecated, use signals instead
   */
  repeated Signal signal = 2 [ deprecated = true ];

  repeated Signal signals = 3;
```

```
  repeated ExtraDimension extra_dimensions = 4;
}

message Signal {

  /*
   * The Fully Qualified Name of the signal is the path to the signal plus the signal's
 name.
   * For example, Vehicle.Chassis.SteeringWheel.HandsOff.HandsOffSteeringState
   * The fully qualified name can have up to 150 characters. Valid characters: a-z, A-
Z, 0-9, : (colon), and _ (underscore).
   */
  string name = 1;

  /*
   * The FWE reported signal value can be one of the following data types.
   */
  oneof SignalValue {
    double double_value = 2;

    bool boolean_value = 3;

    sint32 int8_value = 4;

    uint32 uint8_value = 5;

    sint32 int16_value = 6;

    uint32 uint16_value = 7;

    sint32 int32_value = 8;

    uint32 uint32_value = 9;

    sint64 int64_value = 10;

    uint64 uint64_value = 11;

    float float_value = 12;
    /*
     * An UTF-8 encoded or 7-bit ASCII string
     */
    string string_value = 13;
```

```
  }
}

message ExtraDimension {
  /*
   * The Fully Qualified Name of the attribute is the path to the attribute plus the
 attribute's name.
   * For example, Vehicle.Model.Color
   * The fully qualified name can have up to 150 characters. Valid characters: a-z, A-
Z, 0-9, : (colon), and _ (underscore).
   */
  string name = 1;

  oneof ExtraDimensionValue {
    /*
     * An UTF-8 encoded or 7-bit ASCII string
     */
    string string_value = 2;
  }
}
```

コードの説明は以下のとおりです。

- `time_ms`:

  車両でイベントがトリガーされたときの絶対タイムスタンプ (Unix エポックからのミリ秒単位) 。Edge Agent ソフトウェアは、このタイムスタンプのために車両のクロックで を使用します。

- `signal`:

  シグナル情報`Signal`を含む の配列: name (文字列) および
  は、、`double`、、`bool`、、`int8``uint8`、`int16`、、`uint16`、`int32``uint32``int64``uint64``float`、、の各データ型`signalValue`をサポートします`string`。

- `extra_dimensions`:

  車両属性情報`ExtraDimensions`を含む の配列: name (文字列) で`extraDimensionValue`、現在 `string` データ型のみをサポートしています。

チュートリアル: カスタムデコードインターフェイスを使用してネットワークに依存しないデータ収集を設定する

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

序章

このチュートリアルでは、 AWS IoT FleetWise を設定してデータを収集し、カスタムデコードインターフェイスを利用するネットワークに依存しないデータ収集を使用してコマンドを実行する方法について説明します。ネットワークに依存しないデータ収集では、独自の方法を使用してシグナルをデコードしてから、指定したデータ送信先に送信できます。これにより、 AWS IoT FleetWise 専用のシグナルデコーダーを作成する必要がないため、時間を節約できます。独自の実装を使用してシグナルのサブセットをデコードすることも、デコーダーマニフェストを作成または更新`defaultForUnmappedSignals`するときに を使用することもできます。これにより、車両内のさまざまなソースでシグナルとトリガーを収集するための柔軟性も得られます。

このチュートリアルは、標準のコントローラーエリアネットワーク (CAN バス) インターフェイス上にない車両信号を対象としています。たとえば、カスタムの車内形式またはスキームでエンコードされたデータなどです。

環境設定

このチュートリアルでは、 AWS IoT FleetWise クラウド、および Edge 実装 APIsとしています。

データモデル

次のセクションでは、カスタムデコードインターフェイスを使用して車両プロパティをモデル化する方法について説明します。これは、データ収集とコマンドのユースケースに適用されます。また、IDLs など、車両で使用される基盤となるデータソースモデリングにも適用されます。

この例では、収集する車両センサー (現在の車両位置) とリモートで制御する車両アクチュエータ (Air Conditioner) の 2 つの車両プロパティがあります。どちらもこのスキームで定義されています。

```
// Vehicle WGS84 Coordinates
double Latitude;
double Longitude;

// Vehicle AC
Boolean ActivateAC;
```

次のステップでは、カスタムデコードインターフェイス API を使用して、これらの定義を AWS IoT FleetWise にインポートします。 APIs

シグナルカタログの更新

これらの定義をシグナルカタログにインポートします。 AWS IoT FleetWise にシグナルカタログがすでにある場合は、更新 API を直接使用します。シグナルカタログがない場合は、まずシグナルカタログを作成してから、更新 API を呼び出します。

まず、これらの車両信号の VSS 表現を作成する必要があります。VSS は、 AWS IoT FleetWise の車両データを表す分類として使用されます。次の内容で「Vehicle-signals.json」という名前の JSON ファイルを作成します。

```
// vehicle-signals.json
// Verify that branches and nodes are unique in terms of fully qualified name
// in the signal catalog.
[
 {
    "branch": {
      "fullyQualifiedName": "Vehicle",
      "description": "Vehicle Branch"
    }
  },
  {
    "branch": {
      "fullyQualifiedName": "Vehicle.CurrentLocation",
      "description": "CurrentLocation"
    }
  },
  {
    "sensor": {
      "dataType": "DOUBLE",
      "fullyQualifiedName": "Vehicle.CurrentLocation.Latitude",
      "description": "Latitude"
    }
```

```
  },
  {
    "sensor": {
      "dataType": "DOUBLE",
      "fullyQualifiedName": "Vehicle.CurrentLocation.Longitude",
      "description": "Longitude"
    }
  },
  {
    "actuator": {
      "fullyQualifiedName": "Vehicle.ActivateAC",
      "description": "AC Controller",
      "dataType": "BOOLEAN"
    }
  }
]
```

シグナルカタログがない場合は、 を呼び出す必要がありますcreate-signal-catalog。

```
VEHICLE_NODES=`cat vehicle-signals.json`
aws iotfleetwise create-signal-catalog \
        --name my-signal-catalog \
        --nodes "${VEHICLE_NODES}"
```

シグナルカタログがすでにある場合は、 update-signal-catalog API を使用してこれらのシグナルを追加できます。

```
VEHICLE_NODES=`cat vehicle-signals.json`
aws iotfleetwise update-signal-catalog \
        --name my-signal-catalog \
        --nodes-to-add "${VEHICLE_NODES}"
```

車両モデルとデコーダー

シグナルカタログにシグナルを挿入した後、次のステップは車両モデルを作成し、それらのシグナルをインスタンス化することです。そのためには、 create-model-manifestおよび create-decoder-manifest APIsを使用します。

まず、車両モデルに挿入するシグナル名をフォーマットします。

```
# Prepare the signals for insertion into the vehicle model.
VEHICLE_NODES=`cat vehicle-signals.json`
```

```
VEHICLE_NODES=`echo ${VEHICLE_NODES} | jq -r ".[] | .actuator,.sensor
 | .fullyQualifiedName" | grep Vehicle\\.`
VEHICLE_NODES=`echo "${VEHICLE_NODES}" | jq -Rn [inputs]`
# This is how the vehicle model input looks.
echo $VEHICLE_NODES
# [ "Vehicle.CurrentLocation.Latitude",
#   "Vehicle.CurrentLocation.Longitude",
#   "Vehicle.ActivateAC" ]
# Create the vehicle model with those signals.
aws iotfleetwise create-model-manifest \
    --name my-model-manifest \
    --signal-catalog-arn arn:xxxx:signal-catalog/my-signal-catalog \
    --nodes "${VEHICLE_NODES}"

# Activate the vehicle model.
 aws iotfleetwise update-model-manifest \
    --name my-model-manifest --status ACTIVE
```

次に、カスタムデコードインターフェイスを使用してデコーダーマニフェストを作成します。

> **Note**
>
> この例の一部ではないカスタム IDs を指定する場合にのみ、ネットワークインターフェイスとシグナルを作成する必要があります。
> 完全修飾名 (FQN) がカスタムデコードシグナル ID と異なる場合のデコード情報のマッピングについては、「エッジエージェントデベロッパーガイド」を参照してください。

```
// Create a network interface that is of type : CUSTOM_DECODING_INTERFACE
// custom-interface.json
[
  {
    "interfaceId": "NAMED_SIGNAL",
    "type": "CUSTOM_DECODING_INTERFACE",
    "customDecodingInterface": {
      "name": "NamedSignalInterface"
    }
  },
  {
    "interfaceId": "AC_ACTUATORS",
    "type": "CUSTOM_DECODING_INTERFACE",
    "customDecodingInterface": {
```

```
      "name": "NamedSignalInterface"
    }
  }
]
// custom-decoders.json
// Refer to the fully qualified names of the signals, make them of
// type CUSTOM_DECODING_SIGNAL, and specify them as part of the same interface ID
// that was defined above.
[
    {
      "fullyQualifiedName": "Vehicle.CurrentLocation.Longitude",
      "interfaceId": "NAMED_SIGNAL",
      "type": "CUSTOM_DECODING_SIGNAL",
      "customDecodingSignal": {
        "id": "Vehicle.CurrentLocation.Longitude"
      }
    },
    {
      "fullyQualifiedName": "Vehicle.CurrentLocation.Latitude",
      "interfaceId": "NAMED_SIGNAL",
      "type": "CUSTOM_DECODING_SIGNAL",
      "customDecodingSignal": {
        "id": "Vehicle.CurrentLocation.Latitude"
      }
    },
    {
        "fullyQualifiedName": "Vehicle.ActivateAC",
        "interfaceId": "AC_ACTUATORS",
        "type": "CUSTOM_DECODING_SIGNAL",
        "customDecodingSignal": {
          "id": "Vehicle.ActivateAC"
        }
    }
]
# Create the decoder manifest.
 CUSTOM_INTERFACE=`cat custom-interface.json`
 CUSTOM_DECODERS=`cat custom-decoders.json`

aws iotfleetwise create-decoder-manifest \
   --name my-decoder-manifest \
   --model-manifest-arn arn:xxx:model-manifest/my-model-manifest \
   --network-interfaces "${CUSTOM_INTERFACE}" \
   --signal-decoders "${CUSTOM_DECODERS}"
```

```
 # Activate the decoder manifest.
 aws iotfleetwise update-decoder-manifest \
    --name my-decoder-manifest \
    --status ACTIVE
```

この時点で、 AWS IoT FleetWise でこれらのシグナルを完全にモデル化しました。次に、車両を作成し、作成したモデルに関連付けます。そのために `create-vehicle` API を使用します。

```
aws iotfleetwise create-vehicle \
    --decoder-manifest-arn arn:xxx:decoder-manifest/my-decoder-manifest \
    --association-behavior ValidateIotThingExists \
    --model-manifest-arn arn:xxx:model-manifest/my-model-manifest \
    --vehicle-name "my-vehicle"
```

次のステップでは、 AWS IoT FleetWise Edge コードベースに焦点を当て、必要なコード拡張子を記述します。

> **Note**
>
> Edge 実装の詳細については、「 Edge エージェントデベロッパーガイド」を参照してください。

Send コマンド

次に、ソフトウェアをコンパイルし (ヘッダーと C++ ファイルを CMake ファイルに追加してください) 、クラウド APIs に戻ってこのアクチュエータでコマンドをテストします。

```
// Create a command targeting your vehicle.
aws iot create-command --command-id activateAC \
    --namespace "AWS-IoT-Fleetwise" \
    --endpoint-url endpoint-url \
    --role-arn ${SERVICE_ROLE_ARN} \
    --mandatory-parameters '[ { "name": "$actuatorPath.Vehicle.ActivateAC",
 "defaultValue": {"B": "false"} } ]' \
// You will receive the command ARN.

{
    "commandId": "activateAC",
    "commandArn": "arn:aws:iot:xxx:command/activateAC"
```

```
}

// You can send the command to activate the AC targeting your vehicle.

JOBS_ENDPOINT_URL=`aws iot describe-endpoint --endpoint-type iot:Jobs | jq -
j .endpointAddress`
aws iot-jobs-data start-command-execution \
    --command-arn arn:aws:iot:xxx:command/activateAC \
    --target-arn arn:xxx:vehicle/my-vehicle \
    --parameters '{ "$actuatorPath.Vehicle.ActivateAC" : {"B": "true"}}' \
    --endpoint-url https://${JOBS_ENDPOINT_URL}
// You will receive the corresponding execution ID.
{
    "executionId": "01HSK4ZH6ME7D43RB2BV8JC51D"
}

// If you have the AWS IoT FleetWise Edge Agent running, you can see the logs.
[AcCommandDispatcher.cpp:26] [setActuatorValue()]:
[Actuator Vehicle.ActivateAC executed successfully for command ID
 01HSK4ZH6ME7D43RB2BV8JC51D]
```

AWS IoT FleetWise で AWS CLI と AWS SDKs

このセクションでは、 AWS IoT FleetWise API リクエストの作成について説明します。 AWS IoT FleetWise オペレーションとデータ型の詳細については、AWS 「 IoT FleetWise API リファレンス」を参照してください。

さまざまなプログラミング言語で AWS IoT FleetWise を使用するには、以下の自動機能を含む AWS SDKs を使用します。

- サービスリクエストに暗号署名する
- リクエストを再試行する
- エラーレスポンスの処理をする

コマンドラインアクセスの場合は、 で AWS IoT FleetWise を使用しますAWS CLI。コマンドラインから AWS IoT FleetWise やその他の サービスを制御したり、スクリプトを使用して自動化したりできます。

AWS IoT FleetWise のトラブルシューティング

このセクションのトラブルシューティング情報と解決策を使用して、 AWS IoT FleetWise の問題を解決します。

以下の情報は、 AWS IoT FleetWise の一般的な問題のトラブルシューティングに役立つ場合があります。

トピック

- AWS IoT FleetWise デコーダーマニフェストの問題
- Edge Agent for AWS IoT FleetWise ソフトウェアの問題
- 問題の保存と転送

AWS IoT FleetWise デコーダーマニフェストの問題

デコーダーマニフェストの問題のトラブルシューティングを行います。

デコーダーマニフェスト API コールの診断

エラー	トラブルシューティングのガイドライン
`UpdateOperationFailure.ConflictingDecoderUpdate`	同じデコーダーマニフェストに複数の更新リクエストがあります。しばらく待ってから、もう一度試してください。
`UpdateOperationFailure.InternalFailure`	InternalFailure はカプセル化された例外として起動されます。問題自体は、カプセル化された例外によって異なります。
`UpdateOperationFailure.ActiveDecoderUpdate`	デコーダーマニフェストは `Active` 状態であるため、更新できません。デコーダマニフェストの状態を `DRAFT` に変更してから、もう一度試してください。
`UpdateOperationFailure.ConflictingModelUpdate`	AWS IoT FleetWise は、他のユーザーによって変更されている車両モデル (モデルマニフェス

エラー	トラブルシューティングのガイドライン
	ト) に対して検証しようとしています。しばらく待ってから、もう一度試してください。
`UpdateOperationFailure.ModelManifestValidationResponse : FailureReason.MODEL_DATA_ENTRIES_NOT_FOUND`	車両モデルには、シグナルが関連付けられていません。車両モデルにシグナルを追加し、シグナルが関連するシグナルカタログにあることを確認してください。
`UpdateOperationFailure.ModelManifestValidationResponse : FailureReason.MODEL_NOT_ACTIVE`	車両モデルを更新して `ACTIVE` 状態にしてから、もう一度試してください。
`UpdateOperationFailure.ModelManifestValidationResponse : FailureReason.MODEL_NOT_FOUND`	AWS IoT FleetWise は、デコーダーマニフェストに関連付けられた車両モデルを見つけることができません。車両モデルの Amazon リソースネーム (ARN) を確認して、もう一度試してください。
`UpdateOperationFailure.ModelManifestValidationResponse (FailureReason.MODEL_DATA_ENTRIES_READ_FAILURE`	車両モデルのシグナル名がシグナルカタログに見つからなかったため、車両モデルの検証に失敗しました。車両モデル内のすべてのシグナルが、関連するシグナルカタログに含まれていることを確認してください。
`UpdateOperationFailure.ValidationFailure`	デコーダーマニフェストの更新リクエストに、無効なシグナルまたはネットワークインターフェイスが見つかりました。例外によって返されたすべてのシグナルとネットワークインターフェイスが存在すること、使用されているすべてのシグナルが使用可能なインターフェイスに関連付けられていること、およびシグナルと関連付けられているインターフェイスを削除しないことを確認してください。

エラー	トラブルシューティングのガイドライン
`UpdateOperationFailure.KmsKeyAccessDenied`	オペレーションに使用される AWS Key Management Service（AWS KMS) キーにはアクセス許可の問題があります。使用しているロールがキーにアクセスできることを確認し、もう一度試してください。
`UpdateOperationFailure.DecoderDoesNotExist`	デコーダーマニフェストが存在しません。デコーダーマニフェスト名を確認して、もう一度試してください。

`SIGNAL_DECODER_INCOMPATIBLE_WITH_SIGNAL_CATALOG` を原因とするビジョンシステムデータエラーメッセージには、リクエストが失敗した原因に関する情報がヒントとして応答に含まれます。このヒントを使用して、どのトラブルシューティングガイドラインに従うべきかを判断できます。

> **Note**
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

デコーダーマニフェストのビジョンシステムデータ検証の診断

エラー	トラブルシューティングのガイドライン
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.NO_SIGNAL_IN_CATALOG_FOR_DECODER_SIGNAL)`	AWS IoT FleetWise は、シグナルカタログを使用してシグナルデコーダーで使用されるルートシグナル構造が見つかりませんでした。構造のルートシグナルがシグナルカタログで正しく定義されていることを確認してください。
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.SIGNAL_DECODER_TYPE_INCOMPATIBLE_WITH_MESSAGE_SIGNAL_TYPE)`	シグナルカタログのプリミティブメッセージが、デコーダーマニフェストの更新リクエストと同じデータ型で定義されていませんでした。リクエストで定義されているプリミティブメッ

エラー	トラブルシューティングのガイドライン
	セージが、対応するシグナルカタログ定義と一致することを確認してください。
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.STRUCT_SIZE_MISMATCH)`	シグナルカタログ内の構造体に定義されているプロパティの数が、デコーダーマニフェストでデコードしようとしているプロパティの数と一致しません。シグナルカタログで定義されているシグナルと比較して、デコードするシグナルの数が正しいことを確認してください。
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.SIGNAL_DECODER_INCOMPATIBLE_WITH_SIGNAL_CATALOG)`	AWS IoT FleetWise は、デコーダーマニフェストリクエストで定義された structuredMessageDefinition なしで、シグナルカタログで STRUCT として定義されたシグナルを検出しました。デコーダーマニフェストの更新リクエストで、各構造体が StructuredMessageDefinition として定義されていることを確認してください。
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.SIGNAL_DECODER_INCOMPATIBLE_WITH_SIGNAL_CATALOG)`	デコーダーマニフェストで使用されている構造体のルートシグナルが、シグナルカタログで構造体として正しく定義されていません。デコーダーマニフェストで使用するルートシグナル構造体には、StructFullyQualifiedName フィールドが定義されている必要があります。また、その fullyQualifiedName を持つ STRUCT ノードも必要です。
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.SIGNAL_DECODER_INCOMPATIBLE_WITH_SIGNAL_CATALOG)`	デコーダーマニフェストリクエストで使用されるリーフメッセージの 1 つがプリミティブメッセージとして定義されていません。リクエスト内のすべてのリーフオブジェクトがプリミティブメッセージとして定義されていることを確認してください。

エラー	トラブルシューティングのガイドライン
`InvalidSignalDecoder.withReason(SignalDecoderFailureReason.SIGNAL_DECODER_INCOMPATIBLE_WITH_SIGNAL_CATALOG)`	シグナルカタログの配列オブジェクトが、デコーダーマニフェストの更新リクエストで StructuredMessageListDefinition として定義されていませんでした。デコーダーマニフェストの更新リクエストで、すべての配列プロパティが StructuredMessageListDefinition として定義されていることを確認してください。

Edge Agent for AWS IoT FleetWise ソフトウェアの問題

エッジエージェントソフトウェアの問題のトラブルシューティングを行います。

問題

- 問題: エッジエージェントソフトウェアが起動しない。
- 問題: [ERROR] [IoTFleetWiseEngine::connect]: [Failed to init persistency library]
- 問題: エッジエージェントソフトウェアがオンボードダイアグノーシス (OBD) II の PID と故障診断コード (DTC) を収集しない。
- 問題: Edge Agent for AWS IoT FleetWise ソフトウェアがネットワークからデータを収集しないか、データ検査ルールを適用できません。
- 問題: [ERROR] [AwsIotConnectivityModule::connect]: [Connection failed with error] または [WARN] [AwsIotChannel::send]: [No alive MQTT Connection.]

問題: エッジエージェントソフトウェアが起動しない。

エッジエージェントソフトウェアが起動しない場合、次のエラーが表示されることがあります。

- ```
  Error from reader: * Line 1, Column 1
  Syntax error: value, object or array expected.
  ```

  解決策: Edge Agent for AWS IoT FleetWise ソフトウェア設定ファイルが有効な JSON 形式を使用していることを確認します。例えば、カンマが正しく使用されていることを確認してください。設定ファイルの詳細については、次の手順に従って Edge Agent for AWS IoT FleetWise ソフトウェアデベロッパーガイドをダウンロードします。
  ```

1. AWS IoT FleetWise コンソールを開きます。
2. サービスのホームページの「Get started with AWS IoT FleetWise」セクションで、「Explore Edge Agent」を選択します。

- ```
  [ERROR] [SocketCANBusChannel::connect]: [ SocketCan with name xxx is not accessible]
  [ERROR] [IoTFleetWiseEngine::connect]: [ Failed to Bind Consumers to Producers ]
  ```

  解決策: このエラーは、エッジエージェントソフトウェアが、構成ファイルに定義されているネットワークインターフェイスとのソケット通信を確立できない場合に表示されることがあります。

  構成で定義されているすべてのネットワークインターフェイスが使用可能であることを確認するには、次のコマンドを実行します。

  ```
  ip link show
  ```

  ネットワークインターフェイスをオンラインにするには、次のコマンドを実行します。*network-interface-id* は、ネットワークインターフェイスの ID に置き換えます。

  ```
  sudo ip link set network-interface-id up
  ```

- ```
  [ERROR] [AwsIotConnectivityModule::connect]: [Connection failed with error]
  [WARN] [AwsIotChannel::send]: [No alive MQTT Connection.]
  # or
  [WARN] [AwsIotChannel::send]: [aws-c-common: AWS_ERROR_FILE_INVALID_PATH]
  ```

  解決策: このエラーは、エッジエージェントソフトウェアが AWS IoT Coreへの MQTT 接続を確立できない場合に表示されることがあります。以下が正しく構成されていることを確認し、エッジエージェントソフトウェアを再起動します。

  - `mqttConnection::endpointUrl` – AWS アカウントの IoT デバイスエンドポイント。
  - `mqttConnection::clientID` - エッジエージェントソフトウェアが実行されている車両の ID。
  - `mqttConnection::certificateFilename` - 車両証明書ファイルのパス。
  - `mqttConnection::privateKeyFilename` - 車両のプライベートキーファイルのパス。
  - AWS IoT Core を使用して車両をプロビジョニングしました。詳細については、「Provision AWS IoT FleetWise 車両」を参照してください。

トラブルシューティングの詳細については、AWS IoT Device SDK for C++ の「Frequently Asked Questions」を参照してください。

問題: [ERROR] [IoTFleetWiseEngine::connect]: [Failed to init persistency library]

解決策: このエラーは、エッジエージェントソフトウェアが永続化ストレージを検出できない場合に表示されることがあります。以下が正しく構成されていることを確認し、エッジエージェントソフトウェアを再起動します。

`persistency:persistencyPath` - 収集スキーム、デコーダーマニフェスト、データスナップショットの永続化に使用されるローカルパス。

問題: エッジエージェントソフトウェアがオンボードダイアグノーシス (OBD) II の PID と故障診断コード (DTC) を収集しない。

解決策: このエラーは、`obdInterface:pidRequestIntervalSeconds` または `obdInterface:dtcRequestIntervalSeconds` が 0 に設定されている場合に表示されることがあります。

エッジエージェントソフトウェアがオートマチックトランスミッションの車両で実行されている場合は、`obdInterface:hasTransmissionEcu` が `true` に設定されていることを確認してください。

車両が拡張コントローラーエリアネットワーク (CAN バス) のアービトレーション ID をサポートしている場合は、`obdInterface:useExtendedIds` が `true` に設定されていることを確認してください。

問題: Edge Agent for AWS IoT FleetWise ソフトウェアがネットワークからデータを収集しないか、データ検査ルールを適用できません。

解決策: このエラーは、デフォルトのクォータを超過した場合に表示されることがあります。

リソース	クォータ	調整可能	メモ
シグナル ID の値。	シグナル ID は 50,000 以下にする必要があります	はい	エッジエージェントソフトウェアは、50,000 より大きい ID

リソース	クォータ	調整可能	メモ
			を持つシグナルからはデータを収集しません。このクォータを変更する前に、シグナルカタログに含まれているシグナル数を確認することをお勧めします。
車両あたりのアクティブなデータ収集スキームの数	256	はい	このクォータを変更する前に、クラウドで作成したキャンペーンの数と、各キャンペーンに含まれているスキームの数を確認することをお勧めします。
シグナル履歴バッファのサイズ	20 MB	はい	クォータを超過した場合、エッジエージェントソフトウェアは新しいデータの収集を停止します。

問題: [ERROR] [AwsIotConnectivityModule::connect]: [Connection failed with error] または [WARN] [AwsIotChannel::send]: [No alive MQTT Connection.]

解決策: このエラーは、エッジエージェントソフトウェアがクラウドに接続されていない場合に表示されることがあります。デフォルトでは、エッジエージェントソフトウェアは に ping リクエストを 1 分 AWS IoT Core ごとに送信し、3 分間待機します。応答がない場合、エッジエージェントソフトウェアは自動的にクラウドへの接続を再確立します。

問題の保存と転送

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

問題: 必要なすべての IAM アクセス許可**AccessDeniedException**を持つの受信

解決策: キャンペーンのデータパーティショニング用のストアアンドフォワード機能の早期アクセスリリースには、許可リストが必要です。サービスチームに連絡して、許可リストを通じてリソースに適切なアクセス許可があることを確認してください。

問題: Jobs にアップロード AWS IoT されたデータは を無視します。**endTime**

解決策: ジョブドキュメント`endtime`で無効な を指定しました。たとえば、 `endtime`は ISO 8601 UTC 形式に従っていません) 。 AWS IoT FleetWise エージェントログには、 という警告レベルのステートメントが存在する可能性があります`Malformed IoT Job endTime: customer configured endTime. Not setting endTime`。

問題: ジョブへの AWS IoT データアップロード**REJECTED**の実行ステータスがあります。

解決策: ジョブドキュメント`campaignArn`で無効な を指定しました。たとえば、車両で実行されていないキャンペーンの ARN を指定すると、 AWS IoT FleetWise エージェントログ`CampaignArn value in the received job document does not match the ARN of a Store and Forward campaign`に というエラーレベルのステートメントが表示される場合があります。

AWS IoT FleetWise のセキュリティ

で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 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。 AWS IoT FleetWise 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による AWS 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、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 AWS IoT FleetWise 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。セキュリティとコンプライアンスの目的を達成するために AWS IoT FleetWise を設定する方法を示します。また、 AWS IoT FleetWise 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。

内容

- AWS IoT FleetWise でのデータ保護
- を使用したアクセスの制御 AWS IoT FleetWise
- AWS IoT FleetWise の Identity and Access Management
- AWS IoT FleetWise のコンプライアンス検証
- AWS IoT FleetWise の耐障害性
- AWS IoT FleetWise のインフラストラクチャセキュリティ
- AWS IoT FleetWise の設定と脆弱性の分析
- AWS IoT FleetWise のセキュリティのベストプラクティス

AWS IoT FleetWise でのデータ保護

AWS 責任共有モデル、 AWS IoT FleetWise で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 AWS IoT FleetWise AWS CLIまたは他の AWS のサービス を操作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。

AWS IoT FleetWise は、車両データを AWS クラウドに送信するために、サポートされている車両ハードウェアを開発してインストールするエッジエージェントで使用することを目的としています。法管轄区域によっては、車両からデータを抽出することがデータプライバシー規制の対象となる場合があります。 AWS IoT FleetWise を使用して Edge Agent をインストールする前に、適用法に基づいてコンプライアンス義務を評価することを強くお勧めします。これには、法的に適切なプライバシー通知を提示し、車両データの抽出に必要な同意を得るために適用される法的要件が含まれます。

AWS IoT FleetWise での保管時の暗号化

車両から収集されたデータは、MQTT メッセージプロトコルを含む AWS IoT Core メッセージを介してクラウドに送信されます。 AWS IoT FleetWise はデータを Amazon Timestream データベースに配信します。Timestream 内のデータは暗号化されます。すべての AWS のサービス は、デフォルトで保管中のデータを暗号化します。詳細については、「Amazon S3 ユーザーガイド」の「暗号化によるデータの保護」および「Timestream for LiveAnalytics でのデータ保護」を参照してください。 Amazon S3

保管時の暗号化は AWS Key Management Service （ AWS KMS) と統合され、データの暗号化に使用される暗号化キーを管理します。カスタマーマネージドキーを使用して、 AWS IoT FleetWise によって収集されたデータを暗号化できます。暗号化キーを作成、管理、表示できます AWS KMS。詳細については、「 AWS Key Management Service デベロッパーガイド」の「What is AWS Key Management Service？」を参照してください。

転送中の暗号化

AWS IoT サービスと交換されるすべてのデータは、転送中に Transport Layer Security (TLS) を使用して暗号化されます。詳細については、「AWS IoT デベロッパーガイド」の「トランスポートセキュリティ」を参照してください。

また、 は認証と認可 AWS IoT Core をサポートしているため、 AWS IoT FleetWise リソースへのアクセスを安全に制御できます。車両は X.509 証明書を使用して、 AWS IoT FleetWise を使用するための認証 (サインイン) を取得し、 AWS IoT Core ポリシーを使用して、指定されたアクションを実行するための認可 (アクセス許可を持つ) を取得できます。詳細については、「the section called “車両のプロビジョニング”」を参照してください。

AWS IoT FleetWise でのデータ暗号化

データ暗号化とは、転送中 (AWS IoT FleetWise との間、およびゲートウェイとサーバーの間) および保管中 (ローカルデバイスまたは に保存中) のデータを保護することを意味します AWS のサービス。保管中のデータの保護には、クライアント側の暗号化を使用できます。

> **Note**
>
> AWS IoT FleetWise エッジ処理は、 AWS IoT FleetWise ゲートウェイ内でホストされ、ローカルネットワーク経由でアクセスできる APIs を公開します。これらの APIsは、 AWS IoT FleetWise Edge コネクタが所有するサーバー証明書によってバックアップされた TLS 接続を介して公開されます。これらの API では、クライアント認証にアクセス制御パスワードが使用されます。サーバー証明書のプライベートキーとアクセスコントロールパスワードはどちらもディスクに保存されます。 AWS IoT FleetWise エッジ処理は、保管中のこれらの認証情報のセキュリティのためにファイルシステムの暗号化に依存します。

サーバー側の暗号化とクライアント側の暗号化の詳細については、以下のトピックを参照してください。

内容

- AWS IoT FleetWise での保管時の暗号化
- AWS IoT FleetWise でのキー管理

AWS IoT FleetWise での保管時の暗号化

AWS IoT FleetWise は、データを AWS クラウドとゲートウェイに保存します。

AWS クラウドに保管中のデータ

AWS IoT FleetWise は、デフォルトで保管中のデータを暗号化 AWS のサービス する他の にデータを保存します。保管時の暗号化には AWS Key Management Service (AWS KMS) が統合され、これによって AWS IoT FleetWise のアセットのプロパティ値や集計値の暗号化に使用される暗号キーを管理します。カスタマーマネージドキーを使用して、 AWS IoT FleetWise のアセットプロパティ値と集計値を暗号化できます。暗号化キーを作成、管理、表示できます AWS KMS。

AWS 所有のキー またはカスタマーマネージドキーを選択してデータを暗号化できます。

仕組み

保管時の暗号化は と統合され、データの暗号化に使用される暗号化キー AWS KMS を管理します。

- AWS 所有のキー – デフォルトの暗号化キー。 AWS IoT FleetWise はこのキーを所有しています。このキーを表示または管理したり、 AWS アカウントで使用したりすることはできません。また、

AWS CloudTrail ログにキーに対するオペレーションを表示することはできません。このキーは追加料金なしで使用することができます。

- カスタマーマネージドキー - キーは、お客様が作成、所有、管理するアカウントに保存されます。ユーザーは、KMS キーに関する完全なコントロール権を持ちます。 AWS KMS 追加料金が適用されます。

AWS 所有のキー

AWS 所有のキー はアカウントに保存されません。これらは、multiple で使用するために が AWS 所有および管理する KMS キーのコレクションの一部です AWS アカウント。 AWS のサービス はデータを保護するために AWS 所有のキー を使用できます。

表示、管理、使用 AWS 所有のキー、またはそれらの使用を監査することはできません。ただし、データを暗号化するキーを保護するために何らかの操作を行ったり、プログラムを変更したりする必要はありません。

を使用する場合、料金は発生せず AWS 所有のキー、アカウントの AWS KMS クォータにもカウントされません。

カスタマーマネージドキー

カスタマーマネージドキーは、お客様が作成、所有、管理するアカウント内の KMS キーです。これらの KMS キーはお客様が完全に制御でき、次のような操作が可能です。

- キーポリシー、IAM ポリシー、グラントの確立と維持
- 有効化と無効化
- 暗号化マテリアルのローテーション
- タグの追加
- それらを参照するエイリアスの作成
- 削除のスケジュール設定

CloudTrail と Amazon CloudWatch Logs を使用して、 AWS IoT FleetWise が AWS KMS ユーザーに代わって に送信するリクエストを追跡することもできます。

カスタマーマネージドキーを使用している場合は、アカウントに保存されている KMS キーへのアクセス権を AWS IoT FleetWise に付与する必要があります。 AWS IoT FleetWise はエンベロープ暗

号化とキー階層を使用してデータを暗号化します。 AWS KMS 暗号化キーは、このキー階層のルートキーを暗号化するために使用されます。詳細については、「AWS Key Management Service デベロッパーガイド」の「エンベロープ暗号化」を参照してください。

次のポリシー例では、 AWS IoT FleetWise に AWS KMS キーを使用するアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "Service": "iotfleetwise.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Important

新しいセクションを KMS キーポリシーに追加するときは、ポリシー内の既存のセクションを変更しないでください。 AWS IoT FleetWise で暗号化が有効になっていて、次のいずれかに当てはまる場合、 AWS IoT FleetWise はデータに対してオペレーションを実行できません。

- KMS キーが無効または削除されている。
- サービスに対して KMS キーポリシーが正しく構成されていない。

ビジョンシステムデータに対する保管中の暗号化の使用

> **Note**
> ビジョンシステムデータはプレビューリリースであり、変更される可能性があります。

AWS IoT FleetWise アカウントで AWS KMS キーを有効にしたカスタマーマネージド暗号化があり、ビジョンシステムデータを使用する場合は、複雑なデータ型と互換性を持つように暗号化設定をリセットします。これにより、 AWS IoT FleetWise はビジョンシステムデータに必要な追加のアクセス許可を確立できます。

> **Note**
> ビジョンシステムデータの暗号化設定をリセットしていないと、デコーダーマニフェストが検証中のままになる可能性があります。

1. GetEncryptionConfiguration API オペレーションを使用して、 AWS KMS 暗号化が有効になっているかどうかを確認します。暗号化タイプが `FLEETWISE_DEFAULT_ENCRYPTION` の場合、追加のアクションは必要ありません。
2. 暗号化タイプが `KMS_BASED_ENCRYPTION` の場合は、PutEncryptionConfiguration API オペレーションを使用して暗号化タイプを `FLEETWISE_DEFAULT_ENCRYPTION` にリセットします。

   ```
   aws iotfleetwise put-encryption-configuration \
         --encryption-type FLEETWISE_DEFAULT_ENCRYPTION
   ```

3. PutEncryptionConfiguration API オペレーションを使用して、暗号化タイプを `KMS_BASED_ENCRYPTION` に再度有効化します。

   ```
   aws iotfleetwise put-encryption-configuration \
           --encryption-type KMS_BASED_ENCRYPTION \
           --kms-key-id kms_key_id
   ```

暗号化の有効化の詳細については、「AWS IoT FleetWise でのキー管理」を参照してください。

AWS IoT FleetWise でのキー管理

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

AWS IoT FleetWise クラウドキー管理

デフォルトでは、 AWS IoT FleetWise は AWS マネージドキー を使用して 内のデータを保護します AWS クラウド。カスタマーマネージドキーを使用して AWS IoT FleetWise のデータを暗号化するように設定を更新できます。() を使用して暗号化キーを作成、管理、表示できます AWS Key Management Service AWS KMS。

AWS IoT FleetWise は、 に保存されているカスタマーマネージドキーによるサーバー側の暗号化をサポートし AWS KMS 、次のリソースのデータを暗号化します。

AWS IoT FleetWise リソース	データタイプ	保管中にカスタマーマネージドキーで暗号化されるフィールド
シグナルカタログ		description
	属性	description、allowedValues、defaultValue、min、max
	アクチュエータ	description、allowedValues、min、max
	センサー	description、allowedValues、min、max
車両モデル (モデルマニフェスト)		description
デコーダーマニフェスト		description
	CanInterface	protocolName、protocolVersion

AWS IoT FleetWise リソース	データタイプ	保管中にカスタマーマネージドキーで暗号化されるフィールド
	ObdInterface	requestMessageId、dtcRequestIntervalSeconds、hasTransmissionEcu、obdStandard、pidRequestIntervalSeconds、useExtendedIds
	CanSignal	factor、isBigEndian、isSigned、length、messageId、offset、startBit
	ObdSignal	byteLength、offset、pid、pidResponseLength、scaling、serviceMode、startByte、bitMaskLength、bitRightShift
車両		attributes
キャンペーン		description
	conditionBasedCollectionScheme	expression、conditionLanguageVersion、minimumTriggerIntervalMs、triggerMode
	TimeBasedCollectionScheme	periodMs
状態テンプレート		description

> **Note**
>
> その他のデータとリソースは、 AWS IoT FleetWise によって管理されるキーによるデフォルトの暗号化を使用して暗号化されます。このキーは、 AWS IoT FleetWise アカウントに作成され、保存されます。

詳細については、「 AWS Key Management Service デベロッパーガイド」の「What is AWS Key Management Service ? 」を参照してください。

KMS キーによる暗号化の有効化 (コンソール)

AWS IoT FleetWise でカスタマーマネージドキーを使用するには、 AWS IoT FleetWise の設定を更新する必要があります。

KMS キーによる暗号化を有効にするには (コンソール)

1. AWS IoT FleetWise コンソールを開きます。
2. [設定] に移動します。
3. [暗号化] で、[編集] を選択して [暗号化の編集] ページを開きます。
4. 暗号化キータイプで、別の AWS KMS キーを選択するを選択します。これにより、 AWS KMS に保存されたカスタマーマネージドキーによる暗号化が有効になります。

> **Note**
>
> カスタマーマネージドキー暗号化は、 AWS IoT FleetWise リソースにのみ使用できます。これには、シグナルカタログ、車両モデル (モデルマニフェスト)、デコーダーマニフェスト、車両、フリート、キャンペーンが含まれます。

5. 次のいずれかのオプションを使用して、KMS キーを選択します。
   - 既存の KMS キーを使用するには - リストから KMS キーエイリアスを選択します。
   - 新しい KMS キーを作成するには – AWS KMS キーの作成を選択します。

   > **Note**
   >
   > これにより、 AWS KMS コンソールが開きます。KMS キーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

6. [保存] を選択して、設定を更新します。

KMS キーによる暗号化の有効化 (AWS CLI)

PutEncryptionConfiguration API オペレーションを使用して、 AWS IoT FleetWise アカウントの暗号化を有効にできます。次の例では、 を使用します AWS CLI。

暗号化を有効にするには、次のコマンドを実行します。

- *kms_key_id* を KMS キーの ID に置き換えます。

```
aws iotfleetwise put-encryption-configuration \
      --encryption-type KMS_BASED_ENCRYPTION \
      --kms-key-id kms_key_id
```

Example レスポンス

```
{
 "kmsKeyId": "customer_kms_key_id",
 "encryptionStatus": "PENDING",
 "encryptionType": "KMS_BASED_ENCRYPTION"
}
```

KMS キーポリシー

KMS キーを作成したら、少なくとも次のステートメントを KMS キーポリシーに追加して、 AWS IoT FleetWise と連携させる必要があります。KMS キーポリシーステートメント`iotfleetwise.amazonaws.com`の AWS IoT FleetWise サービスプリンシパルは、 AWS IoT FleetWise が KMS キーにアクセスすることを許可します。

```
{
  "Sid": "Allow FleetWise to encrypt and decrypt data when customer managed KMS key
 based encryption is enabled",
  "Effect": "Allow",
  "Principal": {
    "Service": "iotfleetwise.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:RevokeGrant"
  ],
  "Resource": "*"
```

```
}
```

セキュリティのベストプラクティスとして、KMS キーポリシーに aws:SourceArnおよびaws:SourceAccount条件キーを追加します。IAM グローバル条件キーは、 AWS IoT FleetWise がサービス固有のリソース Amazon リソースネーム (ARNs) にのみ KMS キーを使用するようにするaws:SourceArnのに役立ちます。

の値を設定する場合aws:SourceArn、常に である必要がありますarn:aws:iotfleetwise:us-east-1:account_id:*。これにより、KMS キーはこれに関するすべての AWS IoT FleetWise リソースにアクセスできます AWS アカウント。 AWS IoT FleetWise は、そのすべてのリソースについてアカウントごとに 1 つの KMS キーをサポートします AWS リージョン。に他の値を使用するSourceArnか、ARN リソースフィールドにワイルドカード (*) を使用しないと、 AWS IoT FleetWise が KMS キーにアクセスできなくなります。

の値はアカウント ID aws:SourceAccountです。これは、特定のアカウントでのみ使用できるように KMS キーをさらに制限するために使用されます。KMS キーに aws:SourceAccountおよびaws:SourceArn条件キーを追加する場合は、そのキーが他のサービスまたはアカウントで使用されていないことを確認してください。これにより、障害を回避できます。

次のポリシーには、サービスプリンシパル (サービスの識別子) と、 aws:SourceAccount とアカウント ID に基づいて使用するためにaws:SourceArn設定された AWS リージョン と が含まれます。

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "iotfleetwise.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "AWS-account-ID"
    },
    "ArnLike": {
```

```
        "aws:SourceArn": "arn:aws:iotfleetwise:region:AWS-account-ID:*"
      }
    }
}
```

AWS IoT FleetWise で使用する KMS キーポリシーの編集の詳細については、「 AWS Key Management Service デベロッパーガイド」の「キーポリシーの変更」を参照してください。

> **Important**
>
> KMS キーポリシーに新しいセクションを追加するときは、ポリシー内の既存のセクションを変更しないでください。 AWS IoT FleetWise で暗号化が有効になっていて、次のいずれかに当てはまる場合、 AWS IoT FleetWise はデータに対してオペレーションを実行できません。
>
> - KMS キーが無効または削除されている。
> - サービスに対して KMS キーポリシーが正しく構成されていない。

AWS KMS 暗号化のアクセス許可

AWS KMS 暗号化を有効にした場合は、 AWS IoT FleetWise APIs を呼び出すことができるように、ロールポリシーでアクセス許可を指定する必要があります。次のポリシーでは、すべての AWS IoT FleetWise アクションと AWS KMS 特定のアクセス許可へのアクセスを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotfleetwise:*",
        "kms:GenerateDataKey*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "*"
      ]
    }
```

```
  ]
}
```

ロールが暗号化 APIs を呼び出すには、次のポリシーステートメントが必要です。このポリシーステートメントは、 AWS IoT FleetWise からの アクション`PutEncryptionConfiguration`と`GetEncryptionConfiguration`アクションを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iotfleetwise:GetEncryptionConfiguration",
        "iotfleetwise:PutEncryptionConfiguration",
        "kms:GenerateDataKey*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS KMS キー削除後の復旧

AWS IoT FleetWise による暗号化を有効にした後に AWS KMS キーを削除する場合は、 AWS IoT FleetWise を再度使用する前に、すべてのデータを削除してアカウントをリセットする必要があります。API オペレーションのリストと削除を使用して、アカウントのリソースをクリーンアップできます。

アカウントのリソースをクリーンアップするには

1. リスト APIs `listResponseScope`パラメータを に設定して使用します`METADATA_ONLY`。これにより、リソース名や ARNs やタイムスタンプなどの他のメタデータを含むリソースのリストが提供されます。
2. delete APIs を使用して個々のリソースを削除します。

次の順序でリソースをクリーンアップする必要があります。

1. キャンペーン
   a. `listResponseScope` パラメータを に設定して、すべてのキャンペーンを一覧表示します`METADATA_ONLY`。
   b. キャンペーンを削除します。
2. フリートと車両
   a. `listResponseScope` パラメータが に設定されているすべてのフリートを一覧表示します`METADATA_ONLY`。
   b. `listResponseScope` パラメータを に設定して、各フリートのすべての車両を一覧表示します`METADATA_ONLY`。
   c. 各フリートからすべての車両の関連付けを解除します。
   d. フリートを削除します。
   e. 車両を削除します。
3. デコーダーマニフェスト
   a. `listResponseScope` パラメータを に設定して、すべてのデコーダーマニフェストを一覧表示します`METADATA_ONLY`。
   b. すべてのデコーダーマニフェストを削除します。
4. 車両モデル (モデルマニフェスト)
   a. `listResponseScope` パラメータを に設定して、すべての車両モデルを一覧表示します`METADATA_ONLY`。
   b. すべての車両モデルを削除します。
5. 状態テンプレート
   a. `listResponseScope` パラメータを に設定して、すべての状態テンプレートを一覧表示します`METADATA_ONLY`。
   b. すべての状態テンプレートを削除します。
6. シグナルカタログ
   a. すべてのシグナルカタログを一覧表示します。
   b. すべてのシグナルカタログを削除します。

を使用したアクセスの制御 AWS IoT FleetWise

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

以下のセクションでは、 AWS IoT FleetWise リソースへのアクセスとリソースからのアクセスを制御する方法について説明します。対象となる情報には、 AWS IoT FleetWise がキャンペーン中に車両データを転送できるように、アプリケーションにアクセス権を付与する方法が含まれます。また、Amazon S3 (S3) バケットまたは Amazon Timestream データベースとテーブルへのアクセスを許可してデータを保存する方法、または車両からデータを送信するために使用される MQTT メッセージ AWS IoT FleetWise へのアクセスを許可する方法についても説明します。

これらすべての形式のアクセスを管理するテクノロジーは AWS Identity and Access Management (IAM) です。IAM の詳細については、「IAM とは?」を参照してください。

内容

- MQTT トピックでデータを送受信する AWS IoT FleetWise アクセス許可を付与する
- Amazon S3 送信先 AWS IoT FleetWise へのアクセスを許可する
- Amazon Timestream 送信先 AWS IoT FleetWise へのアクセスを許可する
- を使用してコマンドのペイロードを生成する AWS IoT Device Management アクセス許可を付与する AWS IoT FleetWise

MQTT トピックでデータを送受信する AWS IoT FleetWise アクセス許可を付与する

MQTT トピックを使用すると、車両は AWS IoT MQTT メッセージブローカーを使用してデータを送信します。指定した MQTT トピックをサブスクライブする AWS IoT FleetWise アクセス許可を付与する必要があります。 AWS IoT ルールを使用してアクションを実行したり、データを他の送信先にルーティングしたりする場合は、IAM ロールにポリシーをアタッチして、 AWS IoT FleetWise がデータを IoT ルールに転送できるようにする必要があります。

さらに、他のアプリやデバイスは、車両データをほぼリアルタイムで受信するために指定したトピックにサブスクライブできます。これらのアプリやデバイスには、必要に応じてアクセス許可とアクセス許可を付与する必要があります。

MQTT の使用と必要なロールとアクセス許可の詳細については、以下を参照してください。

- デバイス通信プロトコル
- のルール AWS IoT
- 必要なアクセスを AWS IoT ルールに付与する
- ロールのアクセス許可を渡す

開始する前に、次の点を確認してください。

> **Important**
>
> - AWS IoT FleetWise の車両キャンペーンリソースを作成するときは、同じ AWS リージョンを使用する必要があります。 AWS リージョンを切り替えると、リソースへのアクセスに問題がある可能性があります。
> - AWS IoT FleetWise は、米国東部 (バージニア北部) および欧州 (フランクフルト) で利用できます。

を使用して AWS CLI 、MQTT メッセージングの信頼ポリシーを持つ IAM ロールを作成できます。IAM ロールを作成するには、次のコマンドを実行します。

信頼ポリシーを持つ IAM ロールを作成するには

- *IotTopicExecutionRole* を、作成するロールの名前に置き換えます。
- *trust-policy* は、信頼ポリシーを含む JSON ファイルに置き換えます。

```
aws iam create-role --role-name IotTopicExecutionRole --assume-role-policy-document
 file://trust-policy.json
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "mqttTopicTrustPolicy",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "iotfleetwise.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:iotfleetwise:region:account-id:campaign/campaign-name"
          ],
          "aws:SourceAccount": [
            "account-id"
          ]
        }
      }
    }
  ]
}
```

指定した MQTT トピックにメッセージを発行するアクセス許可を AWS IoT FleetWise に付与するアクセス許可ポリシーを作成します。アクセス許可を作成するには、次のコマンドを実行します。

アクセス許可ポリシーを作成するには

- *AWSIoTFleetwiseAccessIotTopicPermissionsPolicy* を、作成するポリシーの名前に置き換えます。
- *permissions-policy* は、アクセス許可ポリシーを含む JSON ファイルの名前に置き換えます。

```
aws iam create-policy --policy-name AWSIoTFleetwiseAccessIotTopicPermissionsPolicy --
policy-document file://permissions-policy.json
```

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "iot:Publish"
        ],
        "Resource": [
          "topic-arn"
```

```
        ]
      }
    ]
}
```

アクセス許可ポリシーを IAM ロールにアタッチするには

1. 出力から、アクセス許可ポリシーの Amazon リソースネーム (ARN) をコピーします。
2. IAM アクセス許可ポリシーを IAM ロールにアタッチするには、次のコマンドを実行します。

   - *permissions-policy-arn* は、前のステップでコピーした ARN に置き換えます。
   - *IotTopicExecutionRole* を、作成した IAM ロールの名前に置き換えます。

   ```
   aws iam attach-role-policy --policy-arn permissions-policy-arn --role-
   name IotTopicExecutionRole
   ```

詳細については、「IAM ユーザーガイド」の「AWS リソースのアクセス管理」を参照してください。

Amazon S3 送信先 AWS IoT FleetWise へのアクセスを許可する

Amazon S3 送信先を使用する場合、 は車両データを S3 バケットに AWS IoT FleetWise 配信し、オプションでデータ暗号化に所有している AWS KMS キーを使用できます。エラーログ記録が有効になっている場合、 は CloudWatch ロググループとストリームにもデータ配信エラー AWS IoT FleetWise を送信します。配信ストリームを作成するときは、IAM ロールが必要です。

AWS IoT FleetWise は、S3 送信先のサービスプリンシパルでバケットポリシーを使用します。バケットポリシーの追加方法の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。

次のアクセスポリシーを使用して、 AWS IoT FleetWise が S3 バケットにアクセスできるようにします。S3 バケットを所有していない場合、Amazon S3 アクションのリストに `s3:PutObjectAcl` を追加します。これにより、 によって配信されるオブジェクトへのフルアクセスがバケット所有者に付与されます AWS IoT FleetWise。バケット内のオブジェクトへのアクセスを保護する方法の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットポリシーの例」を参照してください。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotfleetwise.amazonaws.com"
        ]
      },
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotfleetwise.amazonaws.com"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::bucket-name/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "campaign-arn",
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

以下のバケットポリシーは、 AWS リージョン内のアカウントのすべてのキャンペーンを対象としています。

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

```
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotfleetwise.amazonaws.com"
        ]
      },
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "iotfleetwise.amazonaws.com"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::bucket-name/*",
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:iotfleetwise:region:account-id:campaign/*",
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

S3 バケットに KMS キーがアタッチされている場合、そのキーには以下のポリシーが必要です。キー管理の詳細については、Amazon Simple Storage Service ユーザーガイドのAWS Key Management Service 「キーによるサーバー側の暗号化 (SSE-KMS) を使用したデータの保護」を参照してください。

```
{
  "Version": "2012-10-17",
  "Effect": "Allow",
  "Principal": {
    "Service": "iotfleetwise.amazonaws.com"
```

```
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
   ],
  "Resource": "key-arn"
}
```

> **Important**
>
> バケットを作成すると、S3 は、デフォルトのアクセスコントロールリスト (ACL) を作成し、リソースに対する完全なコントロールをリソース所有者に付与します。 AWS IoT FleetWise が S3 にデータを配信できない場合は、S3 バケットの ACL を無効にしてください。詳細については、ACLs の無効化」および「オブジェクト所有権の適用」を参照してください。

Amazon Timestream 送信先 AWS IoT FleetWise へのアクセスを許可する

Timestream 送信先を使用すると、 は Timestream テーブルに車両データを AWS IoT FleetWise 配信します。が Timestream AWS IoT FleetWise にデータを送信できるようにするには、ポリシーを IAM ロールにアタッチする必要があります。

コンソールを使用してキャンペーンを作成すると、 AWS IoT FleetWise は必要なポリシーをロールに自動的にアタッチします。

> **Note**
>
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

開始する前に、次の点を確認してください。

> **Important**
>
> - AWS IoT FleetWise の Timestream リソースを作成するときは、同じ AWS リージョンを使用する必要があります。 AWS リージョンを切り替えると、Timestream リソースへのアクセスに問題がある可能性があります。

- AWS IoT FleetWise は、米国東部 (バージニア北部) 、欧州 (フランクフルト) 、アジアパシフィック (ムンバイ) で利用できます。
- サポートされているリージョンのリストについては、「AWS 全般のリファレンス」の「Timestream エンドポイントとクォータ」を参照してください。

- Timestream データベースが必要です。チュートリアルについては、「Amazon Timestream デベロッパーガイド」の「データベースの作成」を参照してください。
- 指定の Timestream データベースにテーブルが作成されている必要があります。チュートリアルについては、「Amazon Timestream デベロッパーガイド」の「テーブルの作成」を参照してください。

を使用して AWS CLI 、Timestream の信頼ポリシーを持つ IAM ロールを作成できます。IAM ロールを作成するには、次のコマンドを実行します。

信頼ポリシーを持つ IAM ロールを作成するには

- *TimestreamExecutionRole* は、作成するロールの名前に置き換えます。
- *trust-policy* を、信頼ポリシーを含む .json ファイルに置き換えます。

```
aws iam create-role --role-name TimestreamExecutionRole --assume-role-policy-document
 file://trust-policy.json
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "timestreamTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "iotfleetwise.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
           "aws:SourceArn": [
            "arn:aws:iotfleetwise:region:account-id:campaign/campaign-name"
```

```
            ],
            "aws:SourceAccount": [
             "account-id"
           ]
         }
       }
     }
   ]
}
```

アクセス許可ポリシーを作成して、Timestream にデータを書き込むアクセス許可を AWS IoT FleetWise に付与します。アクセス許可を作成するには、次のコマンドを実行します。

アクセス許可ポリシーを作成するには

- *AWSIoTFleetwiseAccessTimestreamPermissionsPolicy* は、作成するポリシーの名前に置き換えます。
- *permissions-policy* は、アクセス許可ポリシーを含む JSON ファイルの名前に置き換えます。

```
aws iam create-policy --policy-name AWSIoTFleetwiseAccessTimestreamPermissionsPolicy --
policy-document file://permissions-policy.json
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "timestreamIngestion",
      "Effect": "Allow",
      "Action": [
        "timestream:WriteRecords",
        "timestream:Select",
        "timestream:DescribeTable"
      ],
      "Resource": "table-arn"
    },
    {
      "Sid": "timestreamDescribeEndpoint",
      "Effect": "Allow",
      "Action": [
```

```
        "timestream:DescribeEndpoints"
      ],
      "Resource": "*"
    }
  ]
}
```

アクセス許可ポリシーを IAM ロールにアタッチするには

1. 出力から、アクセス許可ポリシーの Amazon リソースネーム (ARN) をコピーします。
2. IAM アクセス許可ポリシーを IAM ロールにアタッチするには、次のコマンドを実行します。
   - *permissions-policy-arn* は、前のステップでコピーした ARN に置き換えます。
   - *TimestreamExecutionRole* は、作成した IAM ロールの名前に置き換えます。

```
aws iam attach-role-policy --policy-arn permissions-policy-arn --role-
name TimestreamExecutionRole
```

詳細については、「IAM ユーザーガイド」の「AWS リソースのアクセス管理」を参照してください。

を使用してコマンドのペイロードを生成する AWS IoT Device Management アクセス許可を付与する AWS IoT FleetWise

コマンド機能を使用してコマンド実行を開始すると、 AWS IoT Device Management は受信リクエストからコマンドとコマンドパラメータを取得します。次に、 AWS IoT FleetWise リソースにアクセスしてリクエストを検証し、ペイロードを生成するアクセス許可が必要です。その後、ペイロードは MQTT AWS IoT Device Management 経由で車両に送信され、車両がサブスクライブしているコマンドリクエストトピックに送信されます。

まず、ペイロードの生成 AWS IoT Device Management に必要なアクセス許可を付与する IAM ロールを作成する必要があります。次に、 `roleArn`フィールドを使用して、このロールの ARN を `CreateCommand` API に提供します。以下に、いくつかのポリシーの例を示します。

> **Important**
>
> IAM ロールには、車両とコマンドリソースを作成したロール AWS リージョン と同じ を使用する必要があります。切り替えると AWS リージョン、リソースへのアクセスに問題がある可能性があります。

IAM ロールには、次の信頼ポリシーが必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RemoteCommandsTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

すべての車両にアクセス許可を付与する (IoT モノ)

次の例は、 AWS IoT モノとして登録されているすべての車両のペイロードを生成するアクセス許可を付与する方法を示しています。

> **Note**
>
> - このポリシーは過度に許可される場合があります。最小権限の原則を使用して、必要なアクセス許可のみを付与します。
> - 代わりにアクセス許可を拒否するには、IAM ポリシー`"Effect": "Deny"`の `"Effect": "Allow"`を に変更します。

この例では、次のように置き換えます。

- AWS IoT FleetWise リソースを使用している AWS リージョン で *<AWS_REGION>*。

- *<ACCOUNT_ID>*。 AWS アカウント

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotfleetwise:GenerateCommandPayload",
            "Resource": "*"
        }
    ]
}
```

特定の車両にアクセス許可を付与する (IoT モノ)

次の例は、 AWS IoT モノとして登録された特定の車両のペイロードを生成するアクセス許可を付与する方法を示しています。

この例では、次のように置き換えます。

- AWS IoT FleetWise リソースを使用している AWS リージョン で *<AWS_REGION>*。
- *<ACCOUNT_ID>*。 AWS アカウント
- 車両の IoT モノの名前が の *<VEHICLE_NAME>*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotfleetwise:GenerateCommandPayload",
            "Resource": "arn:aws:iot:<AWS_REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>"
        }
    ]
}
```

特定の車両とシグナルにアクセス許可を付与する

次の例は、特定の車両のアクチュエータのペイロードを生成するアクセス許可を付与する方法を示しています。

この例では、次のように置き換えます。

- AWS IoT FleetWise リソースを使用している AWS リージョン で *<AWS_REGION>*。
- *<ACCOUNT_ID>*。 AWS アカウント
- *<VEHICLE_NAME>* と車両の IoT モノの名前。
- *<Vehicle.actuator2> ############ <SIGNAL_FQN#*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "iotfleetwise:GenerateCommandPayload",
            "Resource": "arn:aws:iot:<AWS_REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "iotfleetwise:Signals": ["<SIGNAL_FQN>"]
                }
            }
        }
    ]
}
```

特定の車両と状態テンプレートにアクセス許可を付与する

次の例は、特定の車両および状態テンプレートのペイロードを生成するアクセス許可を付与する方法を示しています。

この例では、次のように置き換えます。

- *<AWS_REGION>* は、 AWS IoT FleetWise リソースを使用している です AWS リージョン 。
- *<ACCOUNT_ID>* はお客様の AWS アカウント 番号です。
- *<VEHICLE_NAME>* は、車両の IoT モノの名前です。
- *<STATE_TEMPLATE_ID>* と状態テンプレートの識別子。

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

```
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "iotfleetwise:GenerateCommandPayload",
            "Resource": [
                "arn:aws:iot:<AWS_REGION>:<ACCOUNT_ID>:thing/<VEHICLE_NAME>",
                "arn:aws:iotfleetwise:<AWS_REGION>:<ACCOUNT_ID>:state-
template/<STATE_TEMPLATE_ID>"]
        }
    ]
}
```

カスタマーマネージド KMS キーを使用するためのアクセス許可を付与する

カスタマーマネージド KMS キーを有効にしている場合 AWS IoT FleetWise、次の例はペイロードを生成するアクセス許可を付与する方法を示しています。

この例では、次のように置き換えます。

- AWS IoT FleetWise リソースを使用している AWS リージョン で *<AWS_REGION>*。
- *<ACCOUNT_ID>*。 AWS アカウント
- *<KMS_KEY_ID>* と KMS キーの ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iotfleetwise:GenerateCommandPayload",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:<AWS_REGION>:<ACCOUNT_ID>:key/<KMS_KEY_ID>"
        }
    ]
}
```

AWS IoT FleetWise の Identity and Access 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 AWS IoT FleetWise リソースの使用を許可する (アクセス許可を付与する) 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
- IoT FleetWise AWS IoT が IAM と連携する方法
- AWS IoT FleetWise のアイデンティティベースのポリシーの例
- AWS IoT FleetWise アイデンティティとアクセスのトラブルシューティング
- AWS IoT FleetWise API アクションとリソースリファレンス

対象者

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

サービスユーザー – AWS IoT FleetWise サービスを使用してジョブを実行する場合、管理者は必要な認証情報とアクセス許可を提供します。さらに多くの AWS IoT FleetWise 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、管理者に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。 AWS IoT FleetWise の機能にアクセスできない場合は、「AWS IoT FleetWise アイデンティティ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 AWS IoT FleetWise リソースを担当している場合は、通常、 AWS IoT FleetWise へのフルアクセスがあります。サービスユーザーがどの AWS IoT FleetWise 機能やリソースにアクセスするかを決め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点検して、IAM の基本概念を理解してください。会社が AWS IoT FleetWise で IAM を使用する方法の詳細については、「」を参照してくださいIoT FleetWise AWS IoT が IAM と連携する方法。

IAM 管理者 – IAM 管理者は、 AWS IoT FleetWise 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 AWS IoT FleetWise 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、「」を参照してください[AWS IoT FleetWise のアイデンティティベースのポリシーの例](#)。

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 (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 Software Development Kit (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 内のアイデンティティです。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 内のアイデンティティです。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。 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、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 AWS アカウント をグループ化して一元管理するためのサービスです。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。

IoT FleetWise AWS IoT が IAM と連携する方法

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

AWS IoT FleetWise で使用できる IAM 機能

IAM 機能	AWS IoT FleetWise 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

IAM 機能	AWS IoT FleetWise のサポート
ACL	いいえ
ABAC (ポリシー内のタグ)	部分的
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	いいえ
サービスリンクロール	いいえ

AWS IoT FleetWise 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。

AWS IoT FleetWise 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。

AWS IoT FleetWise のアイデンティティベースのポリシーの例

AWS IoT FleetWise 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、「」を参照してくださいAWS IoT FleetWise のアイデンティティベースのポリシーの例。

AWS IoT FleetWise 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。

AWS IoT FleetWise のポリシーアクション

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。

AWS IoT FleetWise 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AWS IoT FleetWise で定義されるアクション」を参照してください。

AWS IoT FleetWise のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
iotfleetwise
```

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": [
      "iotfleetwise:action1",
      "iotfleetwise:action2"
]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`List` という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "iotfleetwise:List*"
```

AWS IoT FleetWise 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、「」を参照してくださいAWS IoT FleetWise のアイデンティティベースのポリシーの例。

AWS IoT FleetWise 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": "*"
```

AWS IoT FleetWise リソースタイプとその ARNsAWS IoT FleetWise で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、AWS IoT FleetWise で定義されるアクション」を参照してください。

AWS IoT FleetWise 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、「」を参照してくださいAWS IoT FleetWise のアイデンティティベースのポリシーの例。

AWS IoT FleetWise 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。

AWS IoT FleetWise 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 AWS IoT FleetWise 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、AWS IoT FleetWise で定義されるアクション」を参照してください。

AWS IoT FleetWise 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、「」を参照してください[AWS IoT FleetWise のアイデンティティベースのポリシーの例](#)。

AWS IoT FleetWise 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。

AWS IoT FleetWise を使用した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: 一部

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。

> **Note**
>
> AWS IoT FleetWise は`iam:PassRole`、 `CreateCampaign` API オペレーションに必要な のみをサポートします。

AWS IoT FleetWise 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 を使用する場合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は、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することができます 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。

AWS IoT FleetWise のクロスサービスプリンシパルアクセス許可

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。

AWS IoT FleetWise のサービスロール

サービスロールのサポート: なし

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**
>
> サービスロールのアクセス許可を変更すると、 AWS IoT FleetWise 機能が破損する可能性があります。 AWS IoT FleetWise が指示する場合にのみ、サービスロールを編集します。

AWS IoT FleetWise 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。そのサービスのサービスリンクロールに関するドキュメントを参照するには、「はい」のリンクを選択します。

AWS IoT FleetWise のサービスリンクロールの使用

AWS IoT FleetWise は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスリンクロールは、AWS IoT Fleetwise に直接リンクされる一意のタイプの IAM ロールです。サービスリンクロールは AWS IoT FleetWise によって事前定義され、AWS IoT FleetWise から Amazon CloudWatch にメトリクスを送信するために必要なアクセス許可が含まれています。詳細については、「Amazon CloudWatch で AWS IoT FleetWise をモニタリングする」を参照してください。

サービスリンクロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、AWS IoT FleetWise を簡単にセットアップできます。AWS IoT FleetWise は、サービスリンクロールのアクセス許可を定義します。特に定義されていない限り、AWS IoT FleetWise のみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。このアクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、最初に関連リソースを削除する必要があります。これにより、リソースへのアクセス許可が誤って削除されることがなくなるため、AWS IoT FleetWise リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」を持つサービスを探します。そのサービスのサービスリンクロールに関するドキュメントを参照するには、「はい」のリンクを選択します。

AWS IoT FleetWise のサービスリンクロールのアクセス許可

AWS IoT FleetWise では、AWSServiceRoleForIoTFleetWise という名前のサービスリンクロールが使用されます。これは、AWS IoT FleetWise に用意されているすべてのアクセス許可に使用される AWS マネージドポリシーです。

サービスリンクロール AWSServiceRoleForIoTFleetWise は、次のサービスを信頼してそのロールを引き受けます。

- `IoTFleetWise`

AWSIoTFleetwiseServiceRolePolicy という名前のロールのアクセス許可ポリシーは、指定されたリソースで次のアクションを完了する許可を AWS IoT FleetWise に与えます。

- アクション: リソース `*` での `cloudwatch:PutMetricData`

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロールのアクセス許可」を参照してください。

AWS IoT FleetWise のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。AWS IoT FleetWise コンソール、、AWS CLIまたは AWS API にアカウントを登録すると、AWS IoT FleetWise によってサービスにリンクされたロールが作成されます。詳細については、「AWS IoT FleetWise 設定を構成する」を参照してください。

AWS IoT FleetWise でのサービスリンクロールの作成 (コンソール)

サービスリンクロールを手動で作成する必要はありません。AWS IoT FleetWise コンソール、CLI、または AWS API AWS にアカウントを登録すると、AWS IoT FleetWise によってサービスにリンクされたロールが作成されます。

AWS IoT FleetWise のサービスリンクロールの編集

サービスリンクロール AWSServiceRoleForIoTFleetWise は、AWS IoT FleetWise で編集することはできません。作成済みのサービスリンクロールは、さまざまなエンティティによって参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

サービスリンク役割のクリーンアップ

IAM を使用してサービスにリンクされた役割を削除するには最初に、その役割で使用されているリソースをすべて削除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに AWS IoT FleetWise でロールが使用されていると、削除に失敗することがあります。失敗した場合は数分待ってから操作を再試行してください。コンソール、 AWS CLI、または AWS API を使用してservice-linked-roleを削除する方法については、IAM ユーザーガイドの「サービスにリンクされたロールの使用」を参照してください。

このサービスリンクロールを削除した後で再作成する必要が生じた場合は、AWS IoT FleetWise にアカウントを登録できます。これで、AWS IoT FleetWise によってサービスリンクロールが自動的に再作成されます。

AWS IoT FleetWise のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには、 AWS IoT FleetWise 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。

各リソースタイプの ARN の形式など、 AWS IoT FleetWise で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のAWS IoT FleetWise 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。 ARNs

トピック

- ポリシーに関するベストプラクティス
- AWS IoT FleetWise 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
- Amazon Timestream 内のリソースへのアクセス

ポリシーに関するベストプラクティス

アイデンティティベースのポリシーは、アカウント内で誰かが AWS IoT FleetWise 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 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。

AWS IoT FleetWise コンソールの使用

AWS IoT FleetWise 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 AWS IoT FleetWise 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 AWS IoT FleetWise コンソールを使用できるようにするには、 AWS IoT FleetWise `ConsoleAccess`または `ReadOnly` AWS 管理ポリシーもエンティティにアタッチします。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": "*"
        }
    ]
}
```

Amazon Timestream 内のリソースへのアクセス

AWS IoT FleetWise を使用する前に、 AWS アカウント、IAM、Amazon Timestream リソースを登録して、 AWS クラウド ユーザーに代わって車両データを に送信するアクセス許可を AWS IoT FleetWise に付与する必要があります。登録するには以下が必要です。

- Amazon Timestream データベース。
- 指定の Amazon Timestream データベースに作成されたテーブル。
- AWS IoT FleetWise が Amazon Timestream にデータを送信できるようにする IAM ロール。

手順やポリシーの例などの詳細については、「」を参照してください[AWS IoT FleetWise 設定を構成する](#)。

AWS IoT FleetWise アイデンティティとアクセスのトラブルシューティング

以下の情報は、 AWS IoT FleetWise と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- AWS IoT FleetWise 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
- 自分の 以外のユーザーに my AWS IoT FleetWise リソース AWS アカウント へのアクセスを許可したい

AWS IoT FleetWise 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。

次の例は、`mateojackson` という IAM ユーザーがコンソールを使用して架空の *`myVehicle`* リソースに関する詳細を表示しようとしたとき、`iotfleetwise:`*`GetVehicleStatus`* アクセス許可がない場合に発生するエラーを示しています。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotfleetwise:GetVehicleStatus on resource: myVehicle
```

この場合、Mateo は、`iotfleetwise:`*`GetVehicleStatus`* アクションを使用して *`myVehicle`* リソースにアクセスできるように、管理者にポリシーの更新を依頼します。

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 AWS IoT FleetWise 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アクセス許可が必要です。

次の例は、`marymajor` という IAM ユーザーがコンソールを使用して AWS IoT FleetWise でアクションを実行しようとした場合に発生するエラーを示しています。ただし、このアクションをサービスで実行するには、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。

自分の 以外のユーザーに my AWS IoT FleetWise リソース AWS アカウント 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:

- AWS IoT FleetWise がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいIoT FleetWise AWS IoT が IAM と連携する方法。
- 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 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。

AWS IoT FleetWise API アクションとリソースリファレンス

IAM アイデンティティのポリシーを使用してアクセスを管理する場合は、次の表を参照として使用できます。この表は、各 AWS IoT FleetWise API、アクションを実行するためのアクセス許可を付与できる対応するアクション、およびアクセス許可を付与できる AWS リソースを示しています。

ポリシーの`Action`フィールドでアクションを指定し、ポリシーの`Resource`フィールドでリソースの値を指定します。アクションを指定するには、`iotfleetwise:`プレフィックスの後にアクション名を付けます。例えば、`iotfleetwise:CreateSignalCatalog`。

現在、 AWS IoT FleetWise は次のアクション、リソース、および条件キーをサポートしています。

スクロールバーを使用して、残りのテーブルを表示します。

AWS IoT FleetWise アクション	必要な許可	リソース
AssociateVehicleFleet	iotfleetwise:AssociateVehicleFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id* arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*
CreateCampaign	iotfleetwise:CreateCampaign	arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name* arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*

AWS IoT FleetWise アクション	必要な許可	リソース
		arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*
CreateDecoderManifest	iotfleetwise:CreateDecoderManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name*
CreateFleet	iotfleetwise:CreateFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id* arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
CreateModelManifest	iotfleetwise:CreateModelManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
CreateSignalCatalog	iotfleetwise:CreateSignalCatalog	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*

AWS IoT FleetWise アクション	必要な許可	リソース
CreateStateTemplate	iotfleetwise:CreateStateTemplate	arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id* arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
CreateVehicle	iotfleetwise:CreateVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
BatchCreateVehicle	iotfleetwise:CreateVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
DeleteCampaign	iotfleetwise:DeleteCampaign	arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name*

AWS IoT FleetWise アクション	必要な許可	リソース
DeleteDecoderManifest	iotfleetwise:DeleteDecoderManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
DeleteFleet	iotfleetwise:DeleteFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*
DeleteModelManifest	iotfleetwise:DeleteModelManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
DeleteSignalCatalog	iotfleetwise:DeleteSignalCatalog	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
DeleteStateTemplate	iotfleetwise:DeleteStateTemplate	arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*
DeleteVehicle	iotfleetwise:DeleteVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*
DisassociateVehicleFleet	iotfleetwise:DisassociateVehicleFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*
GetCampaign	iotfleetwise:GetCampaign	arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name*

AWS IoT FleetWise アクション	必要な許可	リソース
GetDecoderManifest	iotfleetwise:GetDecoderManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
GetEncryptionConfiguration	iotfleetwise:GetEncryptionConfiguration	
GetFleet	iotfleetwise:GetFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*
GetLoggingOptions	iotfleetwise:GetLoggingOptions	
GetModelManifest	iotfleetwise:GetModelManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name*
GetRegisterAccountStatus	iotfleetwise:GetRegisterAccountStatus	
GetSignalCatalog	iotfleetwise:GetSignalCatalog	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
GetStateTemplate	iotfleetwise:GetStateTemplate	arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*
GetVehicle	iotfleetwise:GetVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*
GetVehicleStatus	iotfleetwise:GetVehicleStatus	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*

AWS IoT FleetWise アクション	必要な許可	リソース
ImportDecoderManifest	iotfleetwise:ImportDecoderManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
ImportSignalCatalog	iotfleetwise:ImportSignalCatalog	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
ListCampaigns	iotfleetwise:ListCampaigns	
ListDecoderManifestNetworkInterfaces	iotfleetwise:ListDecoderManifestNetworkInterfaces	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
ListDecoderManifests	iotfleetwise:ListDecoderManifests	
ListDecoderManifestSignals	iotfleetwise:ListDecoderManifestSignals	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*
ListFleets	iotfleetwise:ListFleets	
ListFleetsForVehicle	iotfleetwise:ListFleetsForVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id*
ListModelManifestNodes	iotfleetwise:ListModelManifestNodes	arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name*
ListModelManifests	iotfleetwise:ListModelManifests	

AWS IoT FleetWise アクション	必要な許可	リソース
ListSignalCatalogNodes	iotfleetwise:ListSignalCatalogNodes	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
ListSignalCatalogs	iotfleetwise:ListSignalCatalogs	
ListStateTemplates	iotfleetwise:ListStateTemplates	
ListVehicles	iotfleetwise:ListVehicles	
ListVehiclesInFleet	iotfleetwise:ListVehiclesInFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*

AWS IoT FleetWise アクション	必要な許可	リソース
ListTagsForResource	iotfleetwise:ListTagsForResource	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id* arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name* arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*
PutEncryptionConfiguration	iotfleetwise:PutEncryptionConfiguration	
PutLoggingOptions	iotfleetwise:PutLoggingOptions	
RegisterAccount	iotfleetwise:RegisterAccount	

AWS IoT FleetWise アクション	必要な許可	リソース
TagResource	iotfleetwise:TagResource	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id* arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name* arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*

AWS IoT FleetWise アクション	必要な許可	リソース
UntagResource	iotfleetwise:UntagResource	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id* arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name* arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*
UpdateCampaign	iotfleetwise:UpdateCampaign	arn:*partition* :iotfleetwise:*region* : *account_id* :campaign/*campaign-name*
UpdateDecoderManifest	iotfleetwise:UpdateDecoderManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*

AWS IoT FleetWise アクション	必要な許可	リソース
UpdateFleet	iotfleetwise:UpdateFleet	arn:*partition* :iotfleetwise:*region* : *account_id* :fleet/*fleet-id*
UpdateModelManifest	iotfleetwise:UpdateModelManifest	arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name*
UpdateSignalCatalog	iotfleetwise:UpdateSignalCatalog	arn:*partition* :iotfleetwise:*region* : *account_id* :signal-catalog/*name*
UpdateStateTemplate	iotfleetwise:UpdateStateTemplate	arn:*partition* :iotfleetwise:*region* : *account_id* :state-template/*state-template-id*
UpdateVehicle	iotfleetwise:UpdateVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*

AWS IoT FleetWise アクション	必要な許可	リソース
BatchUpdateVehicle	iotfleetwise:UpdateVehicle	arn:*partition* :iotfleetwise:*region* : *account_id* :Vehicle/*Vehicle-id* arn:*partition* :iotfleetwise:*region* : *account_id* :model-manifest/*name* arn:*partition* :iotfleetwise:*region* : *account_id* :decoder-manifest/*name*

AWS IoT FleetWise のコンプライアンス検証

> **Note**
> AWS IoT FleetWise は AWS コンプライアンスプログラムの対象ではありません。

AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスAWS のサービス 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) など) にわたるセキュリティコントロールを保護および 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。

AWS IoT FleetWise 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。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。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。

> **Note**
>
> AWS IoT FleetWise によって処理されたデータは、Amazon Timestream データベースに保存されます。Timestream は、他の AWS アベイラビリティーゾーンまたはリージョンへのバックアップをサポートしています。Timestream SDK を使用して、データにクエリを実行し、任意の宛先に保存する独自のアプリケーションを作成することもできます。
> Amazon Timestream の詳細については、「Amazon Timestream Developer Guide」を参照してください。
> Amazon Timestream は、アジアパシフィック (ムンバイ) リージョンでは利用できません。

AWS IoT FleetWise 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 AWS IoT FleetWise は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で AWS IoT FleetWise にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。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。

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、一時的な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。

これらの API オペレーションは任意のネットワークの場所から呼び出すことができますが、 AWS IoT FleetWise はリソースベースのアクセスポリシーをサポートしており、ソース IP アドレスに基づく制限を含めることができます。 AWS IoT FleetWise ポリシーを使用して、特定の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントまたは特定の VPCs からのアクセスを制御する

こともできます。これにより、実質的に、ネットワーク内の特定の VPC からのみ、特定の AWS IoT FleetWise リソースへの AWS ネットワークアクセスが分離されます。

トピック

- インターフェイス VPC エンドポイントを介した AWS IoT FleetWise への接続

インターフェイス VPC エンドポイントを介した AWS IoT FleetWise への接続

インターネット経由で接続するのではなく、仮想プライベートクラウド (AWS VPC) のインターフェイス VPC エンドポイント (PrivateLink) を使用して、 AWS IoT FleetWise に直接接続できます。インターフェイス VPC エンドポイントを使用する場合、VPC と AWS IoT FleetWise 間の通信は AWS ネットワーク内で完全に行われます。各 VPC エンドポイントは、VPC サブネット内のプライベート IP アドレスを持つ 1 つ以上の Elastic Network Interface (ENI) で表されます。

インターフェイス VPC エンドポイントは、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続なしで、VPC を AWS IoT FleetWise に直接接続します。VPC 内のインスタンスは、 AWS IoT FleetWise API と通信するためにパブリック IP アドレスを必要としません。

VPC を介して AWS IoT FleetWise を使用するには、VPC 内のインスタンスから接続するか、 AWS Virtual Private Network (VPN) または を使用してプライベートネットワークを VPC に接続する必要があります AWS Direct Connect。Amazon VPN については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPN 接続」を参照してください。詳細については AWS Direct Connect、「 AWS Direct Connect ユーザーガイド」の「接続の作成」を参照してください。

コンソールまたは AWS Command Line Interface （ AWS CLI) コマンドを使用して AWS 、インターフェイス VPC エンドポイントを作成して AWS IoT FleetWise に接続できます。詳細については、「インターフェイスエンドポイントの作成」を参照してください。

インターフェイス VPC エンドポイントを作成した後、エンドポイントのプライベート DNS ホスト名を有効にすると、default AWS IoT FleetWise エンドポイントは VPC エンドポイントに解決されます。 AWS IoT FleetWise のデフォルトのサービス名エンドポイントは、次の形式です。

```
iotfleetwise.Region.amazonaws.com
```

プライベート DNS ホスト名を有効にしない場合、Amazon VPC は次の形式で使用できる DNS エンドポイント名を提供します。

```
VPCE_ID.iotfleetwise.Region.vpce.amazonaws.com
```

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

AWS IoT FleetWise は、VPC 内のすべての API アクションの呼び出しをサポートしています。

VPC エンドポイントポリシーを VPC エンドポイントにアタッチして、IAM プリンシパルのアクセスを制御できます。また、セキュリティグループを VPC エンドポイントに関連付けて、ネットワークトラフィックの送信元と送信先 (IP アドレスの範囲など) に基づいてインバウンドとアウトバウンドのアクセスを制御することもできます。詳細については、「VPC エンドポイントによるサービスのアクセスコントロール」を参照してください。

> **Note**
>
> AWS IoT FleetWise は、デュアルスタックモードですべての VPC エンドポイントをサポートします。サービスエンドポイントの詳細については、AWS 「 IoT FleetWise エンドポイントとクォータ」を参照してください。

AWS IoT FleetWise 用の VPC エンドポイントポリシーの作成

Amazon VPC エンドポイント for AWS IoT FleetWise のポリシーを作成して、以下を指定できます。

- アクションを実行できるプリンシパルまたは実行できないプリンシパル
- 実行できるアクションまたは実行できないアクション

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントによるサービスのアクセスコントロール」を参照してください。

Example – 指定された AWS アカウントからのすべてのアクセスを拒否する VPC エンドポイントポリシー

次の VPC エンドポイントポリシーは、エンドポイントを使用した AWS アカウント *123456789012* のすべての API コールを拒否します。

```
{
    "Statement": [
```

```
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Example - 指定した IAM プリンシパル (ユーザー) への VPC アクセスのみを許可する VPC エンドポイントポリシー

次の VPC エンドポイントポリシーでは、 AWS アカウント *123456789012* のユーザー *lijuan* へのフルアクセスのみを許可します。他のすべての IAM プリンシパルによるエンドポイントへのアクセスは拒否されます。

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/lijuan"
                ]
            }
        }]
}
```

Example – AWS IoT FleetWise アクションの VPC エンドポイントポリシー

以下は、 AWS IoT FleetWise のエンドポイントポリシーの例です。エンドポイントにアタッチすると、このポリシーは、*123456789012* の IAM ユーザー fleetWise の AWS アカウント 一覧表示された AWS IoT FleetWise アクションへのアクセスを許可します。 FleetWise *fleetWise*

```
{
    "Statement": [
        {
             "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/fleetWise"
                },
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "iotfleetwise:ListFleets",
                "iotfleetwise:ListCampaigns",
                "iotfleetwise:CreateVehicle",
            ]
           }
    ]
}
```

AWS IoT FleetWise の設定と脆弱性の分析

IoT 環境は、多様な機能を持ち、存続期間が長く、地理的に分散される多数のデバイスで設定されることがあります。このような特性によってデバイスのセットアップが複雑になり、エラーを起こしやすくなります。また、デバイスの計算能力、メモリ、ストレージの機能には制約があることが多いため、デバイスでの暗号化や他の形式のセキュリティの使用は制限されます。多く場合、デバイスは既知の脆弱性を持つソフトウェアを使用しています。これらの要因により、IoT FleetWise のデータを収集する車両など、 AWS IoT デバイスはハッカーにとって魅力的なターゲットとなり、継続的に保護することが困難になります。

設定と IT コントロールは、 AWS お客様と当社のお客様との間の責任共有です。詳細については、AWS 「 責任共有モデル」を参照してください。

AWS IoT FleetWise のセキュリティのベストプラクティス

AWS IoT FleetWise には、独自のセキュリティポリシーを開発および実装する際に考慮すべきセキュリティ機能が多数用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるため、処方箋ではなく、あくまで有用な検討事項とお考えください。

のセキュリティの詳細については、「 AWS IoT デベロッパーガイド」の「 のセキュリティのベストプラクティス AWS IoT Core AWS IoT 」を参照してください。

最小限のアクセス許可を付与する

IAM ロールの最小限のアクセス許可セットを使用して、最小特権の原則に従います。IAM ポリシーの `Action` プロパティおよび `Resource` プロパティに対する `*` ワイルドカードの使用を制限します。代わりに、可能な場合はアクションとリソースの有限セットを宣言します。最小特権およびその他のポリシーのベストプラクティスの詳細については、「the section called “ポリシーに関するベストプラクティス”」を参照してください。

機密情報を記録しない

認証情報やその他の個人を特定できる情報 (PII) のログを記録しないようにしてください。次の安全対策を実施することをお勧めします。

- デバイス名に機密情報を使用しない。
- キャンペーン、デコーダーマニフェスト、車両モデル、シグナルカタログの名前、車両とフリートの IDs など、 AWS IoT FleetWise リソースの名前と IDs に機密情報を使用しないでください。

AWS CloudTrail を使用して API コール履歴を表示する

セキュリティ分析と運用上のトラブルシューティングの目的で、アカウントで行われた AWS IoT FleetWise API コールの履歴を表示できます。アカウントで行われた AWS IoT FleetWise API コールの履歴を受信するには、 で CloudTrail をオンにします AWS Management Console。詳細については、「the section called “CloudTrail ログ”」を参照してください。

デバイスのクロックを同期させる

デバイスの時刻を正確に保つことが重要です。X.509 証明書には有効期限の日時があります。デバイスのクロックは、サーバー証明書が現在も有効であることを確認するために使用されます。時間の経過とともにデバイスのクロックがドリフトしたり、バッテリが放電したりする可能性があります。

詳細については、「AWS IoT Core デベロッパーガイド」の「[Keep your device's clock in sync] (デバイスのクロックを同期させる)」ベストプラクティスを参照してください。

Monitor AWS IoT FleetWise

モニタリングは、 AWS IoT FleetWise およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 AWS IoT FleetWise をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツール AWS を提供します。

- Amazon CloudWatch は、 AWS リソースと AWS で実行しているアプリケーションをリアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したしきい値にメトリクスが達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon EC2 インスタンス、CloudTrail、その他のソースからのログファイルをモニタリングおよび保存し、アクセスすることができます。CloudWatch Logs は、ログファイル内の情報をモニタリングし、特定のしきい値が満たされたときに通知します。高い耐久性を備えたストレージにログデータをアーカイブすることも可能です。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって行われた、またはそのアカウントに代わって実行された API コールと関連イベントをキャプチャします。次に、ユーザー指定の Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース 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 ユーザーガイドをご参照ください。

Amazon CloudWatch で AWS IoT FleetWise をモニタリングする

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

Amazon CloudWatch メトリクスは、 AWS リソースとそのパフォーマンスをモニタリングする方法です。 AWS IoT FleetWise は CloudWatch にメトリクスを送信します。 AWS Management Console、、または API を使用して AWS CLI、 AWS IoT FleetWise が CloudWatch に送信するメト

リクスを一覧表示できます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

> **Important**
>
> AWS IoT FleetWise が CloudWatch にメトリクスを送信できるように設定する必要があります。詳細については、「AWS IoT FleetWise 設定を構成する」を参照してください。

`AWS/IoTFleetWise` 名前空間には、次のメトリクスが含まれます。

シグナルに関するメトリクス

メトリクス	説明
IllegalMessageFromEdge	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージが、必要な形式と一致しませんでした。 単位: カウント ディメンション: なし 有効な統計: Sum
MessageThrottled	車両から AWS IoT FleetWise に送信されたメッセージがスロットリングされました。これは、このアカウントの現在のリージョンにおけるサービス制限を超えているためです。 単位: カウント ディメンション: なし 有効な統計: Sum
ModelingError	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージには、車両モデルに対して検証に失敗したシグナルが含まれています。

メトリクス	説明
	単位: カウント ディメンション: ModelName、StateTemplateName (オプション) 、SignalCatalogName (オプション)
DecodingError	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージには、車両のデコーダーマニフェストに対してデコーダーに失敗するシグナルが含まれています。 単位: カウント ディメンション: DecoderName 有効な統計: Sum
MessageSizeLimitExceeded	車両から AWS IoT FleetWise に送信されたメッセージはドロップされました。これは、現在のリージョンでこのアカウントのメッセージサービスの上限サイズを超えたためです。 単位: カウント ディメンション: なし 有効な統計: Sum

車両メトリクス

メトリクス	説明
VehicleNotFound	車両が不明な、 AWS IoT FleetWise が受信したメッセージ。 単位: カウント ディメンション: なし

メトリクス	説明
	有効な統計: Sum

キャンペーンに関するメトリクス

メトリクス	説明
CampaignInvalid	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージ。キャンペーンは無効です。 単位: カウント ディメンション: CampaignName 有効な統計: Sum
CampaignNotFound	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージ。キャンペーンは不明です。 単位: カウント ディメンション: CampaignName 有効な統計: Sum

状態テンプレートメトリクス

メトリクス	説明
NoStateTemplatesAssociated	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージ。車両に関連付けられた状態テンプレートはありません。 単位: カウント 有効な統計: Sum

キャンペーンデータ送信先メトリクス

メトリクス	説明
TimestreamWriteError	AWS IoT FleetWise は、車両から Amazon Timestream テーブルにメッセージを書き込むことができませんでした。 単位: カウント ディメンション: DatabaseName、TableName 有効な統計: Sum
S3WriteError	AWS IoT FleetWise は、車両から Amazon Simple Storage Service (Amazon S3) バケットにメッセージを書き込むことができませんでした。 単位: カウント ディメンション: BucketName 有効な統計: Sum
S3ReadError	AWS IoT FleetWise は、Amazon Simple Storage Service (Amazon S3) バケット内の車両からオブジェクトキーを読み取ることができませんでした。 単位: カウント ディメンション: BucketName 有効な統計: Sum

カスタマーマネージド AWS KMS キーメトリクス

メトリクス	説明
KMSKeyAccessDenied	AWS IoT FleetWise は、 AWS KMS キーアクセス拒否エラーのため、車両から Timestream テーブルまたは Amazon S3 バケットにメッセージを書き込むことができませんでした。 単位: カウント ディメンション: KMSKeyId 有効な統計: Sum

Amazon CloudWatch Logs で AWS IoT FleetWise をモニタリングする

> **Important**
>
> 現在、特定の AWS IoT FleetWise 機能へのアクセスはゲートされています。詳細については、「AWSAWS IoT FleetWise でのリージョンと機能の可用性」を参照してください。

Amazon CloudWatch Logs は、リソースで発生するイベントをモニタリングし、問題がある場合にアラートを発行します。アラートを受け取った場合は、ログファイルにアクセスして、その特定のイベントに関する情報を取得できます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。

CloudWatch コンソールで AWS IoT FleetWise ログを表示する

> **Important**
>
> CloudWatch コンソールで AWS IoT FleetWise ロググループを表示する前に、次の点に当てはまることを確認してください。
>
> - AWS IoT FleetWise でのログ記録を有効にしました。ログ記録の詳細については、「Configure AWS IoT FleetWise ログ記録」を参照してください。

- AWS IoT オペレーションによって書き込まれたログエントリが既にあります。

CloudWatch コンソールで AWS IoT FleetWise ログを表示するには

1. CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. ロググループを選択します。
4. [ロググループの検索] を選択します。アカウントに対して生成されたログイベントの完全なリストが表示されます。
5. 展開アイコンを選択して個々のストリームを確認し、ログレベルが ERROR のログをすべて見つけます。

   [イベントをフィルター] テキストボックスにクエリを入力することもできます。例えば、次のクエリを実行できます。

   ```
   { $.logLevel = "ERROR" }
   ```

フィルター式の詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「フィルターパターン構文」を参照してください。

Example ログエントリ

```
{
  "accountId": "123456789012",
  "vehicleName": "test-vehicle",
  "message": "Unrecognized signal ID",
  "eventType": "MODELING_ERROR",
  "logLevel": "ERROR",
  "timestamp": 1685743214239,
  "campaignName": "test-campaign",
  "signalCatalogName": "test-catalog",
  "signalId": 10242
}
```

シグナルに関するイベントタイプ

イベントタイプ	説明
MODELING_ERROR	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージには、車両モデルに対して検証に失敗したシグナルが含まれています。 属性: vehicleName、 campaignName (オプション) 、signalCatalogName、signalId (オプション) 、signalValue (オプション) 、signalValueRangeMin (オプション) 、signalValueRangeMax (オプション) 、modelManifestName (オプション) 、signalIds、stateTemplateName
ILLEGAL_MESSAGE_FROM_EDGE	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージが、必要な形式と一致しませんでした。 属性: vehicleName、campaignName、signalCatalogName
DECODING_ERROR	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージには、車両のデコーダーマニフェストに対してデコーダーに失敗するシグナルが含まれています。 属性: campaignName、signalCatalogName、decoderManifestName、(オプション) signalName、(オプション) s3URI
MESSAGE_THROTTLED	車両から AWS IoT FleetWise に送信されたメッセージはスロットリングされました。これは、このアカウントの現在のリージョンにおけるサービス制限を超えているためです。

イベントタイプ	説明
	属性: accountId、vehicleName、メッセージ、eventType、logLevel、タイムスタンプ
MESSAGE_SIZE_LIMIT_EXCEEDED	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージは、メッセージサービスの制限の最大サイズを超えています。 属性: accountId、vehicleName

車両イベントタイプ

イベントタイプ	説明
VEHICLE_NOT_FOUND	車両が不明である、 AWS IoT FleetWise が受信したメッセージ。 属性: vehicleName、 campaignName (オプション) 、stateTemplateName (オプション)

キャンペーンに関するイベントタイプ

イベントタイプ	説明
CAMPAIGN_NOT_FOUND	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージ。キャンペーンは不明でした。 属性: vehicleName (オプション)、campaignName
CAMPAIGN_INVALID	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージで、キャンペーンが無効でした。 属性: vehicleName (オプション)、campaignName

キャンペーンデータ送信先イベントタイプ

イベントタイプ	説明
TIMESTREAM_WRITE_ERROR	AWS IoT FleetWise は、車両から Amazon Timestream テーブルにメッセージを書き込めませんでした。 属性: vehicleName、campaignName、timestreamDatabaseName、timestreamTableName
S3_WRITE_ERROR	AWS IoT FleetWise は、車両から Amazon Simple Storage Service (Amazon S3) バケットにメッセージを書き込めませんでした。 属性: campaignName、destinationName
S3_READ_ERROR	AWS IoT FleetWise は、Amazon Simple Storage Service (Amazon S3) バケット内の車両からオブジェクトキーを読み取ることができませんでした。 属性: campaignName、destinationName

状態テンプレートイベントタイプ

イベントタイプ	説明
STATE_TEMPLATE_NOT_FOUND	車両から送信され、 AWS IoT FleetWise によって受信されたメッセージ。状態テンプレートは不明でした。 属性: vehicleName (オプション) 、stateTemplateName

カスタマーマネージド AWS KMS キーイベントタイプ

イベントタイプ	説明
KMS_KEY_ACCESS_DENIED	AWS IoT FleetWise は、 AWS KMS キーアクセス拒否エラーのため、車両から Timestream テーブルまたは Amazon S3 バケットにメッセージを書き込むことができませんでした。 属性: kmsKeyId (オプション)、resourceArn (オプション)

属性

すべての CloudWatch Logs エントリには、以下の属性が含まれます。

accountId

AWS アカウント ID。

eventType

ログが生成されたイベントタイプ。イベントタイプの値は、ログエントリが生成される原因となったイベントによって異なります。各ログエントリの説明には、そのログエントリの `eventType` の値が含まれます。

logLevel

使用されているログレベル。詳細については、「AWS IoT Core デベロッパーガイド」の「ログレベル」を参照してください。

message

ログに関する具体的な詳細が含まれています。

timestamp

AWS IoT FleetWise がログを処理したときのエポックミリ秒のタイムスタンプ。

オプションの属性

CloudWatch Logs エントリには、`eventType` に応じてオプションで以下の属性が含まれます。

decoderManifestName

シグナルを含むデコーダーマニフェストの名前。

destinationName

車両データの送信先の名前。例えば、Amazon S3 バケット名を示します。

campaignName

キャンペーンの名前。

signalCatalogName

シグナルが含まれているシグナルカタログの名前。

signalId

エラーシグナルの ID。

signalIds

エラーシグナル ID のリスト。

signalName

シグナルの名前。

signalTimestampEpochMs

エラーシグナルのタイムスタンプ。

signalValue

エラーシグナルの値。

signalValueRangeMax

エラーシグナルの最大範囲。

signalValueRangeMin

エラーシグナルの最小範囲。

s3URI

車両メッセージに含まれる Amazon Ion ファイルの Amazon S3 固有の識別子。

timestreamDatabaseName

Timestream データベースの名前。

timestreamTableName

Timestream テーブルの名前。

vehicleName

車両モデルの名前。

Configure AWS IoT FleetWise ログ記録

AWS IoT FleetWise ログデータを CloudWatch ロググループに送信できます。CloudWatch Logs によって可視性が提供され、 AWS IoT FleetWise が車両からのメッセージの処理に失敗した場合に備えることができます。そのような状況は、例えば、構成の誤りやその他のクライアントエラーが原因で発生する可能性があります。何らかのエラーがある場合は通知されるため、問題を特定して軽減できます。

CloudWatch にログを送信するには、事前に CloudWatch ロググループを作成する必要があります。AWS IoT FleetWise で使用したのと同じアカウントとリージョンでロググループを設定します。AWS IoT FleetWise でログインを有効にするときは、ロググループ名を指定します。ログ記録を有効にすると、 AWS IoT FleetWise はログストリームの CloudWatch ロググループにログを配信します。

CloudWatch コンソールで、 AWS IoT FleetWise から送信されたログデータを表示できます。CloudWatch ロググループの構成の詳細については、「ロググループとログストリームの操作」を参照してください。

CloudWatch にログを発行するためのアクセス許可

CloudWatch ロググループのログ記録を構成するには、このセクションで説明するアクセス許可設定が必要です。アクセス許可の管理の詳細については、IAM ユーザーガイドのAWS 「リソースのアクセス管理」を参照してください。

これらのアクセス許可があると、ログ記録の構成の変更、CloudWatch のログ配信の構成、ロググループに関する情報の取得が可能になります。

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

```
            "iotfleetwise:PutLoggingOptions",
            "iotfleetwise:GetLoggingOptions"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"IoTFleetwiseLoggingOptionsAPI"
      }
      {
         "Sid":"IoTFleetwiseLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
            "logs:GetLogDelivery",
            "logs:UpdateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:ListLogDeliveries",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

すべての AWS リソースでアクションが許可されている場合、ポリシーに `"Resource"`の設定で示されます`"*"`。つまり、各アクションがサポートするすべての AWS リソースでアクションが許可されます。

AWS IoT FleetWise でのログ記録の設定 (コンソール)

このセクションでは、 AWS IoT FleetWise コンソールを使用してログ記録を設定する方法について説明します。

AWS IoT FleetWise コンソールを使用してログ記録を設定するには

1. AWS IoT FleetWise コンソールを開きます。
2. 左側のペインで、[設定] を選択します。

3. [設定] ページの [ログ] セクションで、[編集] を選択します。
4. [CloudWatch ログ記録] セクションで、[ロググループ] を入力します。
5. 変更を保存するには、[送信] を選択します。

ログ記録を有効にしたら、CloudWatch コンソールでログデータを表示できます。

AWS IoT FleetWise でデフォルトのログ記録を設定する (CLI)

このセクションでは、 CLI を使用して AWS IoT FleetWise のログ記録を設定する方法について説明します。

ここに示す CLI コマンドに対応する API のメソッドを使用して、 AWS API でこの手順を実行することもできます。GetLoggingOptions API オペレーションを使用して現在の構成を取得し、PutLoggingOptions API オペレーションを使用して構成を変更できます。

CLI を使用して AWS IoT FleetWise のログ記録を設定するには

1. アカウントのログ記録オプションを取得するには、get-logging-options コマンドを使用します。

```
aws iotfleetwise get-logging-options
```

2. ログ記録を有効にするには、put-logging-options コマンドを使用します。

```
aws iotfleetwise put-logging-options --cloud-watch-log-delivery
 logType=ERROR,logGroupName=MyLogGroup
```

各パラメータの意味は次のとおりです。

logType

CloudWatch Logs にデータを送信するログのタイプ。ログ記録を無効にするには、値を OFF に変更します。

logGroupName

このオペレーションでデータを送信する先の CloudWatch Logs グループ。 AWS IoT FleetWise のログ記録を有効にする前に、必ずロググループ名を作成してください。

ログ記録を有効にしたら、「CLI AWS を使用してログエントリを検索する」を参照してください。

を使用した Log AWS IoT FleetWise API コール AWS CloudTrail

AWS IoT FleetWise は AWS CloudTrail、 AWS IoT FleetWise のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、 AWS IoT FleetWise のすべての API コール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、 AWS IoT FleetWise コンソールからの呼び出しと AWS IoT FleetWise 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、 AWS IoT FleetWise 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 [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、 AWS IoT FleetWise に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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 のAWS IoT FleetWise 情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。 AWS IoT FleetWise でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに 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。

AWS IoT FleetWise のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。追跡により、CloudTrailはログファイルをSimple Storage Service (Amazon S3) バケットに配信できます。デフォルトでは、コンソールで作成した証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内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。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次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

All AWS IoT FleetWise アクションは CloudTrail によってログに記録され、AWS 「 IoT FleetWise API リファレンス」に記載されています。例えば、`CreateCampaign`、`AssociateVehicleFleet`、`GetModelManifest` 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 IAM 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またはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

Understand AWS IoT FleetWise ログファイルエントリ

「トレイル」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。

`AssociateVehicleFleet` オペレーションを示す CloudTrail ログエントリの例は、次のとおりです。

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:assumed-role/NikkiWolf",
        "accountId": "111122223333",
        "accessKeyId": "access-key-id",
        "userName": "NikkiWolf"
      },
      "eventTime": "2021-11-30T09:56:35Z",
      "eventSource": "iotfleetwise.amazonaws.com",
      "eventName": "AssociateVehicleFleet",
      "awsRegion": "us-east-1",
```

```
      "sourceIPAddress": "192.0.2.21",
      "userAgent": "aws-cli/2.3.2 Python/3.8.8 Darwin/18.7.0 botocore/2.0.0",
      "requestParameters": {
          "fleetId": "f1234567890",
          "vehicleId": "v0213456789"
       },
      "responseElements": {
      },
      "requestID": "9f861429-11e3-11e8-9eea-0781b5c0ac21",
      "eventID": "17385819-4927-41ee-a6a5-29ml0br812v4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
```

AWS IoT FleetWise デベロッパーガイドのドキュメント履歴

次の表に、 AWS IoT FleetWise のドキュメントリリースを示します。

変更	説明	日付
リージョンの拡張	AWS IoT FleetWise がアジアパシフィック (ムンバイ) リージョン (ゲートアクセスのみ) で利用可能になりました。	2024 年 11 月 21 日
新機能のゲート付き一般提供	AWS IoT FleetWise は、データの保存と転送、MQTT トピックのデータ送信先としての設定、診断トラブルコードデータの収集を行うキャンペーンのゲートアクセスをサポートするようになりました。また、カスタムデコードインターフェイスを使用したネットワークに依存しないデータ収集のゲートアクセス、コマンドの設定、車両の最後の既知の状態のモニタリングもサポートするようになりました。	2024 年 11 月 21 日
キャンペーンデータを MQTT トピックに送信する	AWS IoT FleetWise は、Amazon S3 または Amazon Timestream にデータを保存する機能に加えて、キャンペーン中に収集されたデータを、指定した MQTT トピックに送信できるようになりました。	2024 年 5 月 1 日

ビジョンシステムデータのプレビュー	AWS IoT FleetWise からのビジョンシステムデータのプレビューを使用して、カメラ、レーダー、ライダーなどの車両ビジョンシステムからデータを収集して整理できます。構造化および非構造化の両方のビジョンシステムデータ、メタデータ (イベント ID、キャンペーン、車両)、および標準センサー (テレメトリーデータ) をクラウド内で自動的に同期します。	2023 年 11 月 26 日
AWS KMS カスタマーマネージドキー	AWS IoT FleetWise が AWS KMS カスタマーマネージドキーをサポートするようになりました。KMS キーを使用して、 に保存されている AWS IoT FleetWise リソース (シグナルカタログ、車両モデル、デコーダーマニフェスト、車両、データ収集キャンペーン設定) に関連するサーバー側のデータを暗号化できます AWS クラウド。	2023 年 10 月 16 日
Amazon S3 のオブジェクトストレージ	AWS IoT FleetWise は、Amazon Simple Storage Service (Amazon S3) を使用したデータの保存をサポートするようになりました。キャンペーン中に収集したデータは、Amazon Timestream に加えて Amazon S3 にも保存できます。	2023 年 6 月 1 日

一般提供	これは、 AWS IoT FleetWise のパブリックリリースです。	2022 年 9 月 27 日
初回リリース	これは、 AWS IoT FleetWise デベロッパーガイドのプレビューリリースです。	2021 年 11 月 30 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。