



Fleet Hub for AWS IoT Device 관리 가이드

Fleet Hub for AWS IoT Device Management



Fleet Hub for AWS IoT Device Management: Fleet Hub for AWS IoT Device 관리 가이드

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

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

.....	v
Fleet Hub for AWS IoT Device Management란 무엇입니까?	1
Fleet Hub for AWS IoT Device Management의 작동 방식	1
Fleet Hub 데이터 인덱싱 작동 방식	2
Fleet Hub 경고 작동 방식	2
Fleet Hub 작업 작동 방식	2
관리자를 위한 Fleet Hub for AWS IoT Device Management	3
시작	3
첫 번째 Fleet Hub 애플리케이션 생성	3
Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리	5
Fleet Hub 애플리케이션에 사용자 추가	6
Fleet Hub for AWS IoT Device Management와 상호 작용하는 AWS 및 AWS IoT Core 서비스	7
문제 해결	8
사용자를 위한 Fleet Hub for AWS IoT Device Management	10
시작하기	10
첫 번째 쿼리 만들기	10
첫 번째 경고 만들기	11
디바이스 세부 정보 보기	14
쿼리 및 필터	19
대시보드 보기	19
필터를 사용하여 쿼리 만들기	21
Fleet Hub for AWS IoT Device Management에서 작업 및 작업 템플릿 작업	22
작업 실행	23
로그 보기 및 관리	23
경보	24
경보 생성	26
문제 해결	27
Fleet Hub for AWS IoT Device Management 모니터링	29
AWS CloudTrail을 사용하여 Fleet Hub for AWS IoT Device Management API 호출 로깅	29
CloudTrail의 Fleet Hub 정보	29
Fleet Hub for AWS IoT Device Management 로그 파일 항목의 이해	30
보안	33
데이터 보호	33
유휴 데이터 암호화	34

전송 중 암호화	34
ID 및 액세스 관리	35
대상	35
ID를 통한 인증	36
정책을 사용하여 액세스 관리	39
Fleet Hub for AWS IoT Device Management 에서 IAM을 사용하는 방법	41
자격 증명 기반 정책 예제	47
문제 해결	50
규정 준수 확인	52
복원성	53
AWS 관리형 정책	53
AWSIoT FleetHubFederationAccess	54
정책 업데이트	56
인프라 보안	58
교차 서비스 혼동된 대리인 방지	58
플릿 허브 end-of-life(EOL) FAQs	60
Fleet Hub는 언제를 진행하나요 end-of-life?	60
날짜의 end-of-life Fleet Hub 애플리케이션은 어떻게 되나요?	61
날짜 당일과 이후에 기본 AWS 리소스는 end-of-life 어떻게 됩니까?	61
날짜 이전에 Fleet Hub 애플리케이션을 삭제하려면 어떻게 해야 end-of-life 합니까?	61
Fleet Hub 애플리케이션을 삭제하면 기본 리소스가 자동으로 삭제되나요?	63
기본 AWS 리소스를 삭제하려면 어떻게 해야 하나요?	63
작업을 삭제하려면 어떻게 해야 하나요?	63
Fleet Hub 경보를 삭제하려면 어떻게 해야 하나요?	64
Fleet Hub에서 생성된 IAM Identity Center 사용자를 삭제하려면 어떻게 해야 하나요?	65
날짜 이후 end-of-life 더 이상 작동하지 않는 APIs 항목은 무엇입니까?	65
Fleet Hub의 기존 기능은 무엇이며 콘솔에서 어떻게 액세스할 수 있나요?	65
문서 기록	67

AWS 는 2025년 10월 18일에 Fleet Hub 기능을 중단할 AWS IoT Device Management 예정이며 더 이상 신규 고객을 받지 않습니다. 기존 AWS IoT Device Management Fleet Hub 고객은 2025년 10월 17일까지 Fleet Hub를 사용할 수 있습니다. 자세한 내용은 [Fleet Hub end-of-life \(EOL\) FAQs](#)를 참조하세요.

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

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 `AWSIoT FleetHubFederationAccess` 관리형 정책을 사용합니다. 자세한 내용은 [??? 단원](#)을 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 Fleet Hub for AWS IoT Device Management

이 섹션에는 Fleet Hub for AWS IoT Device Management 웹 애플리케이션을 생성하고 관리하는 방법에 대한 관리자 지침이 포함되어 있습니다.

주제

- [시작](#)
- [Fleet Hub for AWS IoT Device Management와 상호 작용하는 AWS 및 AWS IoT Core 서비스](#)
- [문제 해결](#)

시작

이 섹션에서는 Fleet Hub for AWS IoT Device Management 웹 애플리케이션을 생성하고 설정하는 방법을 설명합니다.

주제

- [첫 번째 Fleet Hub 애플리케이션 생성](#)
- [Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리](#)
- [Fleet Hub 애플리케이션에 사용자 추가](#)

첫 번째 Fleet Hub 애플리케이션 생성

사전 조건

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

- [AWS 계정](#).
- 계정에 대해 [AWS IAM Identity Center](#)이 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 단계에서는 Fleet Hub for AWS IoT Device Management 웹 애플리케이션을 생성하는 방법을 설명합니다.

1. AWS IoT Core 콘솔(<https://console.aws.amazon.com/iot/>)로 이동하여 왼쪽 패널에서 Fleet Hub를 선택한 다음 애플리케이션을 선택합니다.
2. 애플리케이션 페이지에서 애플리케이션 생성(Create application)을 선택합니다.
3. IAM Identity Center 설정 페이지에서 활성화하지 않은 경우 AWS IAM Identity Center (IAM Identity Center) 단계에 따라 활성화합니다. 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 [What Is AWS IAM Identity Center?](#) 및 [Connect to your external identity provider](#)를 참조하세요. Fleet Hub 애플리케이션을 생성할 때 아직 IAM Identity Center가 없는 경우 IAM Identity Center의 조직 인스턴스를 생성해야 합니다. 생성한 Fleet Hub 애플리케이션도 IAM Identity Center의 조직 인스턴스의 AWS 리전 과 동일해야 합니다. 자세한 내용은 [IAM Identity Center 활성화](#) 및 [IAM Identity Center의 조직 인스턴스 관리](#)를 참조하세요.

페이지에서 IAM Identity Center를 이미 활성화했는지 여부를 알려줍니다.

다음을 선택합니다.

4. AWS IoT 인덱스 데이터 페이지에서 Fleet Hub AWS IoT 로의 데이터 흐름 작동 방식 섹션의 정보를 검토합니다. 이 페이지는 AWS IoT Core 플릿 인덱싱을 활성화하고 관리할 수 있는 AWS IoT Core 콘솔의 페이지로 연결됩니다. 이 서비스를 사용하여 레지스트리 데이터, 새도우 데이터, 디바이스 연결 데이터(디바이스 수명 주기 이벤트) 및 디바이스 위반 데이터를 인덱싱, 검색 및 집계할 수 있습니다. 인덱싱 인덱스를 기본적으로 AWS IoT Core 플릿하는 관리형 필드 외에도 사용자 지정 필드를 생성할 수도 있습니다.
- 이미 플릿 인덱싱을 활성화한 경우 이 페이지에는 플릿 인덱싱 설정과 사용자 지정 필드가 표시 됩니다.
 - 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 관리](#)를 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 해결](#)을 참조하세요.

Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리

AWS IoT Core 콘솔 또는를 사용하여 플릿 인덱싱 AWS CLI 을 활성화하고 [AWS IoT 레지스트리](#) 데이터, AWS IoT [디바이스 새도](#)우 데이터, [AWS IoT 연결](#) 데이터 및 [AWS IoT Device Defender 위반](#) 데이터를 인덱싱하도록 데이터 소스를 구성할 수 있습니다. 다음 단계에서는 AWS IoT Core 콘솔에서 Fleet Hub for AWS IoT Device Management 애플리케이션에 대한 플릿 인덱싱을 활성화하는 방법을 설명합니다. 를 사용하여 단계를 보려면 사물 인덱싱 관리를 AWS CLI참조하세요. <https://docs.aws.amazon.com/iot/latest/developerguide/managing-index.html>

Important

2022년 7월 20일은 AWS IoT Device Management 플릿 인덱싱과 AWS IoT Core 명명된 새도우의 통합 및 위반 AWS IoT Device Defender 탐지의 정식 릴리스입니다. 이번 정식 출시 릴리

스를 통해 새도우 이름을 지정하여 특정 명명된 새도우를 인덱싱할 수 있는 기능이 지원됩니다. 2021년 11월 30일부터 2022년 7월 19일까지인 이 기능의 공개 프리뷰 기간 중에 인덱싱을 위해 명명된 새도우를 추가한 경우, 플릿 인덱싱 설정을 재구성하고 특정 새도우 이름을 선택하여 인덱싱 비용을 줄이고 성능을 최적화하는 것이 좋습니다. 플릿 인덱싱 설정을 재구성하는 방법에 대한 자세한 정보는 [플릿 인덱싱 관리](#)를 참조하세요.

1. AWS IoT Core 콘솔(<https://console.aws.amazon.com/iot/>)로 이동하여 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 인덱싱 AWS IoT 하려는 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 관리](#)를 참조하세요.

Fleet Hub 애플리케이션에 사용자 추가

Fleet Hub for AWS IoT Device Management 웹 애플리케이션에는 새로 생성될 때 사용자가 포함되지 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 ID 를 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, 새도우 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.

기능	AWS 서비스	설명
		플릿 인덱싱에 대한 자세한 내용은 플릿 인덱싱 을 참조하세요.
쿼리에 의해 지정된 디바이스 집합에 대한 경보를 만듭니다.	Amazon CloudWatch(CloudWatch)	Fleet Hub 대시보드에는 검색 가능한 필드와 결합하여 경고 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 경고 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. 역할에 다음과 같은 적절한 신뢰 관계가 있는지 확인합니다. JSON <pre data-bbox="927 737 1508 1249"> {"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "iotfleet hub.amazonaws.com" }, "Action": "sts:AssumeRole" }] } </pre> 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.	폴릿 인덱싱을 올바르게 설정했는지 확인합니다. 폴릿 인덱싱에 대한 자세한 내용은 폴릿 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 Fleet Hub for AWS IoT Device Management](#) 단원을 참조하세요.

주제

- [시작하기](#)
- [쿼리 및 필터](#)
- [Fleet Hub for AWS IoT Device Management에서 작업 및 작업 템플릿 작업](#)
- [경보](#)
- [문제 해결](#)

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](#)
- [첫 번째 경보 만들기](#)
- [디바이스 세부 정보 보기](#)

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.

사전 조건

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

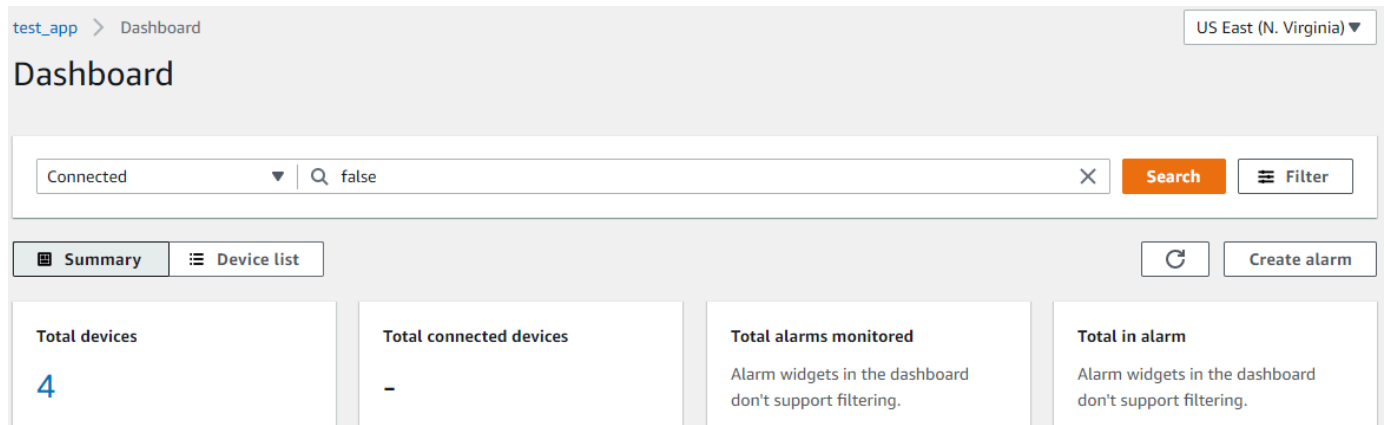
첫 번째 Fleet Hub 쿼리 만들기

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 예](#)를 참조하세요.

첫 번째 경고 만들기

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

사전 조건

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

첫 번째 경고 생성

첫 번째 Fleet Hub 경고 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 경고가 플릿의 모든 디바이스에 적용됩니다.
3. 기본 대시보드 페이지에서 경고 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.

Configure fleet metric aggregation

Choose field

Choose a searchable field from your device's data.

Connected ▼

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

Choose aggregation type

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

Count ▼

Choose period

Choose the frequency on which this alarm will be based.

1 minute ▼

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.

Trigger the alarm whenever...

Metric is
Define alarm conditions

☐ Greater
 > threshold

☒ Greater/Equal
 >= threshold

☐ Lower/Equal
 <= threshold

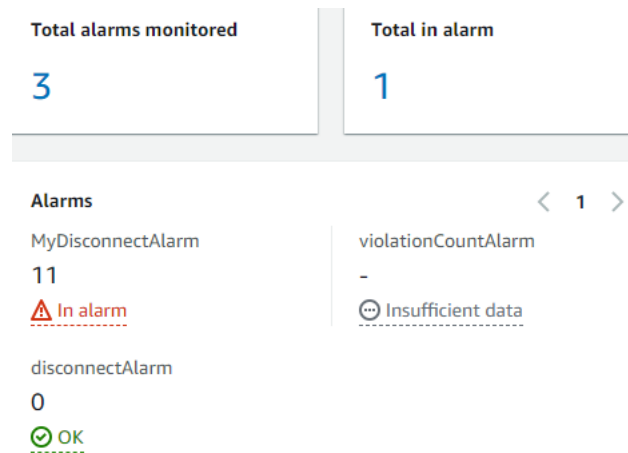
☐ Lower
 < threshold

Than
Enter a threshold value.

1

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 샘플로 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.

Fleet Hub alarms			
☐ Show triggered alarms		Delete	Create alarm
< 1 >			
	Alarm name	Status	Latest update
☐	MyDisconnectAlarm	⚠ Alarm	November 17, 2021 18:20 (UTC)
☐	disconnectAlarm	✅ OK	November 17, 2021 06:15 (UTC)
☐	violationCountAlarm	⌚ Insufficient data	November 17, 2021 06:12 (UTC)

디바이스 세부 정보 보기

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

사전 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.

test-0119 ×
Dashboards
Device groups
Jobs
Fleet Hub alarms
English (US)
Logout

test-0119 > Device groups

US East (N. Virginia) ▼

Run jobs

< 1 > ⚙

Device groups

	Group name	Parent group	Group type	Query	Group description	Created at
☐	LightBulbs	-	Static group	-	-	March 11, 2022 18:59 (UTC)
☐	MyDynamicThingGroup1	-	Dynamic group	attributes.wattage:75	-	October 17, 2021 22:15 (UTC)
☐	MyStaticThingGroup	-	Static group	-	-	March 11, 2022 18:49 (UTC)
☐	MyStaticThingGroup2	LightBulbs	Static group	-	-	March 11, 2022 19:01 (UTC)

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) 옆에서 특정 디바이스를 선택합니다.

test-0119 > Device groups > MyDynamicThingGroup1

MyDynamicThingGroup1

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

Group details

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

Devices in MyDynamicThingGroup1 (2)



< 1 >

Device name

[MyLightBulb1](#)[MyLightBulb](#)

Groups in MyDynamicThingGroup1



< 1 >

Group name

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.

Details

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 방법](#)을 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, 디바이스 디바이스 새도우 데이터, 사물 그룹에 대한 정보가 들어 있습니다.

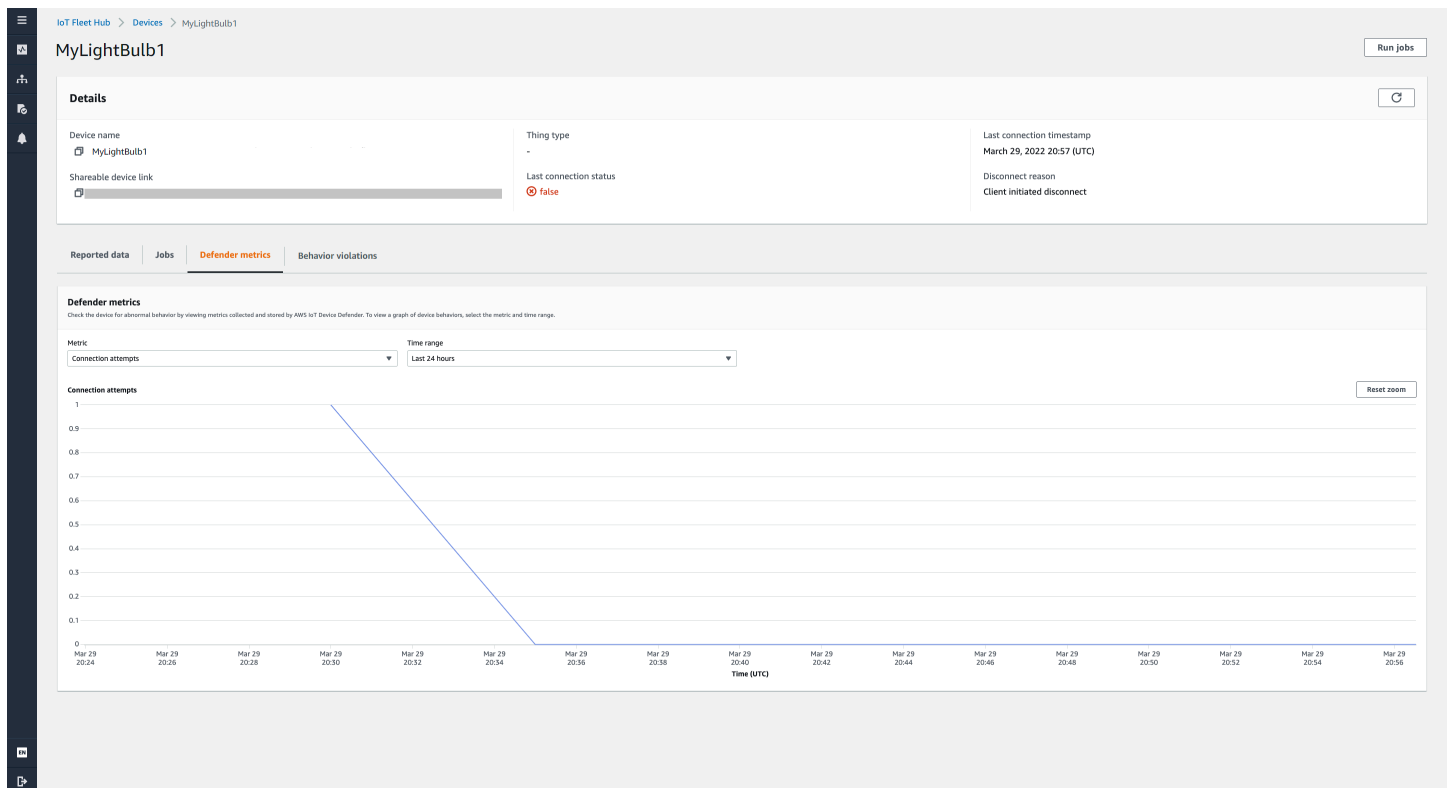
- 디바이스 필드(Device fields) - AWS IoT 플릿 인덱싱에 있는 디바이스의 인덱싱된 필드입니다. 자세한 내용은 [플릿 인덱싱 관리](#)를 참조하세요.
- 디바이스 새도우(Device shadows) - 디바이스와 연결된 새도우입니다. 디바이스 새도우에는 명명되지 않은 클래식 새도우와 명명된 새도우가 모두 포함될 수 있습니다. 디바이스 새도우에 관한 자세한 내용은 [AWS IoT 디바이스 새도우](#) 섹션을 참조하세요.
- 디바이스 그룹(Device groups) - 디바이스와 연결된 디바이스 그룹입니다. 디바이스 그룹에는 정적 사물 그룹과 동적 사물 그룹이 모두 포함될 수 있습니다. 자세한 내용은 [정적 사물 그룹](#)과 [동적 사물 그룹](#)을 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 작업](#)을 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 지표](#)를 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 인덱싱](#)에서 AWS IoT Device Defender 위반을 구성해야 합니다. AWS IoT Device Defender 보안 프로필에서 동작

위반을 설정하는 방법에 대한 자세한 내용은 [AWS IoT Device Defender 감지](#)를 참조하세요. AWS IoT Device Defender 위반 구성 방법에 대한 자세한 내용은 [Fleet Hub 애플리케이션에 대한 플릿 인덱싱 관리](#)와 [사물 인덱싱 관리](#)를 참조하세요.

쿼리 및 필터

Fleet Hub for AWS IoT Device Management의 쿼리를 사용하여 디바이스 플릿의 사물 목록을 만들거나 볼 수 있습니다. 모든 AWS 관리형 필드, 사용자 지정 필드 및 인덱싱된 데이터 소스의 모든 속성을 쿼리 필터로 사용할 수 있습니다. AWS IoT 플릿 인덱싱을 사용하여 [the section called “경보”](#)에 집계를 활성화하기 위한 사용자 정의 필드를 생성할 수도 있습니다. 플릿 인덱싱에 대한 자세한 내용은 [플릿 인덱싱](#)을 참조하세요.

주제

- [대시보드 보기](#)
- [필터를 사용하여 쿼리 만들기](#)

대시보드 보기

Fleet Hub for AWS IoT Device Management 웹 애플리케이션에 로그인하면 플릿의 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

Dashboard

All fields ▼
Search by values
Search
Filter

Summary
Device list
Refresh
Create alarm

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

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

Alarms

test-alarming-alarm
40
In alarm

test-ok-alarm
40
OK

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

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

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

Summary

Device list

Devices (40)

Export current page

Run jobs

<1>

⚙

☐	Name	Thing type	Thing groups	Connected	Last connection timestamp	Disconnect reason
☐	waterSensor2	-	pennsylvania, surface-sensors	⊗ false	-	-
☐	waterSensor17	model-1	surface-sensors	⊗ false	-	-
☐	waterSensor11	model-1	surface-sensors	⊗ false	-	-
☐	waterSensor8	-	surface-sensors	⊗ false	-	-
☐	waterSensor31	-	surface-sensors	⊗ false	-	-
☐	waterSensor16	model-1	ground-sensors	⊗ false	-	-
☐	waterSensor33	-	-	⊗ false	-	-

페이지에 표시된 디바이스를 포함하는 CSV 파일을 다운로드하려면 디바이스 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 주제에서는 Fleet Hub for AWS IoT Device Management 쿼리가 작동하는 필터를 사용하여 쿼리를 만드는 데 필요한 단계를 안내합니다.

쿼리를 사용하여 대시보드 요약 및 목록 보기에 표시되는 디바이스의 수와 유형을 제어할 수 있습니다. AWS 관리형 필드, 사용자 지정 필드 및 AWS IoT 플릿 인덱싱의 인덱싱된 데이터 소스 속성을 사용하여 쿼리를 필터링합니다. 플릿 인덱싱에 대한 자세한 내용은 [플릿 인덱싱](#)을 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 디바이스(사물)를 포함하는 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(Device list) 탭 및 연결된 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) modal의 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 생성하는데 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 쿼리](#)를 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) true의 값이 1입니다. false의 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 새도우 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 활성화 상태일 때 알림을 받는 조직의 사용자가 포함된 이메일 목록의 이름을 입력합니다. 이 목록을 채우려면 심포로 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	Solution
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	Solution
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 직접적으로 호출했는지, 어떤 소스 IP 주소에 직접 호출이 이루어졌는지, 언제 직접 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

주제

- [AWS CloudTrail을 사용하여 Fleet Hub for AWS IoT Device Management API 호출 로깅](#)

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 설명서](#)를 참조하십시오.

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 보기](#)를 참조하십시오.

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 지역에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 지역의 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 다음 자료를 참조하십시오.

- [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 참조](#)에 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. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

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

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하십시오.

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 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다.

CloudTrail 로그 파일은 퍼블릭 API 직접 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 Hub for AWS IoT Device Management의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#) 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Fleet Hub에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 [AWS 제공 범위 내 서비스 규정 준수 프로그램](#).
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Fleet Hub for AWS IoT Device Management를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Fleet Hub를 구성하는 방법을 보여줍니다. 또한 Fleet Hub 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- [Fleet Hub의 데이터 보호](#)
- [에 대한 자격 증명 및 액세스 관리 Fleet Hub for AWS IoT Device Management](#)
- [Fleet Hub for AWS IoT Device Management에 대한 규정 준수 검증](#)
- [Fleet Hub for AWS IoT Device Management의 복원성](#)
- [AWS Fleet Hub for AWS IoT Device Management에 대한 관리형 정책](#)
- [Fleet Hub for AWS IoT Device Management의 인프라 보안](#)
- [교차 서비스 혼동된 대리인 방지](#)

Fleet Hub의 데이터 보호

AWS [공동 책임 모델](#) Fleet Hub for AWS IoT Device Management의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS는 모든 것을 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 클라우드 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관

리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을 참조하세요](#).
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-3](#)을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Fleet Hub 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

유휴 데이터 암호화

Fleet Hub는 서버 측 암호화를 사용하여 저장된 데이터를 보호합니다. 자세한 내용은 AWS IoT 개발자 안내서의 [AWS IoT에서 데이터 암호화](#)를 참조하세요.

전송 중 암호화

흐름의 클라우드 배포에서 Fleet Hub는 전송 계층 보안(TLS) 프로토콜을 사용하여 전송 중 데이터를 보호합니다. 자세한 정보는 AWS IoT 개발자 안내서의 [AWS IoT에서 전송 보안](#)을 참조하세요.

에 대한 자격 증명 및 액세스 관리 Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 어떤 사용자가 Fleet Hub 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 소유)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [대상](#)
- [ID를 통한 인증](#)
- [정책을 사용하여 액세스 관리](#)
- [Fleet Hub for AWS IoT Device Management 에서 IAM을 사용하는 방법](#)
- [에 대한 자격 증명 기반 정책 예제 Fleet Hub for AWS IoT Device Management](#)
- [Fleet Hub for AWS IoT Device Management 자격 증명 및 액세스 문제 해결](#)

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 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 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Fleet Hub의 기능에 액세스할 수 없는 경우 [Fleet Hub for AWS IoT Device Management 자격 증명 및 액세스 문제 해결](#) 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 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Fleet Hub에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 [Fleet Hub for AWS IoT Device Management 에서 IAM을 사용하는 방법](#) 단원을 참조하세요.

IAM 관리자 - IAM 관리자라면 Fleet Hub에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Fleet Hub 자격 증명 기반 정책 예제를 보려면 [에 대한 자격 증명 기반 정책 예제 Fleet Hub for AWS IoT Device Management](#) 단원을 참조하세요.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [로그인하는 방법을 AWS](#) 참조하세요. [AWS 계정](#)

AWS 프로그래밍 방식으로 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 [API 요청용 AWS Signature Version 4](#)를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 [다중 인증](#) 및 IAM 사용 설명서에서 [IAM의 AWS 다중 인증](#)을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정 시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업](#)을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수입하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 [IAM Identity Center란 무엇인가요?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명에 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명에 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체](#)를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 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, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수입할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 [IAM 사용자 사용 사례](#)를 참조하세요.

IAM 역할

[IAM 역할](#)은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수입하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS

CLI 사용하여 역할을 수입할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할 수입 방법](#)을 참조하세요.

임시 보안 인증이 있는 IAM 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. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 [Create a role for a third-party identity provider \(federation\)](#)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 집합](#)을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수입하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부에서는 정책을 리소스에 직접 연결할 AWS 서비스도 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 교차 계정 리소스 액세스](#)를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [Create a role to delegate permissions to an AWS 서비스](#)를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은

나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여](#)를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 [JSON 정책 개요](#)를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수입할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, iam:GetRole 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#)을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [위탁자를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF 및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 [액세스 제어 목록\(ACL\) 개요](#)를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 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 정책에 따라 IAM 엔티티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 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 정보는 IAM 사용 설명서의 [IAM 엔티티에 대한 권한 경계](#)를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 기업이 소유한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔

터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 [Service control policies](#)을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이 포함 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [리소스 제어 정책\(RCPs\)](#)을 참조하세요.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 [세션 정책](#)을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

Fleet Hub for AWS IoT Device Management 에서 IAM을 사용하는 방법

IAM을 사용하여 Fleet Hub에 대한 액세스를 관리하기 전에 Fleet Hub에서 사용할 수 있는 IAM 기능을 알아보세요.

에서 사용할 수 있는 IAM 기능 Fleet Hub for AWS IoT Device Management

IAM 기능	Fleet Hub 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 기능	Fleet Hub 지원
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 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 [AWS IAM으로 작업하는 서비스를](#) 참조하세요.

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 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 [고객 관리형 정책으로 사용자 지정 IAM 권한 정의](#)를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

Fleet Hub의 자격 증명 기반 정책 예제

Fleet Hub 자격 증명 기반 정책 예제를 보려면 [예 대한 자격 증명 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 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [위탁자를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 있는 계정에 있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 [교차 계정 리소스 액세스](#)를 참조하세요.

Fleet Hub에 대한 정책 작업

Note

Fleet Hub 애플리케이션은 AWSIoT FleetHubFederationAccess 관리형 정책을 사용합니다. 자세한 내용은 [??? 단원](#)을 참조하십시오.

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 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 포함하세요.

Fleet Hub 작업 목록을 보려면 서비스 권한 부여 참조의 [Fleet Hub for AWS IoT Device Management에서 정의한 작업](#)을 참조하세요.

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 [에 대한 자격 증명 기반 정책 예제 Fleet Hub for AWS IoT Device Management](#) 단원을 참조하세요.

Fleet Hub 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 [Amazon 리소스 이름\(ARN\)](#)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 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 ARN의 목록을 보려면 서비스 권한 부여 참조의 [Fleet Hub for AWS IoT Device Management에서 정의한 리소스](#)를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 [Fleet Hub for AWS IoT Device Management가 정의한 작업](#)을 참조하세요.

Fleet Hub 자격 증명 기반 정책 예제를 보려면 [에 대한 자격 증명 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 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 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 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS는 논리적 AND 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

Fleet Hub 조건 키 목록을 보려면 서비스 권한 부여 참조의 [Fleet Hub for AWS IoT Device Management의 조건 키](#)를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 [에서 정의한 작업을 Fleet Hub for AWS IoT Device Management](#) 참조하세요.

Fleet Hub 자격 증명 기반 정책 예제를 보려면 [에 대한 자격 증명 기반 정책 예제 Fleet Hub for AWS IoT Device Management](#) 단원을 참조하세요.

Fleet Hub의 액세스 제어 목록(ACL)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Fleet Hub에서 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 여기서 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 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.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 통한 권한 정의](#)를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어\(ABAC\) 사용](#)을 참조하세요.

Fleet Hub에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 [AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는](#) 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 [사용자에서 IAM 역할로 전환\(콘솔\)](#)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 `access AWS. AWS recommends`에 액세스할 수 있습니다. 자세한 내용은 [IAM의 임시 보안 자격 증명](#) 단원을 참조하세요.

Fleet Hub에 대한 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [전달 액세스 세션](#)을 참조하세요.

Fleet Hub 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [Create a role to delegate permissions to an AWS 서비스](#)를 참조하세요.

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 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수입할 수 있습니다. 서비스 연결 역할은 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 [IAM으로 작업하는AWS 서비스](#)를 참조하세요. 서비스 연결 역할 열에서 Yes이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

에 대한 자격 증명 기반 정책 예제 Fleet Hub for AWS IoT Device Management

기본적으로 사용자 및 역할은 Fleet Hub 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면

IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Fleet Hub에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조 [에서 Fleet Hub for AWS IoT Device Management에 대한 작업, 리소스 및 조건 키](#)를 참조하세요.

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. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 관리형 정책](#) 또는 [AWS 직무에 대한 관리형 정책](#)을 참조하세요.
- 최소 권한 적용 - IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 [IAM의 정책 및 권한](#)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특징을 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건](#)을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을

확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer에서 정책 검증](#)을 참조하세요.

- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정컵니다. API 작업을 직접 호출할 때 MFA가 필요하다면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [MFA를 통한 보안 API 액세스](#)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

Fleet Hub 콘솔 사용

Fleet Hub for AWS IoT Device Management 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Fleet Hub 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 여전히 Fleet Hub 콘솔을 사용할 수 있도록 하려면 Fleet Hub ConsoleAccess 또는 ReadOnly AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

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

```

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

```

Fleet Hub for AWS IoT Device Management 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Fleet Hub 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- [Fleet Hub에서 작업을 수행할 권한이 없음](#)
- [iam:PassRole을 수행하도록 인증되지 않음](#)
- [내 AWS 계정 외부의 사람이 내 Fleet Hub 리소스에 액세스하도록 허용하고 싶습니다.](#)

Fleet Hub에서 작업을 수행할 권한이 없음

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

Note

Fleet Hub 애플리케이션은 `AWSIoT FleetHubFederationAccess` 관리형 정책을 사용합니다. 자세한 내용은 [??? 단원](#)을 참조하세요.

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

```
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.

`iam:PassRole`을 수행하도록 인증되지 않음

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

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

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Fleet Hub에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스에 서비스 역할이 부여한 권한이 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 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Fleet Hub 리소스에 액세스하도록 허용하고 싶습니다.

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 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Fleet Hub에서 이러한 기능을 지원하는지 여부를 알아보려면 [Fleet Hub for AWS IoT Device Management](#)에서 [IAM을 사용하는 방법](#) 단원을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 [IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요](#).
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [타사가 AWS 계정 소유한에 대한 액세스 권한 제공을](#) AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 [외부에서 인증된 사용자에게 액세스 권한 제공\(ID 페더레이션\)](#)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 [IAM의 크로스 계정 리소스 액세스](#)를 참조하세요.

Fleet Hub for AWS IoT Device Management에 대한 규정 준수 검증

타사 감사자는 여러 규정 준수 프로그램의 일환으로 Fleet Hub의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 [AWS 서비스 규정 준수 프로그램 제공 범위](#) 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 [AWS 규정 준수 프로그램](#).

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 [Downloading Reports inDownloading AWS Artifact](#)을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- [보안 규정 준수 및 거버넌스](#) - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- [HIPAA 적격 서비스 참조](#) - HIPAA 적격 서비스가 나열되어 있습니다. 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다.
- [AWS 규정 준수 리소스](#) -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.

- [AWS 고객 규정 준수 가이드](#) - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), Payment Card Industry Security Standards Council(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) -이 AWS Config 서비스는 리소스 구성 이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#) - 내 보안 상태에 대한 포괄적인 보기를 AWS 서비스 제공합니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 [Security Hub 제어 참조](#)를 참조하세요.
- [Amazon GuardDuty](#) - 의심스러운 활동과 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- [AWS Audit Manager](#) - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위협과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Fleet Hub for AWS IoT Device Management의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 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.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

AWS Fleet Hub for AWS IoT Device Management에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 [IAM 고객 관리형 정책을 생성](#)하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이러한 정책은 일반적인 사용 사례를 다루며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 관리형 정책](#)을 참조하세요.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 [직무에 관한 AWS 관리형 정책](#)을 참조하세요.

AWS 관리형 정책: AWSIoT FleetHubFederationAccess

AWSIoT FleetHubFederationAccess 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Fleet Hub for AWS IoT Device Management 페더레이션 사용자에게 Fleet Hub 웹 애플리케이션의 AWS IoT 및 기타 AWS 서비스에서 작업을 수행하는 데 필요한 권한을 부여합니다.

Fleet Hub 웹 애플리케이션에 사용자를 추가하는 방법에 대한 자세한 내용은 [??? 단원](#)을 참조하세요.

[AWS 콘솔](#)에서 이 정책을 봅니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `iot` - AWS IoT 디바이스 데이터를 검색하고 플릿 수준 작업을 수행합니다.
- `iotfleethub` - Fleet Hub 앱 메타데이터를 검색합니다.
- `cloudwatch` - CloudWatch 경보 및 지표 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 주제입니다.

JSON

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

```

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

```

AWS 관리형 정책에 대한 Fleet Hub 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Fleet Hub의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 자세한 내용은 Fleet Hub [설명서 기록](#) 페이지를 참조하세요.

변경 사항	설명	날짜
AWSIoT FleetHub FederationAccess – 기존 정책에 대한 업데이트	Fleet Hub는 앱 사용자가 Fleet Hub 앱에서 AWS IoT Device Defender 지표 데이터를 검색할 수 있도록 새로운 권한을 추가했습니다.	2022년 4월 4일
AWSIoT FleetHub FederationAccess – 기존 정책에 대한 업데이트	Fleet Hub는 앱 사용자가 인덱싱을 위해 추가 데이터 원본을 검색할 수 있도록 새로운 권한을 추가했습니다. 앱 사용자가 앱 내에서 AWS IoT 작업을 취소할 수 있는 권한도 추가됩니다.	2021년 11월 15일
AWSIoT FleetHub FederationAccess – 기존 정책에 대한 업데이트	Fleet Hub는 앱 사용자가 사물 그룹 데이터를 검색하고 AWS IoT 작업에 대한 CRUD 작업을 수행할 수 있는 새로운 권한을 추가했습니다.	2021년 5월 24일
AWSIoT FleetHub FederationAccess – 기존 정책에 대한 업데이트	Fleet Hub는 지원되지 않는 Fleet Hub 대시보드 API에 대한 권한을 제거했습니다.	2021년 4월 12일
AWSIoT FleetHub FederationAccess – 새로운 정책	Fleet Hub는 Fleet Hub 애플리케이션 사용자가 디바이스 데이터를 검색하고 AWS IoT 작업을 수행하는 데 필요한 권한을 부여하는 새 정책을 추가했습니다.	2021년 4월 12일
Fleet Hub에서 변경 사항 추적 시작	Fleet Hub는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 4월 12일

Fleet Hub for AWS IoT Device Management의 인프라 보안

관리형 서비스인 Fleet Hub for AWS IoT Device Management는 [Amazon Web Services: 보안 프로세스 개요](#) 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Fleet Hub에 액세스합니다. 클라이언트가 전송 계층 보안(TLS) 1.2 이상을 지원해야 합니다. TLS 1.3을 사용할 것을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 가장은 혼동된 대리자 문제를 초래할 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 방지하기 위해 AWS에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 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 문서에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 Amazon 리소스 이름(ARN)이 포함된 aws:SourceArn 전역 조건 컨텍스트 키를 사용하는 것입니다. Fleet Hub의 경우 aws:SourceArn은 arn:aws:iot:**region**:**account-id**:* 형식을 따라야 합니다. **region**이 Fleet Hub 리전과 일치하고 **account-id**가 고객 계정 ID와 일치하는지 확인합니다.

다음 예는 Fleet Hub 역할 신뢰 정책에서 aws:SourceArn 및 aws:SourceAccount 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다. Fleet Hub 역할 ARN을 찾으려면 AWS IoT 콘솔의 Fleet Hub 섹션으로 이동하여 Fleet Hub 애플리케이션을 선택하여 애플리케이션 세부 정보 페이지를 확인합니다.

JSON

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


플릿 허브 end-of-life(EOL) FAQs

플릿 허브 end-of-life FAQs

- [Fleet Hub는 언제를 진행하나요 end-of-life?](#)
- [날짜의 end-of-life Fleet Hub 애플리케이션은 어떻게 되나요?](#)
- [날짜 당일과 이후에 기본 AWS 리소스는 end-of-life 어떻게 됩니까?](#)
- [날짜 이전에 Fleet Hub 애플리케이션을 삭제하려면 어떻게 해야 end-of-life 합니까?](#)
- [Fleet Hub 애플리케이션을 삭제하면 기본 리소스가 자동으로 삭제되나요?](#)
- [기본 AWS 리소스를 삭제하려면 어떻게 해야 하나요?](#)
- [날짜 이후 end-of-life 더 이상 작동하지 않는 APIs 항목은 무엇입니까?](#)
- [Fleet Hub의 기존 기능은 무엇이며 콘솔에서 어떻게 액세스할 수 있나요?](#)

Fleet Hub는 언제를 진행하나요 end-of-life?

AWS 는 2025년 10월 18일에 Fleet Hub for AWS IoT Device Management를 중단합니다. Fleet Hub 는 단계별 EOL 방식으로 로 전환됩니다. Fleet Hub에서 사용할 수 있는 기능은 AWS IoT Device Management 콘솔 내에서도 사용할 수 있어 비즈니스 요구 사항을 계속 지원할 수 있습니다.

1. 2024년 10월 17일에 AWS 는 신규 고객의 Fleet Hub 온보딩을 중지합니다. 2024년 10월 17일 이전에 Fleet Hub 애플리케이션을 보유하고 있지 않으면 새 Fleet Hub 고객으로 식별됩니다. 그렇지 않으면 기존 Fleet Hub 고객으로 식별됩니다.
2. 기존 Fleet Hub 고객은 2025년 10월 17일까지 Fleet Hub 애플리케이션을 계속 사용할 수 있습니다. 2024년 10월 17일부터 2025년 10월 17일까지 Fleet Hub에 대한 새로운 기능 업데이트는 없으며 중요한 버그 수정을 AWS 지원합니다.
3. 2025년 10월 18일에 AWS 는 Fleet Hub for AWS IoT Device Management에 대한 지원을 중지합니다. 이 날짜에 Fleet Hub가 end-of-life 도달하여 더 이상 Fleet Hub를 사용할 수 없습니다. Fleet Hub의 중단은 다른 AWS IoT Device Management 기능에 영향을 미치지 않습니다. 에서 제공하는 기존 기능을 계속 사용할 수 있습니다 AWS IoT Device Management. 자세한 내용은 [??? 단원](#)을 참조하십시오.

날짜의 end-of-life Fleet Hub 애플리케이션은 어떻게 되나요?

2025년 10월 18EOL일에 Fleet Hub 애플리케이션이 삭제되고 더 이상 Fleet Hub에 액세스할 수 없습니다. Fleet Hub와 연결된 AWS 리소스는 자동으로 삭제되지 않습니다. 이러한 리소스에는 AWS IoT Device Management [작업](#), 플릿 AWS IoT Device Management [지표](#), [경보 및 Amazon 주제와 같은 Fleet Hub](#) 경보 구성 요소가 포함됩니다. CloudWatch SNS 와 독립적으로 AWS Management Console AWS CLI또는 AWS SDK 모니터링 요구 사항에 따라 이러한 리소스에 계속 액세스할 수 있습니다. 기본 AWS 리소스를 삭제하려면 [???](#) 섹션을 참조하세요.

날짜 당일과 이후에 기본 AWS 리소스는 end-of-life 어떻게 됩니까?

모니터링 요구 사항에 따라와 독립적으로 Fleet Hub와 연결된 기본 AWS 리소스 AWS Management Console 에 계속 액세스할 수 있습니다. 이러한 리소스에는 AWS IoT Device Management [작업](#), 플릿 AWS IoT Device Management [지표](#)와 같은 플릿 허브 경보 구성 요소, CloudWatch 경보 및 Amazon SNS 주제가 포함됩니다. Fleet Hub 애플리케이션 사용자는 IAM Identity Center 사용자 풀에서 직접 할당됩니다. IAM Identity Center 사용자가 Fleet Hub 애플리케이션에 액세스하기 위해서만 생성되었고 다른 AWS 서비스에 사용하지 않는 경우 콘솔 내 IAM Identity Center의 사용자 및 애플리케이션 탭에서 삭제할 수 있습니다. 자세한 내용은 [??? 단원](#)을 참조하십시오.

날짜 이전에 Fleet Hub 애플리케이션을 삭제하려면 어떻게 해야 end-of-life 합니까?

EOL 날짜 이전에 Fleet Hub 애플리케이션을 삭제하려면 AWS IoT 콘솔 또는 [--delete-application](#) AWS CLI 명령을 사용합니다.

Note

Fleet Hub 애플리케이션을 삭제해도 Fleet Hub와 연결된 기본 AWS 리소스는 삭제되지 않습니다. 이러한 리소스를 삭제하려면 [the section called “기본 AWS 리소스를 삭제하려면 어떻게 해야 하나요?”](#) 섹션을 참조하세요.

AWS IoT 콘솔을 사용하여 Fleet Hub 애플리케이션을 삭제하려면 단계를 따릅니다.

1. AWS IoT 콘솔로 이동하여 왼쪽 탐색에서 Fleet Hub를 선택한 다음 애플리케이션을 선택합니다.

2. 애플리케이션 페이지에서 삭제하고자 하는 Fleet Hub 애플리케이션을 선택합니다. Delete(삭제)를 선택합니다. 애플리케이션 삭제 확인을 요청하는 프롬프트 창이 표시됩니다. 삭제를 확인하려면 'delete'를 입력한 후 삭제를 선택합니다.

를 사용하여 Fleet Hub 애플리케이션을 삭제하려면 단계를 AWS CLI따릅니다.

1. 를 사용하여 Fleet Hub 애플리케이션을 삭제하려면 애플리케이션 ID를 알아야 AWS CLI합니다. [--list-applications](#) CLI 명령을 먼저 실행하여 모든 Fleet Hub 애플리케이션과 해당 애플리케이션을 나열합니다IDs.

를 사용하여 Fleet Hub 애플리케이션을 나열하려면 다음 명령을 IDs실행합니다.

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

명령의 출력은 다음과 같을 수 있습니다.

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

2. Fleet Hub 애플리케이션을 배포하려면 AWS CLI 명령을 입력합니다.

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

명령은 출력을 생성하지 않습니다. --list-applications CLI 명령을 실행하여 지정된 애플리케이션이 삭제되었는지 확인할 수 있습니다.

Fleet Hub 애플리케이션을 삭제하면 기본 리소스가 자동으로 삭제되나요?

아니요. Fleet Hub 애플리케이션을 삭제해도 기본 리소스는 자동으로 삭제되지 않습니다. Fleet Hub와 연결된 AWS 리소스를 삭제하려면 섹션을 참조하세요 [???](#).

기본 AWS 리소스를 삭제하려면 어떻게 해야 하나요?

Fleet Hub를 사용하면 고객이 AWS IoT Device Management 작업 및 Fleet Hub 경보와 같은 AWS 리소스를 생성할 수 있습니다. Fleet Hub 애플리케이션을 삭제해도 이러한 리소스는 삭제되지 않으며 [???](#)에 설명된 대로 비즈니스 요구 사항을 지원하기 위해 계속 액세스할 수 있습니다. 이러한 기본 리소스를 삭제하려면 아래 단계를 따르세요.

작업을 삭제하려면 어떻게 해야 하나요?

작업을 삭제하려면 먼저 작업을 취소해야 합니다. EOL 날짜 이전에 Fleet Hub에서 직접 작업을 취소할 수 있습니다. 또한 AWS IoT 콘솔을 사용하여 원할 때마다 작업을 취소하고 삭제할 수 있습니다.

Fleet Hub 애플리케이션에서 작업을 취소하려면

1. Fleet Hub 애플리케이션으로 이동하여 작업 탭을 선택합니다.
2. 취소하려는 작업을 선택합니다.
3. 작업 취소를 선택합니다.

AWS IoT 콘솔에서 작업을 취소하고 삭제하려면

1. 원격 작업으로 이동하여 작업 탭을 선택합니다.
2. 취소하려는 작업을 선택합니다.
3. 취소를 선택합니다.

4. 동일한 작업 탭에서 삭제할 작업을 선택합니다.
5. Delete(삭제)를 선택합니다.

Fleet Hub 경보를 삭제하려면 어떻게 해야 하나요?

Fleet Hub 애플리케이션 내에서 직접 Fleet Hub 경보를 삭제할 수 있습니다. 그러면 플릿 지표, CloudWatch 경보 및 Amazon SNS 주제와 같은 모든 기본 구성 요소가 자동으로 삭제됩니다. Fleet Hub 애플리케이션에서 Fleet Hub 경보 탭으로 이동하여 삭제할 경보를 선택하고 삭제를 선택합니다. 또는를 사용하여 Fleet Hub 경보를 삭제할 수 있습니다 AWS Management Console. 다음 단계에 따라 AWS 리전 간에 여러 애플리케이션을 삭제할 수 있습니다.

Fleet Hub 애플리케이션에서 Fleet Hub 경보를 삭제하려면

1. Fleet Hub 애플리케이션에서 Fleet Hub 경보 탭으로 이동합니다.
2. 삭제할 프로젝트를 선택하고 삭제를 선택합니다. 이 작업은 모든 기본 구성 요소를 삭제합니다.

AWS IoT 콘솔에서 플릿 지표를 삭제하려면

1. AWS IoT 콘솔의 왼쪽 탐색에서 관리로 이동합니다. 모든 디바이스 에서 플릿 지표를 선택합니다.
2. 이름이 'iotfleethub' 접두사로 표시된 모든 플릿 지표를 선택합니다.
3. Delete(삭제)를 선택합니다.

CloudWatch 콘솔에서 CloudWatch 경보를 삭제하려면

1. CloudWatch 콘솔 내의 모든 경보 탭으로 이동합니다.
2. 이름이 'iotfleethub' 접두사로 표시된 모든 지표를 선택합니다.
3. 작업으로 이동하여 삭제를 선택합니다.

Amazon SNS 콘솔에서 생성된 경보를 수신하는 Amazon SNS 주제를 삭제하려면

1. Amazon SNS 콘솔의 주제 탭으로 이동합니다.
2. 이름이 'iotfleethub' 접두사로 표시된 모든 주제를 선택합니다.
3. Delete(삭제)를 선택합니다.

Fleet Hub에서 생성된 IAM Identity Center 사용자를 삭제하려면 어떻게 해야 하나요?

IAM Identity Center 사용자가 Fleet Hub 애플리케이션에 액세스하기 위해서만 생성되었고 다른 AWS 서비스에 사용하지 않는 경우 콘솔 내 IAM Identity Center의 사용자 및 애플리케이션 탭에서 삭제할 수 있습니다.

날짜 이후 end-of-life 더 이상 작동하지 않는 APIs 항목은 무엇입니까?

2025년 10월 18일에 Fleet Hub 애플리케이션의 수명 주기 관리와 APIs 관련된 모든를 중단할 예정입니다. 이는 Fleet Hub에만 APIs 연결되며 다른 AWS IoT Device Management 기능에는 영향을 주지 않습니다. 기존 Fleet Hub 고객은 2025년 10월 17APIs일까지 이러한 기능을 계속 사용할 수 있습니다.

- [CreateApplication](#)
- [DeleteApplication](#)
- [DescribeApplication](#)
- [ListApplication](#)
- [ListTagsForResource](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)

Fleet Hub의 기존 기능은 무엇이며 콘솔에서 어떻게 액세스할 수 있나요?

Fleet Hub는 AWS IoT Device Management 기능을 사용하여 구축된 다음과 같은 키 모니터링 및 관리 기능을 제공합니다. 이러한 기능은 모두 Fleet Hub 애플리케이션 외부에서 사용할 수 있습니다. AWS IoT Device Management 콘솔 내에 직접 있으며 비즈니스 요구 사항을 지원하기 위해 계속 액세스할 수 있습니다.

플릿 연결 상태 요약

Fleet Hub 대시보드는 IoT 플릿의 연결 상태를 연결 세부 정보와 함께 요약합니다. 연결 및 연결 해제된 디바이스 수와 연결 해제된 디바이스의 배포를 연결 해제 이유별로 보여줍니다. AWS IoT 콘

솔의 모니터 탭에서 동등한 연결 상태 모니터링 대시보드를 사용할 수 있습니다. 위젯을 활성화하여 연결된 디바이스 수, 연결 해제 속도 및 연결 해제 이유를 모니터링할 수 있습니다. 자세한 내용은 [AWS IoT Device Management adds a unified connectivity metrics monitoring dashboard](#) 섹션을 참조하세요.

Fleet Hub 경보

Fleet Hub 경보를 사용하면 임계값 기반 경보를 생성하고 모니터링할 수 있습니다. Fleet Hub 경보는 플릿 인덱싱 및 Amazon CloudWatch 경보에서 제공하는 AWS IoT Device Management 플릿 지표를 활용합니다. Amazon CloudWatch 콘솔에서 이러한 플릿 지표를 직접 모니터링하고 AWS IoT 콘솔에서 다시 구성할 수 있습니다. 이름이 'iotfleethub'로 접두사로 지정된 플릿 지표 및 CloudWatch 경보는 Fleet Hub와 연결됩니다. 콘솔에서 계속 액세스할 수 있습니다. Amazon CloudWatch를 사용하여 시간 경과에 따라 이러한 지표를 모니터링하고 추세를 볼 수 있습니다. AWS IoT 콘솔에서 추가 플릿 지표를 생성한 다음 모니터링하여 Amazon에서 경보를 설정할 수도 있습니다 CloudWatch. 자세한 내용은 [에서 플릿 지표 보기를 CloudWatch](#) 참조하세요.

디바이스 검색

Fleet Hub를 사용하면 인덱싱된 데이터 소스의 기준을 사용하여 여러 필터를 적용하여 디바이스 검색을 세분화할 수 있습니다. 이 기능은 [플릿 인덱싱](#)의 검색 기능을 활용합니다. 디바이스 검색은 AWS IoT Device Management 콘솔을 통해 고급 사물 검색 페이지에서 직접 사용할 수 있습니다. 고급 사물 검색 페이지를 찾으려면 관리에서 사물을 선택한 다음 모든 디바이스를 선택합니다. 사물 페이지의 오른쪽 상단 모서리에서 고급 검색을 선택합니다.

작업 실행

사물 또는 그룹을 대상으로 선택하여 Fleet Hub에서 직접 작업을 실행할 수 있습니다. 또한 AWS IoT Device Management 콘솔의 작업 페이지에서 작업을 실행할 수 있습니다. 여기서 작업 실행 대상으로 사물, 정적 그룹 또는 동적 그룹을 정의할 수 있습니다.

디바이스 세부 정보 보기

Fleet Hub는 모든 디바이스 페이지에서 디바이스(사물) 수준 세부 보기를 제공합니다. 유사한 디바이스 수준 세부 보기는 AWS IoT Device Management 콘솔의 사물 탭에서 직접 사용하거나 플릿 인덱싱 검색 쿼리 결과를 통해 반환된 특정 사물을 클릭하여 사용할 수 있습니다.

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 정책](#)을 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