플릿 허브 전용 AWS IoT 디바이스 관리 가이드

플릿 허브 용 AWS IoT 디바이스 관리

플릿 허브 용 AWS IoT 디바이스 관리: 플릿 허브 전용 AWS IoT 디바이스 관리 가이드

Table of Contents

Fleet Hub for AWS IoT Device Management란 무엇입니까?

Fleet Hub for AWS IoT Device Management(Fleet Hub)를 사용하면 디바이스 플릿의 상태를 모니터링하기 위한 독립형 웹 애플리케이션을 구축할 수 있습니다. AWS 계정이 없더라도 조직의 사용자가 이러한 애플리케이션을 사용하도록 할 수 있습니다. Fleet Hub를 사용하여 운영 및 보안 문제를 조사하고 해결하는 것과 같은 플릿 전반의 일반적인 작업을 관리할 수 있습니다.

Fleet Hub는 다음 기능을 제공합니다.

- 거의 실시간으로 디바이스 플릿 모니터링.
- 비정상적인 동작에 대해 기술자에게 알리도록 알림 설정.
- 작업 실행.

> **Note**
>
> Fleet Hub가 연결 상태 데이터를 인덱싱하려면 사물이 사물 이름과 일치하는 클라이언트 ID를 사용하여 AWS IoT Core에 연결되어야 합니다.

Fleet Hub for AWS IoT Device Management의 작동 방식

Fleet Hub for AWS IoT Device Management를 사용하여 관리자는 리소스를 프로비저닝하거나 코드를 작성하지 않고도 몇 분 안에 보안 웹 애플리케이션을 만들 수 있습니다. Fleet Hub를 사용하여 만든 웹 애플리케이션은 Active Directory와 같은 기존 자격 증명 시스템과 통합됩니다. 이를 통해 관리자는 자체 인증 및 권한 부여 모델을 적용할 수 있습니다.

Fleet Hub 웹 애플리케이션은 AWS IoT Core 플릿 인덱싱 및 디바이스 모니터링과 통합됩니다. 이러한 통합은 디바이스 상태 데이터를 모니터링하고 플릿의 디바이스가 지정된 상태에 도달하면 경보를 생성할 수 있는 기능을 제공합니다.

Fleet Hub 애플리케이션은 `AWSIoTFleetHubFederationAccess` 관리형 정책을 사용합니다. 자세한 내용은 ??? 단원을 참조하세요.

사용 사례 예시:

- 디바이스 연결 문제 시각화 - 플릿의 연결이 끊긴 디바이스 수, 디바이스의 마지막 연결 상태, 디바이스 연결이 끊긴 이유를 확인할 수 있습니다.

- 경보 설정 - 특정 수의 디바이스가 연결이 끊어질 때 경보를 트리거하는 임계값을 설정할 수 있습니다. 또한 특정 이유로 디바이스의 연결이 끊어지면 경보를 통해 사용자에게 알릴 수 있습니다. 그러면 자세한 디바이스 데이터를 확인하여 조사하고 문제를 해결할 수 있습니다.
- 작업 실행 - 하나 이상의 디바이스에서 원격 작업(예: 펌웨어 업데이트)을 실행할 수 있습니다.

Fleet Hub 데이터 인덱싱 작동 방식

Fleet Hub 콘솔을 사용하여 디바이스 플릿에 대한 플릿 인덱싱을 활성화할 수 있습니다. Fleet Hub에서 플릿 인덱싱을 활성화하면 전체 플릿에 대해 이를 활성화하고 모든 Fleet Hub 애플리케이션에서 사용할 수 있게 됩니다.

활성화되면 플릿 인덱싱을 통해 모든 AWS IoT Core 관리형 필드가 자동으로 인덱싱됩니다. 또한 Fleet Hub 애플리케이션에서 데이터를 쿼리하고 집계하는 데 사용할 수 있는 사용자 정의 데이터를 추가할 수도 있습니다.

Fleet Hub 경보 작동 방식

Fleet Hub 웹 애플리케이션은 사용자가 경보를 만들 수 있는 인터페이스를 제공합니다. 다음 단계에서는 Fleet Hub에서 사용자가 경보를 생성하는 방법을 보여줍니다.

1. 데이터를 집계하는 쿼리 만들기 - 검색 가능한 필드를 사용하여 사용자가 대상으로 지정할 디바이스를 집계하는 쿼리를 지정합니다.
2. 임계값 구성 - 인덱싱된 데이터의 조건(예: 지정된 간격 동안의 연결 상태)에 도달하면 경보를 트리거하는 임계값을 설정합니다.
3. 알림 구성 - 지정된 디바이스에 경보가 발생할 때 Fleet Hub에서 알림을 발송할 수신자 그룹을 지정합니다.

Fleet Hub 작업 작동 방식

Fleet Hub 콘솔을 사용하여 디바이스에서 원격 작업을 실행할 수 있습니다.

작업 템플릿이 활성화되면 Fleet Hub 애플리케이션의 템플릿에서 특정 작업을 생성할 수 있습니다.

관리자를 위한 AWS IoT 장치 관리를 위한 플릿 허브

이 섹션에는 AWS IoT 장치 관리용 Fleet Hub 웹 애플리케이션을 만들고 관리하는 방법에 대한 관리자를 위한 지침이 포함되어 있습니다.

주제

시작하기

이 섹션에서는 AWS IoT 장치 관리용 Fleet Hub 웹 애플리케이션을 만들고 설정하는 방법을 설명합니다.

주제

첫 번째 Fleet Hub 애플리케이션 생성

필수 조건

다음 목록에는 Fleet Hub 웹 애플리케이션을 생성하는 데 필요한 리소스가 나열되어 있습니다.

- AWS 계정.
- 계정에 대해 AWS IAM Identity Center이 활성화되어 있습니다. (아직 이 서비스를 활성화하지 않은 경우 AWS IoT Core 콘솔(https://console.aws.amazon.com/iot/)에서 활성화하라는 메시지를 표시합니다.)

첫 번째 Fleet Hub 애플리케이션 생성

다음 단계는 AWS IoT 장치 관리용 Fleet Hub 웹 애플리케이션을 만드는 방법을 설명합니다.

1. AWS IoT Core 콘솔 (https://console.aws.amazon.com/iot/) 으로 이동한 다음 왼쪽 패널에서 플릿 허브를 선택한 다음 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 애플리케이션 생성(Create application)을 선택합니다.
3. IAM ID 센터 설정 페이지에서 AWS IAM Identity Center (IAM ID 센터) 를 활성화하지 않은 경우 단계에 따라 활성화하십시오. AWS Organizations에서 이메일을 전송합니다. 이메일에 포함된 링크를 선택하여 IAM Identity Center 활성화를 완료합니다.

   > **Note**
   >
   > 자체 ID 제공업체를 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 AWS IAM Identity Center무엇입니까를 참조하십시오. 그리고 외부 ID 공급자에 연결하세요.
   > Fleet Hub 애플리케이션을 생성할 때 IAM Identity Center의 조직 인스턴스가 아직 없다면 해당 인스턴스를 생성해야 합니다. 생성한 플릿 허브 애플리케이션도 IAM ID 센터의 조직 인스턴스와 동일한 AWS 리전 위치에 있어야 합니다. 자세한 내용은 IAM ID 센터의 IAM ID 센터 및 조직 인스턴스 활성화를 참조하십시오.

   페이지에서 IAM Identity Center를 이미 활성화했는지 여부를 알려줍니다.

   다음을 선택합니다.
4. 인덱스 AWS IoT 데이터 페이지에서 플릿 허브에서 플릿 허브로의 데이터 흐름 작동 방식 섹션의 정보를 검토하십시오. AWS IoT 이 페이지는 AWS IoT Core 플릿 인덱싱을 활성화하고 관리할 수 있는 AWS IoT Core 콘솔의 페이지로 연결됩니다. 이 서비스를 사용하여 레지스트리 데이터, 섀도우 데이터, 디바이스 연결 데이터(디바이스 수명 주기 이벤트) 및 디바이스 위반 데이터를 인덱싱, 검색 및 집계할 수 있습니다. AWS IoT Core 플릿 인덱싱이 기본적으로 인덱싱하는 관리 필드 외에도 사용자 지정 필드를 만들 수도 있습니다.

   - 이미 플릿 인덱싱을 활성화한 경우 이 페이지에는 플릿 인덱싱 설정과 사용자 지정 필드가 표시됩니다.

   - 사물 인덱싱 및 사물 연결을 활성화하지 않은 경우, Fleet Hub를 사용하려면 이 두 기능을 활성화해야 합니다.

   플릿 인덱싱 설정 관리 및 검토가 완료되면 다음(Next)을 선택합니다.

   Fleet Hub 애플리케이션에 대한 플릿 인덱싱을 활성화하는 방법에 대한 자세한 내용은 Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리를 참조하세요.

5. 애플리케이션 구성(Configure application) 페이지의 애플리케이션 역할(Application role) 섹션에서 새 서비스 역할을 만들거나 기존 서비스 역할을 선택합니다. Fleet Hub 웹 애플리케이션은 Fleet Hub 리소스를 사용할 때 이 역할을 수임합니다. 페더레이션 사용자는 웹 애플리케이션을 사용할 때 역할과 동일한 권한을 갖습니다.

   - 새 역할을 만드는 경우 역할 이름은 `AWSIotFleetHub_`*`random_string`* 문자열로 시작해야 합니다.

   - 기존 역할을 선택하는 경우 이 정책 문서에 있는 권한이 있는지 확인합니다. Fleet Hub 웹 애플리케이션에 필요한 권한을 보려면 역할 세부 정보 보기(View role details)를 선택합니다. 이 페이지에서 생성한 새 역할에 서비스가 적용되는 정책 문서를 보여 주는 창이 열립니다.

6. 애플리케이션 구성(Configure application) 페이지의 애플리케이션 속성(Application properties) 섹션에 애플리케이션 이름을 입력합니다. 애플리케이션 설명을 입력할 수도 있습니다(선택 사항).

   애플리케이션 생성(Create application)을 선택합니다.

7. 애플리케이션(Applications) 페이지에서, 생성한 애플리케이션을 선택한 다음 세부 정보 보기(View details)를 선택합니다. 애플리케이션의 세부 정보를 검토합니다.

> **Note**
>
> Fleet Hub의 관리자로서 문제를 해결하는 데 도움이 되는 가능한 솔루션에 대한 자세한 내용은 문제 해결을 참조하세요.

Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리

AWS IoT Core 콘솔 또는 를 사용하여 플릿 인덱싱을 활성화하고 AWS IoT 레지스트리 데이터, AWS IoT Device Shadow 데이터, AWS IoT 연결 데이터, AWS IoT Device Defender 위반 데이터 등의 데이터 소스를 인덱싱하도록 구성할 수 있습니다. AWS CLI 다음 단계는 콘솔에서 Fleet Hub for AWS IoT Device Management 애플리케이션의 플릿 인덱싱을 활성화하는 방법을 설명합니다. AWS IoT Core 를 사용하는 AWS CLI단계를 보려면 사물 인덱싱 관리를 참조하십시오.

> **Important**
>
> 2022년 7월 20일은 AWS IoT 디바이스 관리 플릿 인덱싱과 AWS IoT Core 네임드 섀도 및 위반 AWS IoT Device Defender 탐지의 통합에 대한 일반 가용성 릴리스입니다. 이번 정식 출시 릴리스를 통해 섀도우 이름을 지정하여 특정 명명된 섀도우를 인덱싱할 수 있는 기능이 지원됩

니다. 2021년 11월 30일부터 2022년 7월 19일까지인 이 기능의 공개 프리뷰 기간 중에 인덱싱을 위해 명명된 섀도우를 추가한 경우, 플릿 인덱싱 설정을 재구성하고 특정 섀도우 이름을 선택하여 인덱싱 비용을 줄이고 성능을 최적화하는 것이 좋습니다. 플릿 인덱싱 설정을 재구성하는 방법에 대한 자세한 정보는 플릿 인덱싱 관리를 참조하세요.

1. AWS IoT Core 콘솔 (https://console.aws.amazon.com/iot/) 으로 이동한 다음 왼쪽 패널에서 설정을 선택합니다.
2. 설정 페이지에서 플릿 인덱싱(Fleet indexing) 섹션으로 이동한 다음 인덱싱 관리(Manage indexing)를 선택합니다.
3. 플릿 인덱싱 관리 페이지의 구성 섹션에서 사물 인덱싱과 AWS IoT 인덱싱하려는 데이터 소스를 선택합니다. Fleet Hub를 사용하려면 사물 인덱싱 및 사물 연결을 활성화해야 합니다.
4. (선택 사항) 플릿 인덱싱 관리 페이지의 집계를 위한 사용자 지정 필드(선택 사항) 섹션에서 플릿 인덱싱이 기본적으로 인덱싱하는 관리형 필드 외에 추가로 사용자 지정 필드를 생성합니다.

   플릿 인덱싱 설정 관리 및 검토가 완료되면 다음(Next)을 선택합니다.

   플릿 인덱싱이 설정을 업데이트하는 데 잠시 시간이 걸릴 수 있습니다. 플릿 인덱싱을 관리하는 방법에 대한 자세한 내용은 플릿 인덱싱 관리를 참조하세요.

Fleet Hub 애플리케이션에 사용자 추가

Fleet Hub for AWS IoT Device Management용 웹 애플리케이션은 새로 생성될 때 사용자를 포함하지 않습니다. 사용자와 조직의 구성원이 애플리케이션을 사용하려면 먼저 사용자를 추가해야 합니다. 이 주제의 단계에서는 애플리케이션에 사용자를 추가하는 방법을 설명합니다.

계정에 AWS IAM Identity Center (IAM Identity Center) 를 설정하여 기존 ID 시스템의 사용자를 추가합니다. 자체 ID 제공업체를 IAM Identity Center에 연결할 수 있습니다. 자세한 정보는 IAM Identity Center란 무엇인가요?를 참조하세요.

1. 애플리케이션 페이지의 Fleet Hub 애플리케이션 목록에서 웹 애플리케이션을 선택합니다. 세부 정보 보기(View details)를 선택합니다.
2. 애플리케이션 세부 정보 페이지에서 사용자 추가(Add user)를 선택합니다.
3. Fleet Hub 사용자 추가(Add Fleet Hub users) 창에서 애플리케이션에 대한 액세스 권한을 부여하려는 조직의 사용자를 선택합니다. 선택한 사용자 추가(Add selected users)를 선택합니다.
4. 애플리케이션 세부 정보 페이지에서 선택한 사용자가 Fleet Hub 사용자 목록에 표시되는지 확인합니다.

Fleet Hub for AWS IoT Device Management와 상호 작용하는 AWS 및 AWS IoT Core 서비스

이 주제에서는 Fleet Hub for AWS IoT Device Management가 다른 AWS 서비스와 상호 작용하여 Fleet Hub 웹 애플리케이션에 기능을 제공하는 방법을 설명합니다.

다음 표는 Fleet Hub for AWS IoT Device Management가 각 기능을 구현하기 위해 어떤 AWS 서비스를 사용하는지 보여줍니다.

기능	AWS 서비스	설명
Active Directory와 같은 기존 자격 증명 시스템을 통합합니다.	AWS IAM Identity Center(IAM Identity Center)	기존 ID 시스템의 사용자를 추가하려면 계정에 AWS IAM Identity Center(IAM Identity Center)을 설정합니다. 자체 ID 제공업체를 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 AWS IAM Identity Center이란 무엇인가요? 및 작업 인력 ID를 참조하세요.
AWS 관리형 필드, 사용자 지정 필드 및 인덱싱된 데이터 소스의 속성을 사용하여 쿼리를 생성합니다.	AWS IoT 플릿 인덱싱	플릿 인덱싱 서비스를 사용하여 레지스트리 데이터, 섀도우 데이터 및 디바이스 연결 데이터(디바이스 수명 주기 이벤트)를 인덱싱, 검색 및 집계합니다. AWS IoT 플릿 인덱싱이 기본적으로 인덱싱하는 관리형 필드 외에 집계를 위해 사용자 지정 필드를 생성할 수도 있습니다. 플릿 인덱싱에 대한 자세한 내용은 플릿 인덱싱을 참조하세요.

기능	AWS 서비스	설명
쿼리에 의해 지정된 디바이스 집합에 대한 경보를 만듭니다.	Amazon CloudWatch(CloudWatch)	Fleet Hub 대시보드에는 검색 가능한 필드와 결합하여 경보 임계값을 생성하는 데 사용할 수 있는 CloudWatch 지표가 표시됩니다. 예를 들어 연결된 디바이스 수가 지정된 수량 미만으로 떨어질 때마다 Amazon Simple Notification Service(Amazon SNS) 알림을 생성하는 CloudWatch 경보를 만들 수 있습니다. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch란 무엇입니까?를 참조하세요. AWS IoT Core가 CloudWatch와 함께 작동하여 지표 및 경보를 생성하는 방법에 대한 자세한 내용은 CloudWatch를 사용하여 AWS IoT 경보 및 지표 모니터링을 참조하세요.

문제 해결

이 단원에서는 Fleet Hub의 관리자로서 문제를 해결하는 데 도움이 되는 문제 해결 정보와 가능한 해결책을 제공합니다.

증상	Solution
내 웹 애플리케이션 링크가 작동하지 않습니다.	애플리케이션을 생성한 후 링크가 작동하려면 몇 시간이 걸릴 수 있습니다.
내 웹 애플리케이션에 로그인할 수 없습니다.	애플리케이션에 사용자를 하나 이상 추가했는지 확인합니다.

증상	Solution
	역할에 다음과 같은 적절한 신뢰 관계가 있는지 확인합니다. `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` IAM 신뢰 관계를 편집하는 방법에 대한 자세한 내용은 기존 역할에 대한 신뢰 관계 편집을 참조하세요.
웹 애플리케이션을 생성할 수 없습니다.	웹 애플리케이션 수 제한에 도달하지 않았는지 확인합니다.
내가 기대하는 사용자 지정 필드가 표시되지 않습니다.	플릿 인덱싱을 올바르게 설정했는지 확인합니다. 플릿 인덱싱에 대한 자세한 내용은 플릿 인덱싱을 참조하세요.

사용자를 위한 Fleet Hub for AWS IoT Device Management

이 단원에서는 사용자를 위해 Fleet Hub for AWS IoT Device Management 웹 애플리케이션에 대한 기본 정보를 소개합니다. Fleet Hub 웹 애플리케이션을 생성하고 사용자를 추가하는 방법에 대한 자세한 내용은 관리자를 위한 AWS IoT 장치 관리를 위한 플릿 허브 단원을 참조하세요.

주제

시작하기

이 단원에는 Fleet Hub for AWS IoT Device Management 웹 애플리케이션의 기능을 처음 사용하는 사용자를 위한 정보가 포함되어 있습니다.

주제

첫 번째 쿼리 만들기

이 주제에서는 간단한 Fleet Hub for AWS IoT Device Management 쿼리를 만드는 데 필요한 단계를 안내합니다. 쿼리는 검색 쿼리 구문을 사용하여 지정됩니다.

필수 조건

- 디바이스(사물)를 포함하는 AWS IoT Core 계정에 연결된 Fleet Hub 애플리케이션.
- Fleet Hub 애플리케이션을 사용할 권한이 있는 조직의 계정.

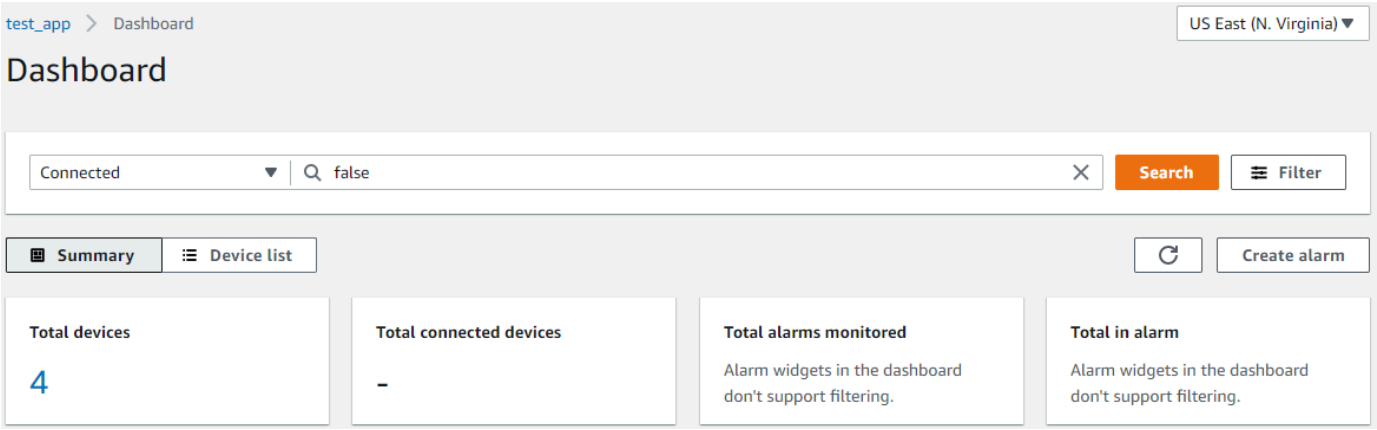
첫 번째 Fleet Hub 쿼리 만들기

첫 번째 Fleet Hub 쿼리 만들기

1. Fleet Hub 애플리케이션으로 이동합니다.

   기본 대시보드 보기에는 관리형 속성 및 사용자 지정 속성이 포함된 모든 디바이스 목록이 표시됩니다. 속성(attributes) 접두사를 포함하는 속성은 사용자 지정 속성입니다.

2. 페이지 상단 메뉴의 모든 필드(All fields)에서 연결됨(Connected)을 선택합니다. 드롭다운 메뉴 옆의 텍스트 상자에 **`false`**를 입력합니다.



3. 검색을 수행하려면 검색(Search)을 선택합니다. AWS IoT Core에 연결되지 않은 모든 디바이스 목록이 표시됩니다.

쿼리 구문 및 예제 쿼리에 대한 자세한 내용은 쿼리 구문,사물 쿼리 예 및 사물 그룹 쿼리 예를 참조하세요.

첫 번째 경보 만들기

이 주제에서는 간단한 Fleet Hub for AWS IoT Device Management 경보를 만드는 데 필요한 단계를 안내합니다.

필수 조건

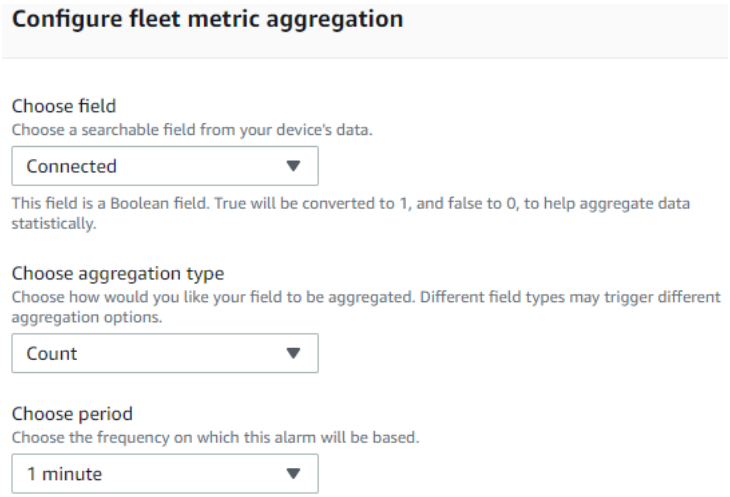
- 디바이스(사물)를 포함하는 AWS IoT Core 계정에 연결된 Fleet Hub 애플리케이션.
- Fleet Hub 애플리케이션을 사용할 권한이 있는 조직의 계정.

첫 번째 경보 생성

첫 번째 Fleet Hub 경보 생성

1. Fleet Hub 애플리케이션으로 이동합니다.
2. 특정 디바이스 집합을 대상으로 지정하려면 쿼리를 생성합니다. 간단한 쿼리를 만드는 방법에 대한 지침은 the section called “첫 번째 쿼리 만들기” 단원을 참조하세요. 쿼리를 생성하지 않으면 경보가 플릿의 모든 디바이스에 적용됩니다.
3. 기본 대시보드 페이지에서 경보 생성(Create alarm)을 선택합니다.
4. 집계 지표 구축(Build aggregation metric) 페이지에서 쿼리가 대상 쿼리(Target query) 아래에 나타나는지 확인합니다. 플릿 지표 집계 구성(Configure fleet metric aggregation) 섹션의 필드 선택(Choose field) 메뉴에서 연결됨(Connected)을 선택합니다. AWS 관리형 필드는 디바이스가 AWS IoT Core에 연결되어 있는지 여부를 나타냅니다. 필드 선택(Choose field) 메뉴에는 AWS 관리형 필드와 AWS IoT 플릿 인덱싱에서 관리자가 생성한 사용자 정의 필드가 포함되어 있습니다.
5. 집계 유형 선택(Choose aggregation type)에서 다음 옵션 중 하나를 선택합니다.
   - 최대(Maximum) -- 최대 임계값을 구성합니다.
   - 개수(Count) -- 특정 개수를 임계값으로 구성합니다.
   - 합계(Sum) -- 합계를 임계값으로 구성합니다.
   - 최소(Minimum) -- 최소 임계값을 구성합니다.
   - 평균(Average) -- 평균 임계값을 구성합니다.
6. 기간 선택(Choose period)에서, 이전 메뉴에서 지정한 경보를 트리거할 조건 지속 시간을 선택합니다.

   플릿 지표 집계 구성(Configure fleet metric aggregation)에 대한 설정의 예는 다음과 같습니다.



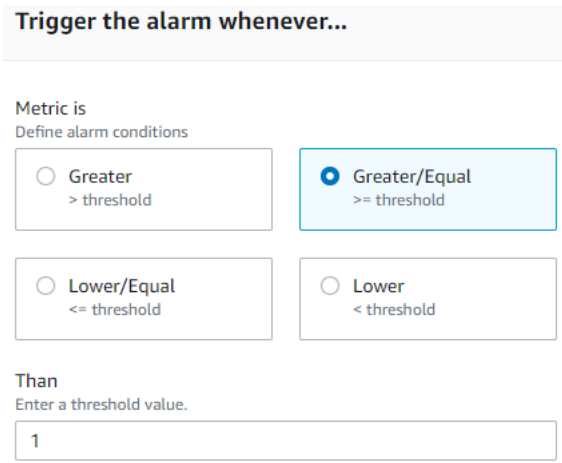
다음(Next)을 선택합니다.

7. 임계값 설정(Set threshold) 페이지의 …할 때마다 경보 트리거(Trigger the alarm whenever...) 섹션에서 다음 옵션 중 하나를 선택합니다.

   - 큼(Greater) -- 집계 지표 및 유형이 지정된 값을 초과할 때 경보합니다.
   - 크거나 같음(Greater/Equal) -- 집계 지표 및 유형이 지정된 값과 같거나 그 값을 초과할 때 경보합니다.
   - 작음(Lower) -- 집계 지표 및 유형이 지정된 값 미만으로 떨어지면 경보합니다.
   - 작거나 같음(Lower/Equal) -- 집계 지표 및 유형이 지정된 값과 같거나 그 값 미만으로 떨어지면 경보합니다.

8. 보다(Than) 텍스트 상자에서, 경보의 임계값으로 사용할 값을 지정합니다.

   임계값 설정(Set threshold) 예는 다음과 같습니다.



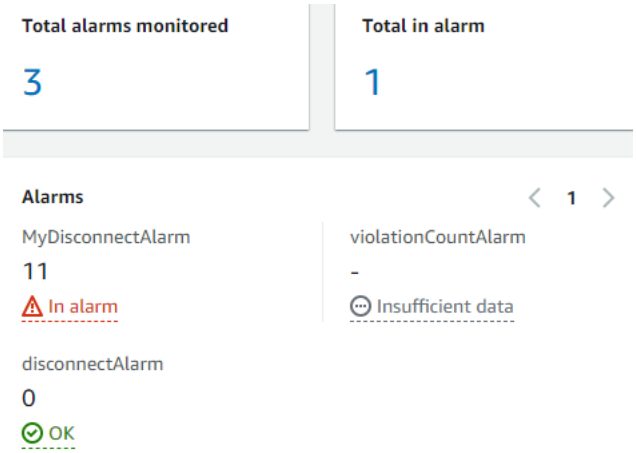
   다음(Next)을 선택합니다.

9. 사용자 알림(Notify user) 페이지의 알림 -- 선택사항(Notify -- optional) 섹션에 경보가 활성 상태일 때 알림을 받는 조직의 사용자가 포함된 이메일 목록의 이름을 입력합니다. 이 목록을 채우려면 쉼표로 구분된 이메일 주소 목록을 입력합니다.

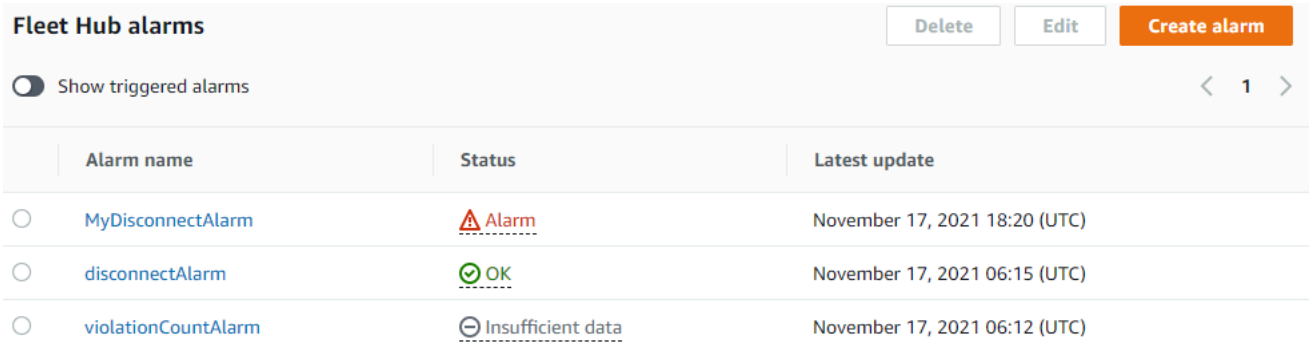
10. 경보 세부 정보(Alarm details) 섹션에서 경보 이름을 입력하고 경보의 설명을 입력합니다. 다음(Next)을 선택합니다.

11. 검토(Review) 페이지에서, 이전 페이지에서 입력한 정보를 확인합니다. 제출(Submit)을 선택합니다. 기본 대시보드로 돌아갑니다.

12. 기본 대시보드에서 알람 위젯은 생성한 모든 경보의 정보를 표시합니다.



생성한 경보의 세부 정보를 보려면 왼쪽 탐색 패널에서 Fleet Hub 경보(Fleet Hub alarms)를 선택합니다.



디바이스 세부 정보 보기

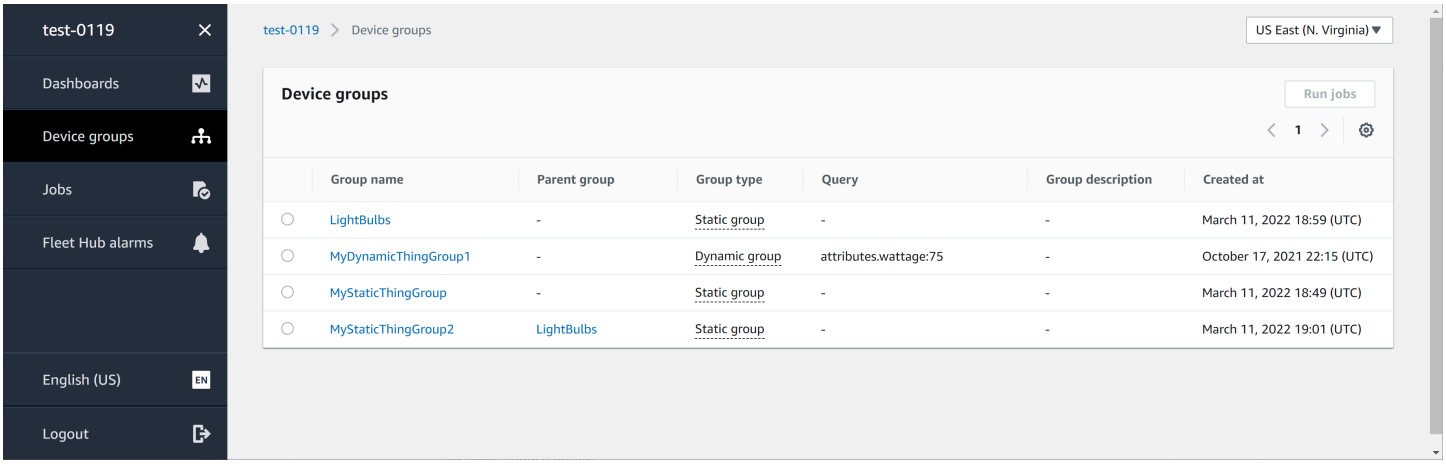
이 주제에서는 디바이스 그룹 및 디바이스에 대한 세부 정보를 보는 데 필요한 단계를 안내합니다.

필수 조건

- 디바이스(사물)를 포함하는 AWS IoT Core 계정에 연결된 Fleet Hub 애플리케이션.
- Fleet Hub 애플리케이션을 사용할 권한이 있는 조직의 계정.

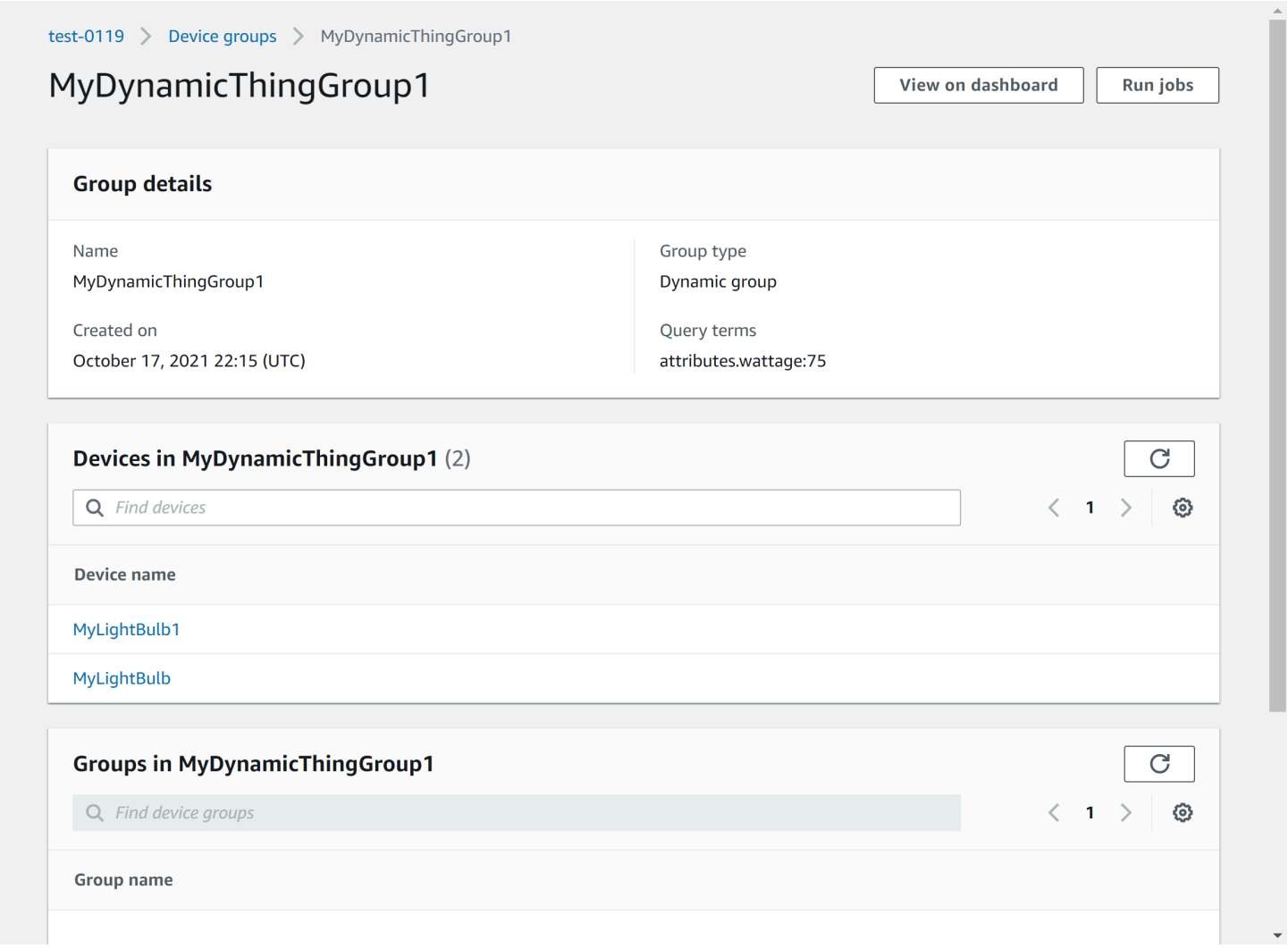
디바이스 그룹

Fleet Hub 웹 애플리케이션에 로그인하면 왼쪽 탐색 패널에 디바이스 그룹(Device groups)이 있습니다. 디바이스 그룹(Device groups) 페이지에는 Fleet Hub 웹 애플리케이션의 모든 디바이스 그룹이 나열됩니다. 디바이스 그룹의 세부 정보를 보려면 그룹 이름(Group name) 열에서 특정 디바이스 그룹을 선택합니다.



디바이스 그룹 세부 정보

디바이스 그룹 세부 정보(Device group details) 페이지에는 선택한 디바이스 그룹에 대한 정보가 들어 있습니다. 디바이스의 세부 정보를 보려면 ***XXX***의 디바이스(Devices in XXX) 섹션의 디바이스 이름(Device name) 열에서 특정 디바이스를 선택합니다.



디바이스 세부 정보

디바이스 세부 정보(Device details) 페이지에는 선택한 디바이스에 대한 정보가 들어 있습니다.

> **Note**
>
> 클라이언트가 AWS IoT에 연결할 때 사물 이름과 다른 클라이언트 ID를 사용하는 경우 플릿 인덱싱에서 '사물'의 연결 상태를 인덱싱하지 않습니다.

세부 정보

세부 정보(Details) 섹션에는 디바이스에 대한 다음 정보가 나와 있습니다.

- 디바이스 이름(Device name) - 디바이스를 나타내는 사물 리소스의 이름입니다. 자세한 내용은 레지스트리를 사용하여 사물을 관리하는 방법을 참조하세요.

- 사물 유형(Thing type) - 디바이스와 연결된 사물 유형입니다. 사물 유형을 사용하여 사물 유형이 동일한 모든 사물에 공통된 정보를 저장할 수 있습니다. 자세한 내용은 사물 유형 섹션을 참조하세요.

- 마지막 연결 타임스탬프(Last connection timestamp) - 디바이스가 AWS IoT에 마지막으로 연결되었을 때의 타임스탬프입니다.

- 공유 가능한 디바이스 링크(Shareable device link) - 선택한 디바이스의 디바이스 세부 정보(Device details) 페이지를 가리키는 공유 가능한 링크입니다.

- 마지막 연결 상태(Last connection status) - AWS IoT에 연결된 디바이스의 연결 상태입니다. 디바이스가 연결되어 있는 경우 값은 `true`입니다. 연결되지 않은 경우 값은 `false`입니다.

- 연결 해제 이유(Disconnect reason) - 디바이스 연결이 해제된 이유입니다.

보고된 데이터

보고된 데이터(Reported data) 섹션에는 디바이스의 레지스트리 데이터, 디바이스디바이스 섀도우 데이터, 사물 그룹에 대한 정보가 들어 있습니다.

- 디바이스 필드(Device fields) - AWS IoT 플릿 인덱싱에 있는 디바이스의 인덱싱된 필드입니다. 자세한 내용은 플릿 인덱싱 관리를 참조하세요.

- 디바이스 섀도우(Device shadows) - 디바이스와 연결된 섀도우입니다. 디바이스 섀도우에는 명명되지 않은 클래식 섀도우와 명명된 섀도우가 모두 포함될 수 있습니다. 디바이스 섀도우에 관한 자세한 내용은 AWS IoT 디바이스 섀도우 섹션을 참조하세요.

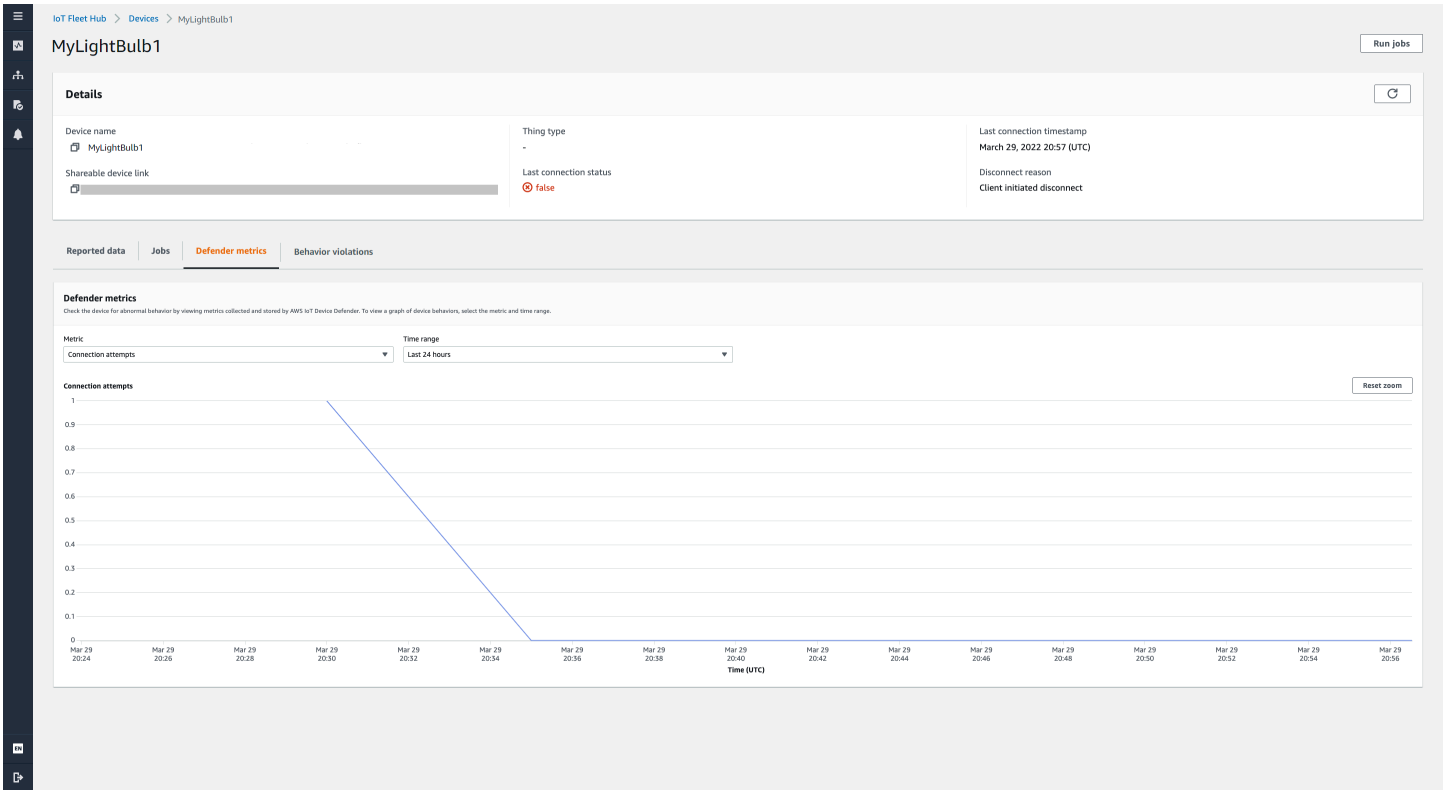
- 디바이스 그룹(Device groups) - 디바이스와 연결된 디바이스 그룹입니다. 디바이스 그룹에는 정적 사물 그룹과 동적 사물 그룹이 모두 포함될 수 있습니다. 자세한 내용은 정적 사물 그룹과 동적 사물 그룹을 참조하세요.

작업

작업(Jobs) 섹션에는 디바이스에서 실행 중인 모든 작업이 표시됩니다. 각 작업에는 대상 및 런타임 정보를 포함하여 작업에 대한 요약 정보를 표시하는 세부 정보 페이지가 있습니다. 자세한 내용은 Fleet Hub for AWS IoT에서 작업 및 작업 템플릿 작업 및 작업을 참조하세요.

Defender 지표

Defender 지표(Defender metrics) 섹션에는 현재 선택한 디바이스와 연결된 AWS IoT Device Defender 지표가 표시됩니다. 표시된 지표 데이터를 사용하여 선택한 기간 동안의 디바이스 작업을 시각화할 수 있습니다. Fleet Hub 애플리케이션에서 Defender 지표 데이터를 보려면 Fleet Hub 관리자가 먼저 선택한 디바이스와 연결된 AWS IoT Device Defender 지표를 설정해야 합니다. 디바이스에 대한 AWS IoT Device Defender 지표를 생성 및 설정하는 방법에 대한 자세한 내용은 사용자 지정 지표, 디바이스 측 지표, 클라우드 측 지표를 참조하세요.



동작 위반

동작 위반(Behavior violations) 섹션에는 현재 선택한 디바이스와 연결된 인덱싱된 AWS IoT Device Defender 감지 위반 데이터가 표시됩니다. 동작 위반 데이터에는 위반 횟수, 마지막 위반 시간 및 마지막 위반 지표 값이 포함될 수 있습니다. Fleet Hub 애플리케이션에서 동작 위반 데이터를 보려면 Fleet Hub 관리자가 보안 프로필에서 AWS IoT Device Defender 동작 위반을 설정하고 플릿 인덱싱에서 AWS IoT Device Defender 위반을 구성해야 합니다. AWS IoT Device Defender 보안 프로필에서 동작

위반을 설정하는 방법에 대한 자세한 내용은 AWS IoT Device Defender 감지를 참조하세요. AWS IoT Device Defender 위반 구성 방법에 대한 자세한 내용은 Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리와 사물 인덱싱 관리를 참조하세요.

쿼리 및 필터

Fleet Hub for AWS IoT Device Management 쿼리를 사용하여 디바이스 플릿에 있는 사물의 목록을 생성하고 볼 수 있습니다. 인덱싱된 데이터 소스의 모든 AWS관리 필드, 사용자 지정 필드 및 모든 속성을 쿼리 필터로 사용할 수 있습니다. 플릿 인덱싱을 사용하여 AWS IoT 집계를 활성화할 사용자 지정 필드를 만들 수도 있습니다. the section called “경보” 플릿 인덱싱에 대한 자세한 내용은 플릿 인덱싱을 참조하세요.

주제

- 대시보드 보기
- 필터를 사용하여 쿼리 만들기

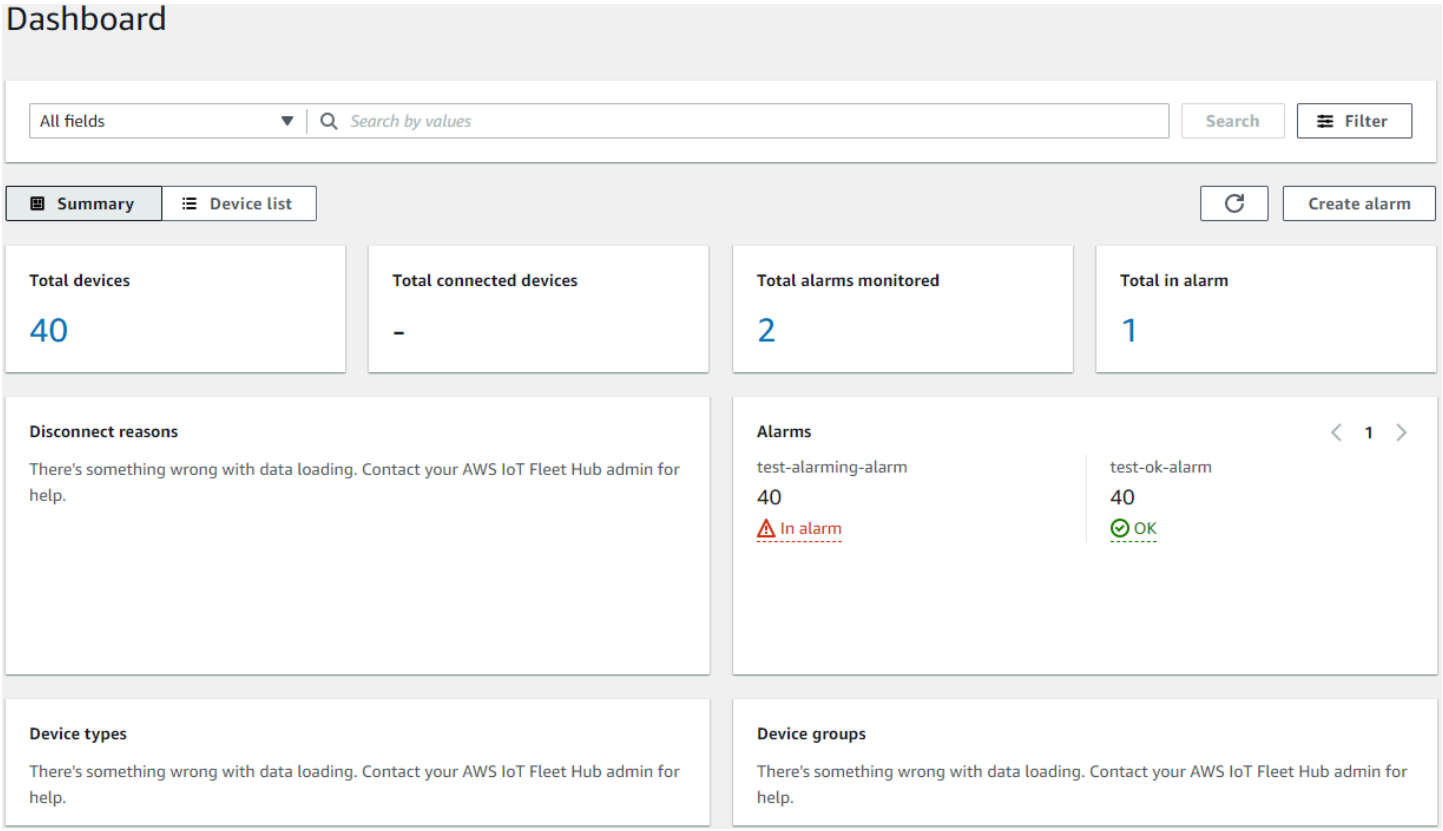
대시보드 보기

Fleet Hub for AWS IoT Device Management 웹 애플리케이션에 로그인하면 플릿에 있는 디바이스에 대한 두 가지 데이터 보기를 제공하는 대시보드가 표시됩니다.

요약

요약 보기에는 플릿의 모든 디바이스에 대한 데이터의 롤업된 보기가 표시됩니다. 여기서는 다음 정보를 제공합니다.

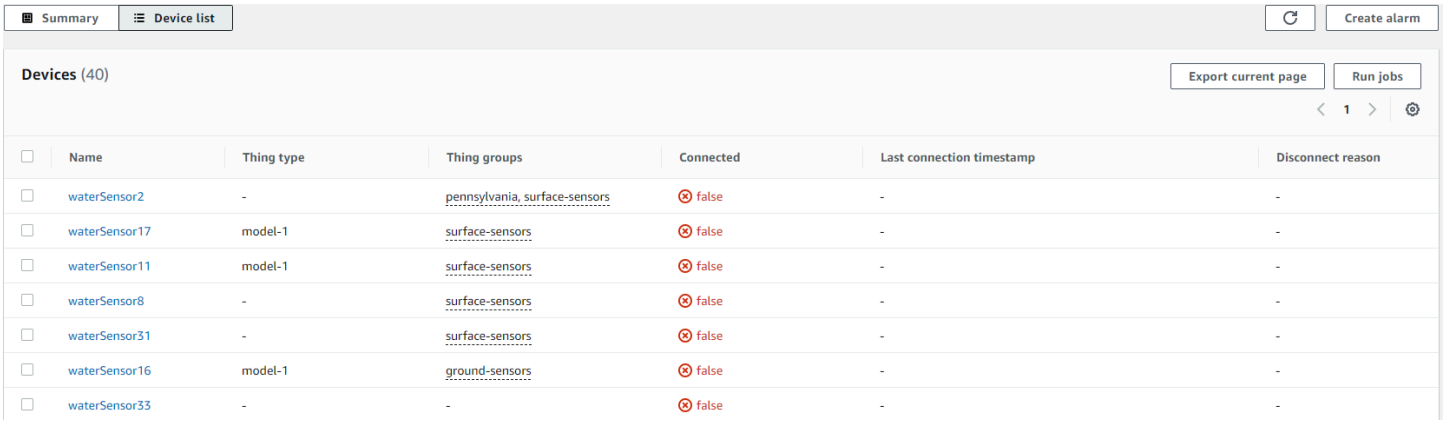
- 총 디바이스 수
- 연결된 디바이스 수
- 디바이스 연결이 끊어진 이유 목록
- 플릿에 대해 생성한 사물 유형 및 각 유형의 디바이스 수
- 플릿에 대해 생성한 사물 그룹 및 각 그룹의 디바이스 수



디바이스 목록

디바이스 목록(Device list) 보기에는 플릿의 디바이스를 나열하는 테이블이 표시됩니다. 이 테이블에는 목록의 각 디바이스에 대한 다음 정보가 표시됩니다.

- 디바이스 이름
- 디바이스의 연결 상태
- 디바이스의 마지막 연결에 대한 타임스탬프
- 연결되지 않은 디바이스의 경우 연결이 끊어진 이유
- 디바이스의 사물 유형
- 디바이스의 사물 그룹
- 플릿 인덱싱 서비스에서 사용자가 생성한 사용자 지정 필드



페이지에 표시된 장치가 포함된 CSV 파일을 다운로드하려면 장치 목록에서 현재 페이지 내보내기를 선택합니다. 목록에 페이지가 매겨진 경우 현재 페이지에 표시된 데이터만 다운로드되고 다음 페이지의 데이터는 다운로드되지 않습니다.

쿼리 및 필터를 사용하여 첫 번째 보기에서 요약 데이터를 생성하고 디바이스 목록에 나타나는 디바이스 수를 줄일 수 있습니다. 쿼리 및 필터를 사용하여 플릿의 디바이스에 대한 보다 구체적인 정보를 얻는 방법에 대한 자세한 내용은 the section called “쿼리 생성” 단원을 참조하세요.

필터를 사용하여 쿼리 만들기

이 항목에서는 Fleet Hub for AWS IoT Device Management 쿼리의 작동 방식을 설명하고 필터를 사용하여 쿼리를 생성하는 데 필요한 단계를 안내합니다.

쿼리를 사용하여 대시보드 요약 및 목록 보기에 표시되는 디바이스의 수와 유형을 제어할 수 있습니다. AWS-managed 필드, 사용자 지정 필드 및 AWS IoT 플릿 인덱싱에서 인덱싱된 데이터 원본의 모든 속성을 사용하여 쿼리를 필터링합니다. 플릿 인덱싱에 대한 자세한 내용은 플릿 인덱싱을 참조하세요.

쿼리에 키워드를 추가할 수도 있습니다. 키워드는 검색 가능한 모든 필드에 적용됩니다. 또한 키워드는 단일 쿼리에 적용할 수 있는 필터 제한(3개)을 기준으로 계산됩니다.

다음 섹션에서는 일반적인 쿼리를 생성하는 데 필요한 단계를 설명합니다.

쿼리 생성

다음 단계에서는 일반적인 쿼리를 생성하는 방법을 설명합니다.

사전 조건

- 여러 기기 (사물) 가 포함된 AWS IoT Core 계정에 연결된 Fleet Hub 애플리케이션
- Fleet Hub 애플리케이션을 사용할 권한이 있는 계정

콘솔에서 필터를 사용하여 첫 번째 Fleet Hub 쿼리 생성

1. Fleet Hub 애플리케이션으로 이동합니다.
2. 기본 대시보드에서 디바이스 목록 탭과 관련 AWS IoT Core 계정의 총 디바이스 (사물) 수를 볼 수 있는지 확인합니다.
3. 기본 대시보드에서 디바이스 목록(Device list) 탭을 선택합니다. 관리형 속성 및 사용자 지정 속성이 포함된 모든 디바이스 목록이 표시되는지 확인합니다. 사용자 지정 속성에는 속성(attributes) 접두사가 있습니다.
4. 페이지 맨 위에 쿼리에 포함하려는 키워드를 입력합니다. 키워드 쿼리는 모든 필드에 적용됩니다.
5. 페이지 상단에서 필터(Filter)를 선택합니다.
6. 필터(Filter) 모달의 필드(Field) 아래에서 필터로 사용할 필드를 선택합니다. 연산자(Operator)에서 옵션을 선택합니다. 마지막으로, 값(Value)에서 필터에 사용할 필드 값을 선택합니다.

   최대 3개의 필터를 추가할 수 있습니다. 키워드 쿼리는 이 숫자에 대해 계산됩니다.
7. 쿼리를 수행하려면 필터 적용(Apply filters)을 선택합니다. 결과에는 쿼리와 일치하는 모든 디바이스가 표시됩니다.

Fleet Hub for AWS IoT Device Management에서 작업 및 작업 템플릿 작업

> **Note**
>
> 작업 템플릿 기능은 미리 보기 중이기 때문에 변경될 수도 있습니다.

작업은 AWS IoT에 연결되는 하나 이상의 디바이스로 전송되어 실행되는 원격 작업입니다. 예를 들어 애플리케이션 또는 펌웨어 업데이트를 다운로드하여 설치하거나, 재부팅하거나, 인증서를 교체하거나, 원격 문제 해결 작업을 수행하도록 일련의 디바이스에 지시하는 작업을 정의할 수 있습니다. Fleet Hub for AWS IoT Device Management 웹 애플리케이션에서 사전 구성된 작업을 실행할 수 있습니다. 조직의 관리자가 AWS IoT 콘솔에서 작업 템플릿을 생성하여 Fleet Hub 사용자가 템플릿을 사용할 수 있도록 하는 정책을 연결합니다. Fleet Hub 애플리케이션에서 작업이 실행되는 디바이스 또는 디바이스 그룹을 지정합니다.

또한 관리자는 애플리케이션에서 볼 수 있는 디바이스 그룹을 만듭니다. 이 그룹을 보려면 탐색 창에서 디바이스 그룹(Device groups)을 선택합니다. 디바이스 그룹을 대상으로 지정할 때 작업 실행 방법에 대해 다음 두 가지 옵션 유형 중 하나를 지정할 수 있습니다.

- 스냅샷(snapshot): 작업이 한 번 실행됩니다.
- 지속(continuous): 초기 실행 후 작업은 그룹에 추가된 모든 디바이스에서 실행됩니다.

작업 템플릿 생성 및 관리에 대한 자세한 내용은 작업 템플릿 단원을 참조하세요. 작업이 작동하는 방식에 대한 자세한 내용은 작업 단원을 참조하세요.

작업 실행

Fleet Hub 애플리케이션의 여러 위치에서 작업을 실행할 수 있지만 다음 단계는 항상 동일합니다.

1. 대상 그룹이나 하나 이상의 디바이스를 선택합니다.
2. 작업 실행(Run job)을 선택합니다.
3. 작업 대상 선택(Job target selection)에서 지속(continuous) 또는 스냅샷(snapshot) 중 하나를 선택합니다.
4. 작업 템플릿을 선택합니다. 작업 요약(Job summary) 아래의 텍스트가, 실행하려는 작업 유형을 설명하는지 확인합니다.
5. 작업 이름을 입력합니다(선택 사항).
6. 실행(Run)을 선택합니다.

대상을 선택하고 Fleet Hub 애플리케이션의 다음 위치에서 이 단계를 수행할 수 있습니다.

- 대시보드의 디바이스 목록 탭.
- 특정 디바이스의 세부 정보 페이지.
- 디바이스 그룹 페이지.
- 특정 디바이스 그룹의 세부 정보 페이지.

로그 보기 및 관리

다음 위치에서 플릿에서 실행 중인 작업을 볼 수 있습니다.

- 작업 목록 페이지 — 이 페이지에는 플릿에서 실행 중인 모든 작업이 표시됩니다. 이 페이지를 보려면 탐색 창에서 작업(Jobs)을 선택합니다.
- 특정 디바이스의 세부 정보 페이지 — 이 페이지에는 디바이스에서 실행 중인 모든 작업이 표시됩니다.

각 작업에는 대상 및 런타임 정보를 포함하여 작업에 대한 요약 정보를 표시하는 세부 정보 페이지가 있습니다. 이 페이지에는 각 디바이스에서 작업의 런타임 상태가 표시됩니다. 다음 합계도 표시됩니다.

- 실행 수.
- 취소된 실행 수.
- 성공한 실행 수.
- 실패한 실행 수.
- 거부된 실행 수.
- 대기 중인 실행 수.
- 진행 중인 실행 수.
- 제거된 실행 수.
- 시간 초과 실행 수.

작업을 취소하려면 작업을 선택하고 취소(Cancel)를 선택합니다.

경보

이 단원에서는 Fleet Hub for AWS IoT Device Management 경보가 작동하는 방식과 경보를 생성하는 데 필요한 단계를 안내합니다.

Fleet Hub 경보를 생성하면 경보가 현재 대시보드에 표시된 모든 디바이스에 적용됩니다. 쿼리를 적용하지 않으면 경보가 플릿의 모든 디바이스에 적용됩니다. 대시보드 사용 및 쿼리 생성에 대한 자세한 내용은 the section called “쿼리 및 필터” 단원을 참조하세요.

경보는 Amazon CloudWatch(CloudWatch) 지표를 AWS IoT 플릿 인덱싱 서비스의 검색 가능한 필드와 함께 사용하여 CloudWatch 경보를 생성합니다. 예를 들어 플릿 내 디바이스의 평균 배터리 잔량이 50% 미만으로 떨어질 때마다 Amazon Simple Notification Service(Amazon SNS) 메시지를 생성하는 경보를 생성할 수 있습니다.

Fleet Hub 경보는 플릿 인덱싱 서비스의 GetStatistics 및 GetPercentiles 기능을 사용하여 집계 데이터를 쿼리합니다. 예를 들어 사용자 지정 숫자 필드를 추적하는 경보를 만들 때, 지정된 속성의 다음 값에 적용되는 경보 임계값을 만들 수 있습니다.

- 최대
- 개수
- 합계

- 최소
- 평균
- 10번째, 50번째, 90번째, 95번째 또는 99번째 백분위수의 값

플릿 인덱싱 서비스에서 집계 데이터를 쿼리하는 방법에 대한 자세한 내용은 집계 데이터 쿼리를 참조하세요.

다음 표에는 AWS 관리형 및 사용자 지정 필드에 사용할 수 있는 집계 유형의 몇 가지 예가 나열되어 있습니다.

필드	집계 유형
사물 유형(AWS 관리형 문자열 필드)	개수
사물 그룹(AWS 관리형 문자열 필드)	개수
연결됨(AWS 관리형 부울 필드) `true`의 값이 1입니다. `false`의 값이 0입니다.	• 최대 • 개수 • 합계 • 최소 • 평균
shadow.reported.batterylevel(플릿 인덱싱 서비스에서 생성된 숫자 집계 필드)	• 최대 • 개수 • 합계 • 최소 • 평균 • p10(10번째 백분위수) • p50(50번째 백분위수) • p90(90번째 백분위수) • p95(95번째 백분위수) • p99(99번째 백분위수)

집계 필드 및 유형을 지정하는 것 외에 다음 값도 지정합니다.

- 경보를 트리거하는 데 지정된 경보 임계값에 필요한 시간(1분 또는 5분).
- 지정된 집계 필드 및 유형에 적용할 다음 비교 연산자 중 하나.
  - 큼
  - 크거나 같음
  - 작음
  - 작거나 같음
- 지정한 비교 연산자와 함께 사용할 값.
- 경보가 트리거될 때마다 Amazon SNS 메시지를 수신하는 조직 내 사용자의 이메일 주소 목록.
- 경보 이름.

Fleet Hub 경보를 생성하려면 the section called “경보 생성” 단원을 참조하세요.

경보 생성

이 단원에서는 Fleet Hub for AWS IoT Device Management 경보를 생성하는 데 필요한 단계를 안내합니다. 관리자가 shadow.reported.batterylevel이라는 디바이스 섀도우 필드에서 집계 필드를 생성했다고 가정합니다. 이 사용자 지정 필드는 장치의 배터리 잔량을 나타냅니다. 관리자에게 AWS IoT 플릿 인덱싱 서비스에서 검색 가능한 사용자 지정 필드를 생성하도록 요청해야 합니다.

생성한 경보는 1분 동안 디바이스의 평균 배터리 잔량이 50% 미만으로 떨어질 때마다 조직 내 사용자 목록에 Amazon Simple Notification Service(Amazon SNS) 메시지를 보냅니다.

Fleet Hub 쿼리 생성

1. Fleet Hub 애플리케이션으로 이동합니다.
2. 특정 디바이스 집합을 대상으로 지정하려면 쿼리를 생성합니다. 간단한 쿼리를 만드는 방법에 대한 지침은 the section called “필터를 사용하여 쿼리 만들기” 단원을 참조하세요. 쿼리를 생성하지 않으면 경보가 플릿의 모든 디바이스에 적용됩니다.
3. 기본 대시보드 페이지에서 경보 생성을 선택합니다.
4. 집계 지표 구축(Build aggregation metric) 페이지에서 쿼리가 대상 쿼리(Target query) 아래에 나타나는지 확인합니다. 플릿 지표 집계 구성(Configure fleet metric aggregation) 섹션의 필드 선택(Choose field)에서 shadow.reported.batterylevel을 선택합니다. 이 메뉴에는 AWS 관리형 필드 및 AWS IoT 플릿 인덱싱 서비스에서 관리자가 만든 사용자 지정 필드가 포함되어 있습니다.
5. 집계 유형 선택(Choose aggregation type)에서 평균(Average)을 선택합니다. 이 선택은 디바이스 플릿의 평균 배터리 잔량 값을 기준으로 경보를 설정합니다.

6. 기간 선택(Choose period)에서 1분을 선택합니다. 이렇게 하면 디바이스 플릿이 1분 동안 지정된 경보 상태로 유지될 때 경보가 트리거됩니다.

   다음(Next)을 선택합니다.

7. 임계값 설정(Set threshold) 페이지의 …할 때마다 경보 트리거(Trigger the alarm whenever...) 섹션에서 작거나 같음(Lower/Equal)을 선택합니다. 이렇게 하면 평균 배터리 잔량 값이 지정한 값 미만으로 떨어질 때 경보가 트리거됩니다.

8. 보다(Than) 텍스트 상자에 50을 입력합니다.

   다음(Next)을 선택합니다.

9. 사용자 알림(Notify user) 페이지의 알림 -- 선택사항(Notify -- optional) 섹션에 경보가 활성 상태일 때 알림을 받는 조직의 사용자가 포함된 이메일 목록의 이름을 입력합니다. 이 목록을 채우려면 쉼표로 구분된 이메일 주소 목록을 입력합니다.

10. 경보 세부 정보(Alarm details) 섹션에서 경보 이름을 입력하고 경보의 설명을 입력합니다. 다음(Next)을 선택합니다.

11. 검토(Review) 페이지에서, 이전 페이지에서 입력한 정보를 확인합니다. 제출(Submit)을 선택합니다. 기본 대시보드로 돌아갑니다.

12. 기본 대시보드의 왼쪽 탐색 창에서 Fleet Hub 경보(Fleet Hub alarms)를 선택합니다. 생성한 경보가 표시되는지 확인합니다.

문제 해결

이 단원에서는 Fleet Hub의 사용자로서 문제를 해결하는 데 도움이 되는 문제 해결 정보와 가능한 해결책을 제공합니다.

증상	솔루션
쿼리에 더 많은 필터나 용어를 추가할 수 없습니다.	4개의 쿼리 용어 및 필터 제한에 도달하지 않았는지 확인합니다.
사용자 지정 지표를 찾을 수 없습니다.	관리자에게 플릿 인덱싱 서비스에서 지표를 생성하도록 요청합니다.
내 경보에 데이터가 표시되지 않습니다.	경보 데이터를 로드하는 데 몇 분이 소요될 수 있습니다.

증상	솔루션
경보 대상 디바이스를 변경해야 합니다.	대시보드로 이동하여 쿼리를 변경합니다.
대시보드에서 리전을 변경할 때 오류가 표시됩니다.	관리자에게 선택한 리전에서 플릿 인덱싱이 활성화되었는지 확인합니다.
내 '사물'의 연결 상태는 플리팅 인덱싱으로 인덱싱되지 않습니다.	클라이언트가 AWS IoT에 연결할 때 사물 이름과 동일한 클라이언트 ID를 사용하고 있는지 확인하세요. 클라이언트가 AWS IoT에 연결할 때 사물 이름과 다른 ID를 사용하는 경우 플릿 인덱싱에서 '사물'의 연결 상태를 인덱싱하지 않습니다.

Fleet Hub for AWS IoT Device Management 모니터링

모니터링은 Fleet Hub 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지 관리하는 데 중요한 부분입니다. AWS는 Fleet Hub를 모니터링하고, 이상이 있을 때 이를 보고하고, 적절할 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail은 직접 수행하거나 AWS 계정을 대신하여 수행한 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지, 어떤 소스 IP 주소에 호출이 이루어졌는지, 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

주제

AWS CloudTrail을 사용하여 Fleet Hub for AWS IoT Device Management API 호출 로깅

Fleet Hub for AWS IoT Device Management는 AWS CloudTrail와(과) 통합됩니다. CloudTrail 서비스는 사용자, 역할 또는 AWS 서비스가 Fleet Hub에서 수행하는 작업에 대한 기록을 제공합니다. CloudTrail은 Fleet Hub에 대한 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Fleet Hub 콘솔에서 수행한 호출과 Fleet Hub API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Fleet Hub 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다.

CloudTrail에서 수집하는 정보를 사용하여 Fleet Hub에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Fleet Hub 정보

AWS CloudTrail은 계정 생성 시 AWS 계정에서 활성화됩니다. Fleet Hub에서 활동이 발생하면 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Fleet Hub에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적(trail)을 사용하여 Amazon Simple Storage Service(Amazon S3) 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다.

또한 기타 AWS 서비스를 사용하여 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 구성할 수도 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신
- 여러 계정에서 CloudTrail 로그 파일 수신

CloudTrail은 모든 Fleet Hub 작업을 로그합니다. 이는 AWS IoT API 참조에 문서로 작성됩니다. 예를 들어 `CreateApplication` 및 `UpdateApplication` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management 사용자 자격 증명으로 했는지 여부
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Fleet Hub for AWS IoT Device Management 로그 파일 항목의 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다.

CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다.

CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

Example

다음 CloudTrail 로그 항목은 `CreateApplication` 작업에 대한 정보를 나타냅니다.

```
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "principal-id",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user-name",
            "accountId": "123456789012",
            "accessKeyId": "access-key",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "principal-id",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2020-12-04T19:59:53Z"
                }
            }
        },
        "eventTime": "2020-12-04T20:02:38Z",
        "eventSource": "iotfleethub.amazonaws.com",
        "eventName": "CreateApplication",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "72.22.186.61",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
            "applicationDescription": "Test application description",
            "applicationName": "Test application name",
            "clientToken": "c9bc7f45-3737-4ee9-9b0f-5de1aab169b2"
        },
        "responseElements": {
            "applicationUrl": "https://application-id.app.iotfleethub.aws",
            "applicationArn": "arn:aws:iotfleethub:us-
east-1:123456789012:application/application-id",
            "applicationId": "application-id"
```

```
        },
        "requestID": "5456304e-31c5-4336-9bbe-a375e3728eee",
        "eventID": "9ffb5d72-9267-4f4e-88e6-d26051133c8c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "recipientAccountId": "123456789012"
    }
```

Fleet Hub의 보안은 다음과 같습니다. AWS IoT 디바이스 관리

클라우드 보안: AWS 최우선 과제입니다. 로서 AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 두 기업 간의 공동 책임입니다. AWS 그리고 당신. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 — AWS 실행 중인 인프라를 보호할 책임이 있습니다. AWS 의 서비스 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 제3자 감사자는 보안 조치의 일환으로 당사 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS 규정 준수 프로그램 . Fleet Hub에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 다음을 참조하십시오. AWS 규정 준수 프로그램별 범위 내 서비스 .
- 클라우드에서의 보안 — 귀하의 책임은 다음에 의해 결정됩니다. AWS 사용하는 서비스. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Fleet Hub를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. AWS IoT 디바이스 관리. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Fleet Hub를 구성하는 방법을 보여줍니다. 다른 사람을 사용하는 방법도 배우게 됩니다. AWS Fleet Hub 리소스를 모니터링하고 보호하는 데 도움이 되는 서비스입니다.

주제

- Fleet Hub의 데이터 보호
- Identity 및 Access Management에 대한 Fleet Hub for AWS IoT Device Management
- Fleet Hub에 대한 규정 준수 검증 AWS IoT 디바이스 관리
- Fleet Hub의 레질리언스: AWS IoT 디바이스 관리
- AWS 플릿 허브의 관리형 정책 AWS IoT 디바이스 관리
- 플릿 허브의 인프라 보안 AWS IoT 디바이스 관리
- 교차 서비스 혼동된 대리인 방지

Fleet Hub의 데이터 보호

The AWS 공동 책임 모델: : Fleet Hub의 데이터 보호에 적용됩니다. AWS IoT 디바이스 관리. 이 모델에 설명된 대로, AWS 모든 시스템을 운영하는 글로벌 인프라를 보호하는 책임이 있습니다. AWS 클라우드. 이 인프라에서 호스팅되는 콘텐츠에 대한 통제권을 유지할 책임은 귀하에게 있습니다. 또한 귀하는 에 대한 보안 구성 및 관리 작업을 담당합니다. AWS 서비스 사용하는 것. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 다음을 참조하십시오. AWS 공동 책임 모델 및 관련 GDPR 블로그 게시물 AWS 보안 블로그.

데이터 보호를 위해 다음을 보호하는 것이 좋습니다. AWS 계정 자격 증명 및 개별 사용자 설정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM). 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSL/를 사용하여 다음과 TLS 통신할 수 있습니다. AWS 있습니다. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- 다음을 사용하여 사용자 활동 API 로깅을 설정하고 사용자 활동을 기록합니다. AWS CloudTrail. CloudTrail 트레일을 사용하여 캡처하는 방법에 대한 자세한 내용은 AWS 활동에 대한 자세한 내용은 CloudTrail 트레일 사용을 참조하십시오. AWS CloudTrail 사용자 가이드.
- 사용 AWS 암호화 솔루션 및 모든 기본 보안 제어 기능 포함 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 액세스 시 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 AWS 명령줄 인터페이스 또는 API an을 통해 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 (FIPS) 140-3을 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Fleet Hub 또는 기타 제품을 사용하는 경우가 포함됩니다. AWS 서비스 콘솔을 사용하면API, AWS CLI, 또는 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다. URL

유휴 데이터 암호화

Fleet Hub는 서버 측 암호화를 사용하여 저장된 데이터를 보호합니다. 자세한 내용은 데이터 암호화를 참조하십시오. AWS IoT의 AWS IoT 개발자 가이드.

전송 중 암호화

플로우의 클라우드 배포에서 Fleet Hub는 전송 계층 보안 (TLS) 프로토콜을 사용하여 전송 중인 데이터를 보호합니다. 자세한 내용은 전송 보안을 참조하십시오. AWS IoT의 AWS IoT 개발자 가이드.

Identity 및 Access Management에 대한 Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM) 는 AWS 서비스 이를 통해 관리자는 다음 항목에 대한 액세스를 안전하게 제어할 수 있습니다. AWS 있습니다. IAM관리자는 Fleet Hub 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM는 AWS 서비스 추가 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- 수정할 수 있다면 방법이 무엇입니까? Fleet Hub for AWS IoT Device Management 다음과 함께 작동합니다. IAM
- 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management
- 문제 해결 Fleet Hub for AWS IoT Device Management ID 및 액세스

고객

사용 방법 AWS Identity and Access Management (IAM) 는 Fleet Hub에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Fleet Hub 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Fleet Hub 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있

습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Fleet Hub의 기능에 액세스할 수 없는 경우 문제 해결 Fleet Hub for AWS IoT Device Management ID 및 액세스 단원을 참조하세요.

서비스 관리자 - 회사에서 Fleet Hub 리소스를 책임지고 있는 경우 Fleet Hub에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Fleet Hub 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한 변경 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 Fleet IAM Hub를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오수정할 수 있다면 방법이 무엇입니까? Fleet Hub for AWS IoT Device Management 다음과 함께 작동합니다. IAM .

IAM관리자 — IAM 관리자인 경우 Fleet Hub에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다. 에서 IAM 사용할 수 있는 Fleet Hub ID 기반 정책의 예를 보려면 을 참조하십시오. 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management

ID를 통한 인증

인증은 로그인하는 방법입니다. AWS ID 자격 증명 사용. 인증 (로그인) 을 받아야 합니다. AWS다음과 같이) AWS 계정 루트 사용자 IAM사용자로서, 또는 IAM 역할을 맡아서

에 로그인할 수 있습니다. AWS ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 사용할 수 있습니다. AWS IAM Identity Center 페더레이션 ID의 예로는 (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 있습니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 액세스하는 경우 AWS 페더레이션을 사용하면 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 로그인할 수 있습니다. AWS Management Console 또는 AWS 액세스 포털. 로그인에 대한 자세한 내용은 AWS로그인하는 방법을 참조하십시오. AWS 계정의 AWS 로그인 사용자 가이드.

액세스하는 경우 AWS 프로그래밍 방식으로, AWS 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 를 제공합니다. 사용하지 않는 경우 AWS 도구를 사용하려면 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 서명을 참조하십시오. AWS APIIAM사용 설명서의 요청.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예: AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 다단계 인증을 참조하십시오. AWS IAM Identity Center 사용 설명서 및 다단계 인증 사용 () MFA 의 AWS(출처: IAM 사용 설명서).

AWS 계정 루트 사용자

를 생성할 때 AWS 계정모든 계정에 완전히 액세스할 수 있는 하나의 로그인 ID로 시작합니다. AWS 서비스 및 계정 내 리소스. 이 ID를 다음과 같이 부릅니다. AWS 계정 루트 사용자는 계정을 만들 때 사용한 이메일 주소와 암호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 사용자가 ID 공급자와의 페더레이션을 사용하여 액세스하도록 하는 것입니다. AWS 서비스 임시 자격 증명을 사용하여

페더레이션 ID는 기업 사용자 디렉토리의 사용자, 웹 ID 제공업체, AWS Directory Service, ID 센터 디렉터리 또는 액세스하는 모든 사용자 AWS 서비스 ID 소스를 통해 제공된 자격 증명을 사용합니다. 페더레이션된 ID가 액세스하는 경우 AWS 계정역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해서는 다음을 사용하는 것이 좋습니다. AWS IAM Identity Center. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 위치에서 사용할 수 있습니다. AWS 계정 및 애플리케이션. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. ... 에서 AWS IAM Identity Center 사용자 가이드.

IAM 사용자 및 그룹

IAM사용자는 내 정체성에 속해 있습니다. AWS 계정 이는 한 사람이나 애플리케이션에 대한 특정 권한을 가지고 있습니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 내 안의 정체성입니다. AWS 계정 여기에는 특정 권한이 있습니다. 사용자와 비슷하지만 특정 IAM 사용자와는 관련이 없습니다. 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS Management Console 역할을 바꿔서 말이죠. 를 호출하여 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API오퍼레이션을 사용하거나 사용자 지정을 사용합니다URL. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할 수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 집합에 대한 자세한 내용은 권한 집합의 사용 권한 집합을 참조하십시오. AWS IAM Identity Center 사용 설명서.
- 임시 IAM 사용자 권한 — IAM 사용자 또는 역할은 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 경우에는 AWS 서비스역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 IAM 계정 간 리소스 액세스를 참조하십시오. IAM
- 서비스 간 액세스 — 일부 AWS 서비스 다른 기능 사용 AWS 서비스. 예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 AWS, 귀하는 주도자로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 건 주체의 권한을 사용합니다. AWS 서비스, 요청과 결합 AWS 서비스 다운스트림 서비스에 요청할 수 있습니다. FAS요청은 서비스가 다른 서비스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. AWS 서비스 또는 완료해야 할 리소스. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자

세한 내용은 권한을 위임하기 위한 역할 만들기를 참조하십시오. AWS 서비스(출처: IAM 사용 설명서).

- 서비스 연결 역할 - 서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스. 서비스가 사용자를 대신하여 작업을 수행하는 역할을 맡을 수 있습니다. 서비스 연결 역할은 다음과 같습니다. AWS 계정 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

- Amazon에서 실행되는 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행 중이고 다음을 생성하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI 또는 AWS API요청. EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. 할당하려면 AWS EC2 인스턴스에 역할을 부여하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

에서 액세스를 제어할 수 있습니다. AWS 정책을 생성하여 정책에 연결함으로써 AWS ID 또는 리소스. 정책은 다음의 객체입니다. AWS 이는 ID 또는 리소스와 연결될 경우 해당 권한을 정의합니다. AWS 주체 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 에 저장됩니다. AWS JSON문서로. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 에서 역할 정보를 가져올 수 있습니다. AWS Management Console, AWS CLI, 또는 AWS API.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 조직의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정. 관리형 정책에는 다음이 포함됩니다. AWS 관리형 정책 및 고객 관리형 정책. 관리형 정책과 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 또는 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 사용할 수 없습니다. AWS 리소스 기반 정책의 관리형 정책. IAM

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지는 않지만 리소스 기반 정책과 JSON 비슷합니다.

아마존 S3, AWS WAF, VPC Amazon은 지원하는 서비스의 예입니다ACLs. 자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는

권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCPs) — SCPs 조직 또는 OU (조직 구성 단위) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations. AWS Organizations 여러 개를 그룹화하고 중앙에서 관리하는 서비스입니다. AWS 계정 귀사가 소유한 것입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP 제한합니다. AWS 계정 루트 사용자. Organizations 및 SCPs 에 대한 자세한 내용은 의 서비스 제어 정책을 참조하십시오. AWS Organizations 사용 설명서.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 방법을 알아보려면 AWS 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 결정하려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

수정할 수 있다면 방법이 무엇입니까? Fleet Hub for AWS IoT Device Management 다음과 함께 작동합니다. IAM

Fleet Hub에 대한 액세스를 관리하는 IAM 데 사용하기 전에 플릿 허브에서 사용할 수 있는 IAM 기능에 대해 알아보십시오.

IAM함께 사용할 수 있는 기능 Fleet Hub for AWS IoT Device Management

IAM기능	Fleet Hub 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예

IAM기능	Fleet Hub 지원
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	아니요

Fleet Hub 및 기타 방법을 개괄적으로 파악하려면 AWS 서비스가 대부분의 IAM 기능과 호환됩니다. 을 참조하십시오. AWSIAM사용 IAM 설명서에서 함께 작동하는 서비스.

Fleet Hub에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Fleet Hub의 자격 증명 기반 정책 예제

Fleet Hub 자격 증명 기반 정책 예제를 보려면 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management 단원을 참조하세요.

Fleet Hub 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 또는 AWS 서비스.

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 경우 AWS 계정신뢰할 수 있는 계정의 IAM 관리자는 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

Fleet Hub에 대한 정책 작업

> **Note**
>
> Fleet Hub 애플리케이션은 `AWSIoTFleetHubFederationAccess` 관리형 정책을 사용합니다. 자세한 내용은 ??? 단원을 참조하십시오.

정책 작업 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 조치의 이름은 관련 조치와 동일합니다. AWS API오퍼레이션. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

Fleet Hub 작업 목록을 보려면 다음으로 정의된 작업을 참조하십시오. Fleet Hub for AWS IoT Device Management서비스 권한 부여 참조에서.

Fleet Hub의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
iotfleethub
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

Fleet Hub 자격 증명 기반 정책 예제를 보려면 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management 단원을 참조하세요.

Fleet Hub 정책 리소스

정책 리소스 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

ResourceJSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Fleet Hub 리소스 유형 및 해당 유형의 목록을 보려면 ARNs 다음에 정의된 리소스를 참조하십시오. Fleet Hub for AWS IoT Device Management서비스 권한 부여 참조에서. 각 리소스의 어떤 작업을 지정

할 수 있는지 알아보려면 다음으로 정의된 작업을 참조하십시오. ARN Fleet Hub for AWS IoT Device Management.

Fleet Hub 자격 증명 기반 정책 예제를 보려면 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management 단원을 참조하세요.

Fleet Hub에 대한 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 다음을 사용할 수 있습니다. AWS JSON정책을 통해 누가 무엇에 액세스할 수 있는지 지정합니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

명령문에 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에 여러 키를 지정하는 경우 AWS 논리 `AND` 연산을 사용하여 요소를 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 AWS 논리 `OR` 연산을 사용하여 조건을 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모두 보려면 AWS 글로벌 조건 키는 다음을 참조하십시오. AWSIAM사용 설명서의 글로벌 조건 컨텍스트 키.

Fleet Hub 조건 키 목록을 보려면 다음 조건 키를 참조하십시오. Fleet Hub for AWS IoT Device Management서비스 인증 참조에서. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 다음으로 정의된 작업을 참조하십시오. Fleet Hub for AWS IoT Device Management.

Fleet Hub 자격 증명 기반 정책 예제를 보려면 아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management 단원을 참조하세요.

플릿 허브의 액세스 제어 목록 (ACLs)

지원ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지는 않지만 리소스 기반 정책과 JSON 비슷합니다.

플릿 허브를 사용한 속성 기반 액세스 제어 () ABAC

지원 ABAC (정책의 태그): 예

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. In AWS, 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 엔티티에 태그를 첨부할 수 있습니다. AWS 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서. 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

Fleet Hub에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

약간 AWS 서비스 임시 자격 증명을 사용하여 로그인하면 작동하지 않습니다. 다음을 포함한 추가 정보는 AWS 서비스 임시 자격 증명으로 작업하려면 다음을 참조하십시오. AWS 서비스IAM사용 설명서에 나와 있습니다. IAM

에 로그인하면 임시 자격 증명을 사용하는 것입니다. AWS Management Console 사용자 이름과 암호를 제외한 모든 방법을 사용합니다. 예를 들어, 액세스할 때 AWS 회사의 Single Sign-On (SSO) 링크를 사용하면 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.

를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. AWS CLI 또는 AWS API. 그러면 해당 임시 자격 증명을 사용하여 액세스할 수 있습니다. AWS. AWS 장기 액세스 키를 사용하는 대신 임시 자

격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

Fleet Hub에 대한 교차 서비스 보안 주체 권한

순방향 액세스 세션 지원 (FAS): 예

IAM사용자 또는 역할을 사용하여 작업을 수행하는 경우 AWS, 귀하는 주도자로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 건 주체의 권한을 사용합니다. AWS 서비스, 요청과 결합 AWS 서비스 다운스트림 서비스에 요청할 수 있습니다. FAS요청은 서비스가 다른 서비스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. AWS 서비스 또는 완료해야 할 리소스. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

Fleet Hub 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 권한을 위임하기 위한 역할 만들기를 참조하십시오. AWS 서비스(출처: IAM 사용 설명서).

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Fleet Hub 기능이 중단될 수 있습니다. Fleet Hub가 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Fleet Hub의 서비스 연결 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스. 서비스가 사용자를 대신하여 작업을 수행하는 역할을 맡을 수 있습니다. 서비스 연결 역할은 다음과 같습니다. AWS 계정 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS 함께 작동하는 서비스. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

아이덴티티 기반 정책 예제: Fleet Hub for AWS IoT Device Management

기본적으로 사용자 및 역할은 Fleet Hub 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 다음을 사용하여 작업을 수행할 수 없습니다. AWS Management Console, AWS Command Line Interface (AWS CLI), 또는 AWS API. 사용자에게 필요한 리소스에서 작업을 수행할 수 있는 권한을 부여하기 위해 IAM 관리자는 IAM 정책을 생성할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서에서 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 형식을 포함하여 Fleet Hub에서 정의한 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 작업, 리소스 및 조건 키를 참조하십시오. Fleet Hub for AWS IoT Device Management서비스 권한 부여 참조에서.

주제

- 정책 모범 사례
- Fleet Hub 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Fleet Hub 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이러한 조치로 인해 비용이 발생할 수 있습니다. AWS 계정. ID 기반 정책을 만들거나 편집할 때는 다음 지침 및 권장 사항을 따르십시오.

- 시작해 보세요. AWS 관리형 정책 및 최소 권한 권한으로의 이동 — 사용자와 워크로드에 권한 부여를 시작하려면 다음을 사용하십시오. AWS 여러 일반 사용 사례에 대한 권한을 부여하는 관리형 정책. 다음 사이트에서 사용할 수 있습니다. AWS 계정. 를 정의하여 권한을 더 줄이는 것이 좋습니다. AWS 사용 사례에 맞는 고객 관리형 정책. 자세한 내용은 단원을 참조하세요.AWS 관리형 정책 또는 AWSIAM사용자 가이드의 작업 기능에 대한 관리형 정책.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건

을 작성할 수 SSL 있습니다. 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. AWS 서비스예: AWS CloudFormation. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.

- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM
- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 AWS 계정 보안을 강화하려면 MFA 켜십시오. API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하십시오. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

Fleet Hub 콘솔 사용

액세스하려면 Fleet Hub for AWS IoT Device Management 콘솔에는 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 자신의 Fleet Hub 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. AWS 계정. 필요한 최소 권한보다 더 제한적인 ID 기반 정책을 만들면 해당 정책을 사용하는 엔티티 (사용자 또는 역할) 에 대해 콘솔이 의도한 대로 작동하지 않습니다.

전화만 거는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. AWS CLI 또는 AWS API. 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자와 역할이 Fleet Hub 콘솔을 계속 사용할 수 있도록 하려면 플릿 허브를 `ConsoleAccess` 연결하거나 `ReadOnly` AWS 엔티티에 대한 관리형 정책. 자세한 내용은 사용 설명서의 IAM사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 다음을 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다. AWS CLI 또는 AWS API.

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

문제 해결 Fleet Hub for AWS IoT Device Management ID 및 액세스

다음 정보를 사용하면 Fleet Hub 및 를 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- Fleet Hub에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 제 외부 사람들을 허용하고 싶어요. AWS 내 Fleet Hub 리소스에 액세스할 수 있는 계정

Fleet Hub에서 작업을 수행할 권한이 없음

만약 AWS Management Console 작업을 수행할 권한이 없다는 메시지가 표시되면 관리자에게 도움을 요청해야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

> **Note**
>
> Fleet Hub 애플리케이션은 `AWSIoTFleetHubFederationAccess` 관리형 정책을 사용합니다. 자세한 내용은 ??? 단원을 참조하십시오.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. `iotfleethub:`*`GetWidget`*

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

이 경우 Mateo는 *`my-example-widget`* 작업을 사용하여 `iotfleethub:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Fleet Hub에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

약간 AWS 서비스 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 Fleet Hub에서 콘솔을 사용하여 작업을 `marymajor` 수행하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 다음 연락처로 문의하십시오. AWS 관리자에게. 관리자는 로그인 자격 증명을 제공한 사람입니다.

제 외부 사람들을 허용하고 싶어요. AWS 내 Fleet Hub 리소스에 액세스할 수 있는 계정

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록 (ACLs) 을 지원하는 서비스의 경우 해당 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Fleet Hub에서 이러한 기능을 지원하는지 여부를 알아보려면 수정할 수 있다면 방법이 무엇입니까? Fleet Hub for AWS IoT Device Management 다음과 함께 작동합니다. IAM 단원을 참조하세요.
- 전 세계의 리소스에 대한 액세스를 제공하는 방법을 알아보려면 AWS 계정 소유한 사용자는 다른 IAM 사용자에게 액세스 권한 제공을 참조하십시오. AWS 계정IAM사용 설명서에 있는 소유권.
- 리소스에 대한 액세스 권한을 제3자에게 제공하는 방법 알아보기 AWS 계정액세스 제공을 참조하십시오. AWS 계정IAM사용 설명서의 제3자가 소유합니다.
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

Fleet Hub에 대한 규정 준수 검증 AWS IoT 디바이스 관리

제3자 감사자는 여러 평가의 일환으로 Fleet Hub의 보안 및 규정 준수를 평가합니다. AWS 규정 준수 프로그램. 여기에는SOC, PCI RAMPHIPAA, Fed 등이 포함됩니다.

여부를 알아보려면 AWS 서비스 특정 규정 준수 프로그램의 범위에 속하는지 확인하려면 다음을 참조하십시오. AWS 서비스 규정 준수 프로그램별 범위 내 프로그램별 범위에서 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 을 참조하십시오. AWS 규정 준수 프로그램 .

다음을 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. AWS Artifact. 자세한 내용은 보고서 다운로드를 참조하십시오. AWS Artifact.

사용 시 귀하의 규정 준수 책임 AWS 서비스 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 기본 환경을 배포하기 위한 단계를 제공합니다. AWS 보안 및 규정 준수에 중점을 두고 있습니다.

- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서는 회사에서 사용할 수 있는 방법을 설명합니다. AWS 적격 HIPAA 애플리케이션을 만들려면.

  > **Note**
  >
  > 전부는 아닙니다. AWS 서비스 HIPAA자격이 있습니다. 자세한 내용은 HIPAA적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스 — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에는 보안 모범 사례가 요약되어 있습니다. AWS 서비스 또한 이 지침을 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 (PCI) 포함) 의 보안 제어에 매핑하십시오. ISO
- 다음 규칙을 사용하여 리소스를 평가합니다. AWS Config 개발자 가이드 — The AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이것은 AWS 서비스 내부 보안 상태를 포괄적으로 보여줍니다. AWS. Security Hub는 보안 제어를 사용하여 다음을 평가합니다. AWS 리소스를 제공하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- 아마존 GuardDuty — 이거 AWS 서비스 고객에 대한 잠재적 위협을 탐지합니다. AWS 계정의심스럽고 악의적인 활동이 있는지 환경을 모니터링하여 워크로드, 컨테이너 및 데이터를 모니터링합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하는 PCI DSS 등 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이것은 AWS 서비스 지속적으로 감사할 수 있도록 도와줍니다. AWS 사용을 통해 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Fleet Hub의 레질리언스: AWS IoT 디바이스 관리

The AWS 글로벌 인프라는 다음을 중심으로 구축됩니다. AWS 지역 및 가용 영역. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 리전을 제공하며 이러한 가용 리전은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

에 대한 자세한 내용은 AWS 지역 및 가용 영역을 참조하십시오. AWS 글로벌 인프라.

AWS 플릿 허브의 관리형 정책 AWS IoT 디바이스 관리

사용자, 그룹, 역할에 권한을 추가하려면 더 쉽게 사용할 수 있습니다. AWS 정책을 직접 작성하는 것보다 관리형 정책. 팀에 필요한 권한만 제공하는 IAM고객 관리형 정책을 만들려면 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 다음을 사용할 수 있습니다. AWS 관리형 정책. 이러한 정책은 일반적인 사용 사례를 다루며 다음과 같은 국가에서 사용할 수 있습니다. AWS 계정. 에 대한 자세한 내용은 AWS 관리형 정책을 참조하십시오. AWSIAM사용 설명서의 관리형 정책.

AWS 서비스 유지 관리 및 업데이트 AWS 관리형 정책. 에서는 권한을 변경할 수 없습니다. AWS 관리형 정책. 서비스는 경우에 따라 권한을 추가할 수 있습니다. AWS 새 기능을 지원하는 관리형 정책. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스가 업데이트할 가능성이 가장 높습니다. AWS 새 기능이 출시되거나 새 작업을 사용할 수 있게 될 때의 관리형 정책. 서비스는 권한의 권한을 제거하지 않습니다. AWS 관리형 정책을 사용하므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한, AWS 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 지원합니다. 예를 들어, ReadOnlyAccess AWS 관리형 정책은 모든 사용자에게 읽기 전용 액세스를 제공합니다. AWS 서비스 및 리소스. 서비스가 새 기능을 출시하면 AWS 새 작업 및 리소스에 대한 읽기 전용 권한을 추가합니다. 직무 정책 목록 및 설명은 을 참조하십시오. AWSIAM사용 설명서의 직무 관리 정책.

AWS 관리형 정책: AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess`정책을 IAM ID에 연결할 수 있습니다.

이 정책은 Fleet Hub에 다음을 부여합니다. AWS IoT 기기 관리 (연동 사용자) 는 조치를 취하는 데 필요한 권한을 부여했습니다. AWS IoT 및 기타 AWS 플릿 허브 웹 애플리케이션의 서비스.

Fleet Hub 웹 애플리케이션에 사용자를 추가하는 방법에 대한 자세한 내용은 ??? 단원을 참조하세요.

이 정책은 다음에서 확인하십시오. AWS 콘솔.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `iot`- 검색 AWS IoT 장치 데이터 및 플릿 수준의 작업을 수행합니다.
- `iotfleethub` - Fleet Hub 앱 메타데이터를 검색합니다.
- `cloudwatch`- CloudWatch 알람 및 메트릭 데이터를 검색합니다. 또한 Fleet Hub 경보로 범위가 지정된 작업을 생성하고 삭제할 수 있습니다.
- `sns` - 생성, 읽기, 삭제, 구독 및 구독 취소 작업을 수행합니다. 이러한 작업의 범위는 Fleet Hub SNS 항목으로 제한됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeIndex",
                "iot:DescribeThingGroup",
                "iot:GetBucketsAggregation",
                "iot:GetCardinality",
                "iot:GetIndexingConfiguration",
                "iot:GetPercentiles",
                "iot:GetStatistics",
                "iot:SearchIndex",
                "iot:CreateFleetMetric",
                "iot:ListFleetMetrics",
                "iot:DeleteFleetMetric",
                "iot:DescribeFleetMetric",
                "iot:UpdateFleetMetric",
                "iot:DescribeCustomMetric",
                "iot:ListCustomMetrics",
                "iot:ListDimensions",
                "iot:ListMetricValues",
                "iot:ListThingGroups",
                "iot:ListThingsInThingGroup",
                "iot:ListJobTemplates",
                "iot:DescribeJobTemplate",
                "iot:ListJobs",
                "iot:CreateJob",
                "iot:CancelJob",
                "iot:DescribeJob",
                "iot:ListJobExecutionsForJob",
```

```
                "iot:ListJobExecutionsForThing",
                "iot:DescribeJobExecution",
                "iot:ListSecurityProfiles",
                "iot:DescribeSecurityProfile",
                "iot:ListActiveViolations",
                "iot:GetThingShadow",
                "iot:ListNamedShadowsForThing",
                "iot:CancelJobExecution",
                "iot:DescribeEndpoint",
                "iotfleethub:DescribeApplication",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:Subscribe",
                "sns:Unsubscribe"
            ],
            "Resource": "arn:aws:sns:*:*:iotfleethub*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory"
            ],
            "Resource": "arn:aws:cloudwatch:*:*:iotfleethub*"
        }
    ]
}
```

플릿 허브 업데이트: AWS 관리형 정책

업데이트에 대한 세부 정보 보기 AWS 이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Fleet Hub에 대한 관리형 정책. 자세한 내용은 Fleet Hub 설명서 기록 페이지를 참조하세요.

변경 사항	설명	날짜
AWSIoTFleetHubFederationAccess - 기존 정책에 대한 업데이트	Fleet Hub는 앱 사용자가 검색할 수 있도록 새 권한을 추가했습니다. AWS IoT Device Defender 플릿 허브 앱의 지표 데이터.	2022년 4월 4일
AWSIoTFleetHubFederationAccess -기존 정책 업데이트	Fleet Hub는 앱 사용자가 인덱싱을 위해 추가 데이터 원본을 검색할 수 있도록 새로운 권한을 추가했습니다. 앱 사용자가 취소할 수 있는 권한도 추가되었습니다. AWS IoT 앱 내에서 작업 실행.	2021년 11월 15일
AWSIoTFleetHubFederationAccess -기존 정책 업데이트	Fleet Hub는 앱 사용자가 사물 그룹 데이터를 검색하고 다음과 같은 CRUD 작업을 수행할 수 있는 새 권한을 추가했습니다. AWS IoT 작업.	2021년 5월 24일
AWSIoTFleetHubFederationAccess -기존 정책 업데이트	플릿 허브는 지원되지 않는 플릿 허브 대시보드에 APIs 대한 권한을 제거했습니다.	2021년 4월 12일
AWSIoTFleetHubFederationAccess - 새 정책	Fleet Hub는 Fleet Hub 애플리케이션 사용자가 장치 데이터를 검색하고 수행하는 데 필요한 권한을 부여하는 새 정책을 추가했습니다. AWS IoT 조치.	2021년 4월 12일

변경 사항	설명	날짜
Fleet Hub에서 변경 사항 추적 시작	플릿 허브는 플릿 허브의 변경 사항을 추적하기 시작했습니다. AWS 관리형 정책.	2021년 4월 12일

플릿 허브의 인프라 보안 AWS IoT 디바이스 관리

Fleet Hub는 매니지드 서비스로서 다음을 수행합니다. AWS IoT 장치 관리는 다음에 의해 보호됩니다. AWS Amazon Web Services: 보안 프로세스 개요 백서에 설명된 글로벌 네트워크 보안 절차.

다음을 사용합니다. AWS 게시된 API 통화를 통해 네트워크를 통해 Fleet Hub에 액세스합니다. 클라이언트는 전송 계층 보안 (TLS) 1.2 이상을 지원해야 합니다. TLS1.3을 사용하는 것이 좋습니다. 또한 클라이언트는 Ephemeral Diffie-Hellman () 또는 Ephemeral Diffie-Hellman () 또는 타원 곡선 Epemeral Diffie-Hellman (PFS) 과 같이 완벽한 순방향 기밀성 () 을 갖춘 암호 제품군을 지원해야 합니다. DHE ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID 및 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 다음을 사용할 수 있습니다. AWS Security Token Service (AWS STS) 를 사용하여 요청에 서명하기 위한 임시 보안 자격 증명을 생성합니다.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. In AWS서비스 간 사칭으로 인해 대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(직접적으로 호출하는 서비스)가 다른 서비스(직접적으로 호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하려면 AWS 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 통해 모든 서비스의 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

Fleet Hub가 리소스에 다른 서비스를 제공하는 권한을 제한하려면 리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

혼동되는 대리자 문제를 방지하는 가장 효과적인 방법은 리소스의 전체 Amazon 리소스 이름 (ARN) 과 함께 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. Fleet Hub의 경우

aws:SourceArn은 arn:aws:iot:*region*:*account-id*:* 형식을 따라야 합니다. 다음 사항을 확인하십시오.*region* 플릿 허브 지역과 일치하고 *account-id* 고객 계정 ID와 일치합니다.

다음 예는 Fleet Hub 역할 신뢰 정책에서 aws:SourceArn 및 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다. 플릿 허브 역할을 ARN 찾으려면 플릿 허브 섹션으로 이동하십시오. AWS IoT 콘솔에서 플릿 허브 애플리케이션을 선택하여 애플리케이션 세부 정보 페이지를 확인하십시오.

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

문서 기록

다음 테이블에는 Fleet Hub 설명서 업데이트가 설명되어 있습니다. Fleet Hub에 대한 AWS 관리형 정책의 변경 사항은 Fleet Hub for AWS IoT Device Management에 대한 AWS 관리형 정책을 참조하세요.

변경 사항	설명	날짜
Fleet Hub for AWS IoT Device Management의 정식 출시 릴리스	미리 보기 기간 동안 Fleet Hub for AWS IoT Device Management에 대한 개선 사항을 반영하도록 콘텐츠를 업데이트했습니다.	2021년 5월 25일
Fleet Hub for AWS IoT Device Management의 미리 보기 릴리스	Fleet Hub for AWS IoT Device Management 사용 설명서의 미리 보기 릴리스 버전을 게시했습니다.	2020년 12월 16일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.