Fleet Hub AWS IoT 设备管理指南

用于 AWS IoT 设备管理的舰队中心

用于 AWS IoT 设备管理的舰队中心: Fleet Hub AWS IoT 设备管理指南

Table of Contents

什么是 Fleet Hub for AWS IoT Device Management？

借助 Fleet Hub for AWS IoT Device Management (Fleet Hub)，您可以构建独立的 Web 应用程序来监控设备机群的运行状况。您可以将这些应用程序提供给组织中的用户，即使他们没有AWS账户。使用 Fleet Hub 管理常见的机群范围任务，例如调查和修复操作和安全问题。

Fleet Hub 提供以下功能。

- 近乎实时地监控设备机群。
- 设置告警以将异常行为告知技术人员。
- 运行任务

> **Note**
>
> 要使 Fleet Hub 对连接状态数据编制索引，您的事物必须连接到 AWS IoT Core（客户端 ID 等于事物名称）。

Fleet Hub for AWS IoT Device Management 的工作原理

管理员可以使用 Fleet Hub for AWS IoT Device Management 在几分钟内创建安全的 Web 应用程序，而无需预置任何资源或编写任何代码。您通过使用 Fleet Hub 创建的 Web 应用程序与现有身份系统（如 Active Directory）集成。这样，您的管理员就可以应用自己的身份验证和授权模型。

Fleet Hub Web 应用程序与 AWS IoT Core 机群索引和设备监控集成。这些集成使您能够监控设备运行状况数据，并在您机群中的设备达到指定状态时创建告警。

Fleet Hub 应用程序使用 `AWSIoTFleetHubFederationAccess` 托管策略。有关更多信息，请参阅???。

使用案例示例：

- 可视化设备连接问题 — 您可以查看机群中断开连接的设备数量、设备的上次连接状态以及设备断开连接的原因。
- 设置告警 — 您可以设置阈值以在特定数量的设备断开连接时触发告警。当设备因特定原因断开连接时，告警也会通知您。然后，您可以查看详细的设备数据以进行调查和排除故障。
- 运行任务 - 您可以在一台或多台设备上运行远程操作（如固件更新）。

Fleet Hub 数据索引的工作原理

您可以使用 Fleet Hub 控制台为您的设备机群集激活机群索引。当您在 Fleet Hub 中激活机群索引时，您将为整个机群激活该索引，并使其对所有 Fleet Hub 应用程序都可用。

启用后，机群索引将自动索引所有由 AWS IoT Core 管理的字段。您还可以使用机群索引来添加自定义数据，您可以使用这些数据在 Fleet Hub 应用程序中查询和聚合数据。

Fleet Hub 告警的工作原理

Freet Hub Web 应用程序提供了一个允许用户创建告警的界面。以下步骤演示用户如何在 Fleet Hub 创建告警。

1. 创建查询以聚合数据 — 指定一个查询，该查询通过使用可搜索字段聚合用户要定位的设备。
2. 配置阈值 — 设置一个阈值，当达到索引数据中的条件（例如指定时间间隔内的连接状态）时触发告警。
3. 配置通知 — 指定一组收件人，当指定设备处于告警状态时，Fleet Hub 会通知这些收件人。

Fleet Hub 任务的工作原理

您可以使用 Fleet Hub 控制台在设备上运行远程操作。

启用任务模板后，您可以使用 Fleet Hub 应用程序中的模板创建特定任务。

适用于管理员的 Fleet Hub AWS IoT 设备管理

本节包含管理员如何创建和管理 Fleet Hub AWS IoT 设备管理 Web 应用程序的指南。

主题

开始使用

本节介绍如何为 AWS IoT 设备管理 Web 应用程序创建和设置 Fleet Hub。

主题

创建您的首个 Fleet Hub 应用程序

先决条件

以下列表包含创建 Fleet Hub Web 应用程序所需的资源。

- AWS 账户。
- 为您的账户启用的 AWS IAM Identity Center。（如果您尚未激活此服务，AWS IoT Core 控制台 (https://console.aws.amazon.com/iot/) 会提示您这样做。）

创建您的首个 Fleet Hub Web 应用程序

以下步骤介绍如何为 AWS IoT 设备管理 Web 应用程序创建 Fleet Hub。

1. 导航到 AWS IoT Core 控制台 (https://console.aws.amazon.com/iot/)，然后在左侧面板中选择 Fleet Hub，然后选择 “应用程序”。

2. 在应用程序页面上，选择 Create application（创建应用程序）。
3. 在设置 IAM 身份中心页面上，如果您尚未激活 AWS IAM Identity Center （IAM 身份中心），请按照步骤将其激活。 AWS Organizations 将向您发送电子邮件。选择电子邮件中的链接即可激活 IAM Identity Center。

> **Note**
>
> 您可以将自己的身份提供商连接到 IAM Identity Center。有关更多信息，请参阅什么是 AWS IAM Identity Center？ 和 Connect 连接到您的外部身份提供商。
> 在创建 Fleet Hub 应用程序时，如果您还没有 IAM Identity Center 的组织实例，则必须创建。您创建的 Fleet Hub 应用程序还必须与 IAM Identity Center 的组织实例相同 AWS 区域 。有关更多信息，请参阅启用 IAM 身份中心和 IAM 身份中心的组织实例。

该页面告诉您是否已激活了 IAM Identity Center。

选择下一步。

4. 在索引 AWS IoT 数据页面上，查看从 Fleet Hub AWS IoT 到舰队中心的数据流的工作原理部分中的信息。此页面将您链接到 AWS IoT Core 控制台中的页面，您可以在其中激活和管理 AWS IoT Core 队列索引。您可利用这一服务对注册表数据、影子数据和设备连接数据（设备生命周期事件）建立索引、搜索和聚合。除了默认为 AWS IoT Core 队列编制索引的托管字段外，您还可以创建自定义字段。

   - 如果您已激活机群索引，此页将显示您的机群索引设置以及自定义字段。
   - 如果您尚未启用事物索引和事物连接，则必须这样做才能使用 Fleet Hub。

   管理和查看机群索引设置后，选择 Next（下一步）。

   有关如何为 Fleet Hub 应用程序激活机群索引的更多信息，请参阅管理 Fleet Hub 应用程序的机群索引。
5. 在 Configure application（配置应用程序）页面上，在 Application role（应用程序角色）部分中，创建一个新的服务角色或选择一个现有服务角色。您的 Fleet Hub Web 应用程序在使用 Fleet Hub 资源时担任此角色。联合身份用户在使用 Web 应用程序时具有与角色相同的权限。

   - 如果创建新角色，则角色名称必须以以下字符串开头：`AWSIotFleetHub_`*`random_string`*。

- 如果选择现有角色，请确保该角色具有此策略文档中的权限。要查看您的 Fleet Hub Web 应用程序所需的权限，请选择 View role details（查看角色详细信息）。此时将打开一个窗口，其中显示服务应用于您从此页创建的任何新角色的策略文档。

6. 在 Configure application（配置应用程序）页面上，在 Application properties（应用程序属性）部分中，输入应用程序的名称。（可选）您还可以输入应用程序说明。

   选择 Create application（创建应用程序）。

7. 在 Applications（应用程序）选项卡上，选择您创建的应用程序，然后选择 View details（查看详细信息）。查看应用程序详细信息。

> **Note**
>
> 有关以 Fleet Hub 管理员身份解决问题的可能解决方案的更多信息，请参阅故障排除。

管理 Fleet Hub 应用程序的机群索引

您可以使用 AWS IoT Core 控制台或激活队列索引并将以下数据源配置为索引：AWS IoT 注册表数据、Dev AWS IoT ice Shadow 数据、AWS IoT 连接数据和AWS IoT Device Defender 违规数据。AWS CLI 以下步骤介绍如何在 AWS IoT Core 控制台中为 AWS IoT 设备管理应用程序的 Fleet Hub 激活队列索引。要使用查看步骤 AWS CLI，请参阅管理事物索引。

> **Important**
>
> 2022 年 7 月 20 日是 AWS IoT 设备管理队列索引与 AWS IoT Core 命名阴影集成并 AWS IoT Device Defender 检测违规行为的正式发布版。在此 GA 版中，您可以通过指定影子名称为特定的命名影子编制索引。如果您在 2021 年 11 月 30 日至 2022 年 7 月 19 日此功能的公开预览期添加了命名影子以编制索引，我们鼓励您重新配置实例集索引设置并选择特定的影子名称，以降低索引成本并优化性能。有关如何重新配置实例集索引设置的更多信息，请参阅 Managing fleet indexing（管理实例集索引）。

1. 导航到 AWS IoT Core 控制台 (https://console.aws.amazon.com/iot/)，然后在左侧面板中选择 “设置”。

2. 在 Settings（设置）页面上，导航到 Fleet indexing（机群索引）部分，然后选择 Manage indexing（管理索引）。
3. 在管理队列索引页面的配置部分，选择事物索引和 AWS IoT 要索引的数据源。您必须激活事物索引和事物连接才能使用 Fleet Hub。
4. （可选）在 Manage fleet indexing（管理实例集索引）页面的 Custom fields for aggregation-optional（聚合的自定义字段 – 可选）部分中，除了实例集索引默认编制索引的托管字段外，还可以创建自定义字段。

   管理和查看机群索引设置后，选择 Next（下一步）。

   机群索引可能需要一点时间才能更新设置。有关如何管理机群索引的更多信息，请参阅管理机群索引服务。

向 Fleet Hub 应用程序添加用户

您的 Fleet Hub AWS IoT 设备管理 Web 应用程序在新创建时不包含任何用户。您必须先添加用户，然后您和组织的成员才能使用该应用程序。本主题中的步骤介绍了如何向应用程序添加用户。

您可以通过为您的账户设置 AWS IAM Identity Center（IAM 身份中心）来添加现有身份系统中的用户。您可以将自己的身份提供商连接到 IAM Identity Center。有关更多信息，请参阅什么是 IAM Identity Center？

1. 在 Application（应用程序）页面上，从 Fleet Hub application（Fleet Hub 应用程序）列表中选择您的 Web 应用程序。请选择查看详细信息。
2. 在应用程序详细信息页面上，选择 Add user（添加用户）。
3. 在 Add Fleet Hub users（添加 Fleet Hub 用户）窗口、从组织中选择您希望有权访问应用程序的用户。选择 Add selected users（添加选定用户）。
4. 在应用程序详细信息页面上，验证您是否看到了您在 Fleet Hub 列表中选择的用户。

与 Fleet Hub for AWS IoT Device Management 交互的 AWS 和 AWS IoT Core 服务

本主题说明 Fleet Hub for AWS IoT Device Management 中的特征如何与其它 AWS 服务交互，以为您的 Fleet Hub Web 应用程序中的功能提供支持。

下表指出了 Fleet Hub for AWS IoT Device Management 将使用什么AWS服务来实现每个特征。

能力	AWS 服务	描述
集成现有的身份系统，如活动 Active Directory。	AWS IAM Identity Center (IAM Identity Center)	您可以通过为账户设置 AWS IAM Identity Center（IAM Identity Center）从现有身份系统中添加用户。您可以将自己的身份提供商连接到 IAM Identity Center。 有关更多信息，请参阅什么是 AWS IAM Identity Center？以及工作人员身份。
使用 AWS 托管式字段、自定义字段以及编制了索引的数据来源中的任何属性创建查询。	AWS IoT 机群索引	您可利用机群索引服务为注册表数据、影子数据和设备连接数据（设备生命周期事件）建立索引、进行搜索和聚合。除了 AWS IoT 实例集索引在默认情况下编制索引的托管式字段外，您还可以创建自定义字段以进行聚合。 有关机群索引的更多信息，请参阅 Fleet 索引服务。
为查询指定的一组设备创建告警。	Amazon CloudWatch (CloudWatch)	Fleet Hub 控制面板显示 CloudWatch 指标，您可以将这些指标与可搜索字段结合使用，以创建告警阈值。例如，每当互联设备数量低于指定数量时，您可创建 CloudWatch 告警，生成 Amazon Simple Notification Service (Amazon SNS) 通知。 有关 CloudWatch 的更多信息，请参阅什么是 Amazon CloudWatch？ 有关 AWS IoT

能力	AWS 服务	描述
		Core 如何与 CloudWatch 搭配创建指标和告警的信息，请参阅使用 CloudWatch 监控 AWS IoT 告警和指标。

故障排除

本部分提供故障排除信息和可能的解决方案，以帮助您作为 Fleet Hub 管理员解决问题。

症状	解决方案
我的 Web 应用程序链接不起作用。	创建应用程序后，可能需要几个小时才能使链接正常工作。
我无法登录我的 Web 应用程序。	确保您已将至少一个用户添加到应用程序。 确保您的角色具有适当的信任关系，例如以下内容： `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` 有关如何编辑 IAM 信任关系的更多信息，请参阅编辑现有角色的信任关系。
我无法创建 Web 应用程序。	确保您尚未达到 Web 应用程序总数的限制。

症状	解决方案
我没有看到预期的自定义字段。	检查以确保您已正确设置机群索引。 有关机群索引的更多信息，请参阅 机群索引服务。

用户的 Fleet Hub for AWS IoT Device Management

本部分包含 Fleet Hub AWS IoT 设备管理 Web 应用程序的用户相关信息。有关创建 Freet Hub 应用程序并向其添加用户的信息，请参阅 适用于管理员的 Fleet Hub AWS IoT 设备管理。

主题

开始使用

本部分包含有关使用 Fleat Hub for AWS IoT Device Management Web 应用程序特征的入门信息。

主题

创建您的第一个查询

本主题将指导您完成创建简单 Fleet Hub for AWS IoT Device Management 查询的步骤。可使用搜索查询语法来指定查询。

先决条件

- 与包含设备的 AWS IoT Core 账户关联的 Fleet Hub 应用程序。
- 组织中有权使用 Fleet Hub 应用程序的账户。

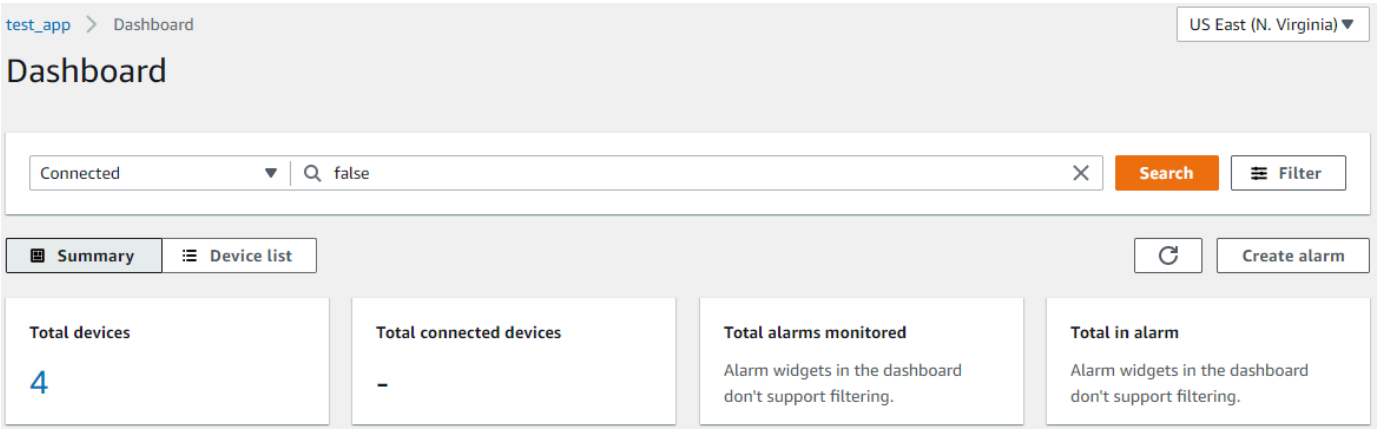
创建您的首个 Fleet Hub 查询

创建您的首个 Fleet Hub 查询

1. 导航到您的 Fleet Hub 应用程序。

   默认控制面板视图显示包含托管属性和自定义属性的所有设备的列表。包含 attributes（属性）前缀的是自定义属性。

2. 在页面顶部的菜单上，在 All fields（所有字段）中选择 Connected（已连接）。在下拉菜单旁边的文本框中输入 **`false`**。



3. 要执行搜索，请选择 Search（搜索）。您可以看到未连接到 AWS IoT Core 的所有设备的列表。

有关查询语法和示例查询的更多信息，请参阅查询语法、事物查询示例和事物组查询示例。

创建您的第一个告警

本主题将指导您完成创建简单 Fleet Hub for AWS IoT Device Management 告警的步骤。

先决条件

- 与包含设备的 AWS IoT Core 账户关联的 Fleet Hub 应用程序。
- 组织中有权使用 Fleet Hub 应用程序的账户。

创建您的第一个告警

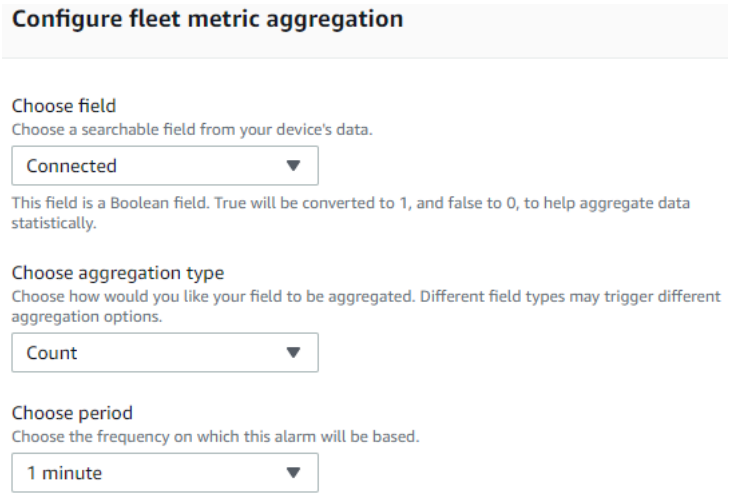
创建您的首个 Fleet Hub 告警

1. 导航到您的 Fleet Hub 应用程序。

2. 如果要针对特定的一组设备，请创建查询。有关如何创建简单查询的说明，请参阅 the section called “创建您的第一个查询”。如果您没有创建查询，您的告警将应用于机群中的所有设备。
3. 在默认的控制面板页面上，选择 Create alarm（创建告警）。
4. 在 Build aggregation metric（构建聚合指标）页面上，验证您的查询是否显示在 Target query（目标查询）中。在 Configure fleet metric aggregation（配置机群指标聚合）部分中的 Choose field（选择字段）菜单中，选择 Connected（已连接）。该AWS托管字段指示设备是否连接到了 AWS IoT Core。Choose field（选择字段）菜单包含 AWS 托管字段和管理员在 AWS IoT 机群索引服务中创建的自定义字段。
5. 对于 Choose aggregation type（选择聚合类型），请从以下选项中选择。

   - Maximum（最高）— 配置最高阈值。
   - Count（计数）— 将特定计数配置为阈值。
   - Sum（总和）— 将总和配置为阈值。
   - Minimum（最低）— 配置最低阈值。
   - Average（平均）— 配置平均阈值。
6. 对于 Choose period（选择持续时间），选择前面菜单中指定的条件持续时间，以触发告警。

   设置配置机群指标聚合的示例如下：

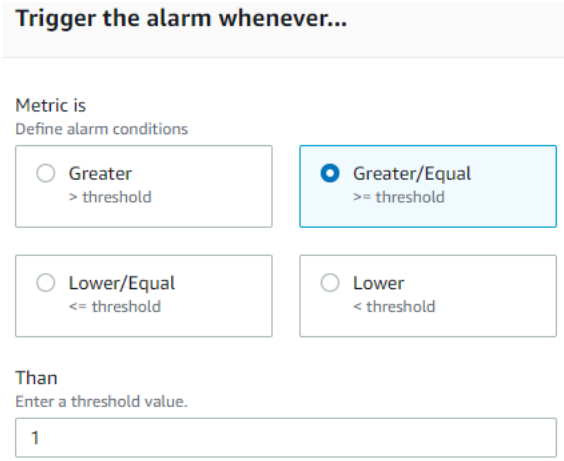
   选择 Next（下一步）。
7. 在 Set threshold（设置阈值）页面上的 Trigger the alarm whenever...（告警触发条件）部分中，选择以下选项之一。

   - Greater（大于）— 聚合指标和类型超过指定值时发出告警。
   - Greater/Equal（大于/等于）— 聚合指标和类型等于或超过指定值时发出告警。

- Lower（小于）— 聚合指标和类型小于指定值时发出告警。
- Lower/Equal（小于/等于）— 聚合指标和类型等于或小于指定值时发出告警。

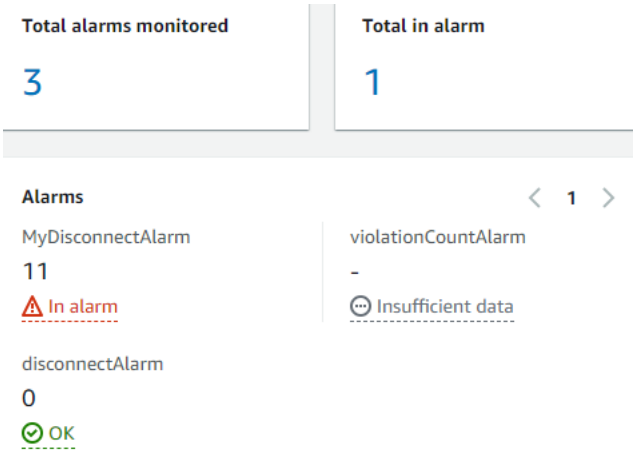
8. 在 Than（目标值）文本框中，指定用作告警阈值的值。

   设置设置阈值的示例如下：

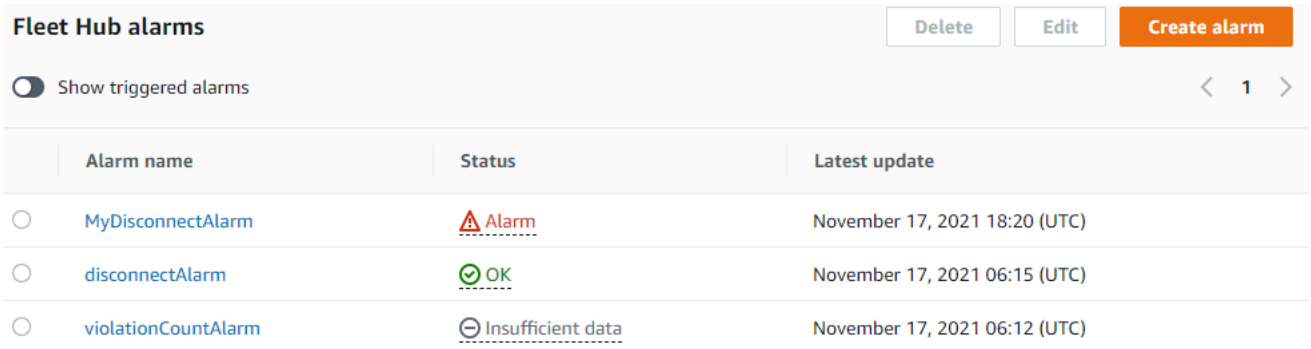


   选择 Next（下一步）。

9. 在 Notify user（通知用户）页面上，在 Notify — optional（通知 - 可选）部分中，输入电子邮件列表的名称，该列表应包含当告警被激活时组织中将接收通知的用户。输入以逗号分隔的电子邮件地址列表以填充此列表。
10. 在 Alarm details（告警详细信息）部分，输入告警的名称，并可选择是否输入告警的描述。选择 Next（下一步）。
11. 在 Review（审核）页面上，审核您在之前页面输入的信息。选择提交。返回到默认控制面板。
12. 在默认控制面板上，告警小组件会显示您创建的所有告警信息。



   要查看您创建的告警详细信息，请在左侧导航面板中选择 Fleet Hub alarms（Fleet Hub 告警）。



查看设备详细信息

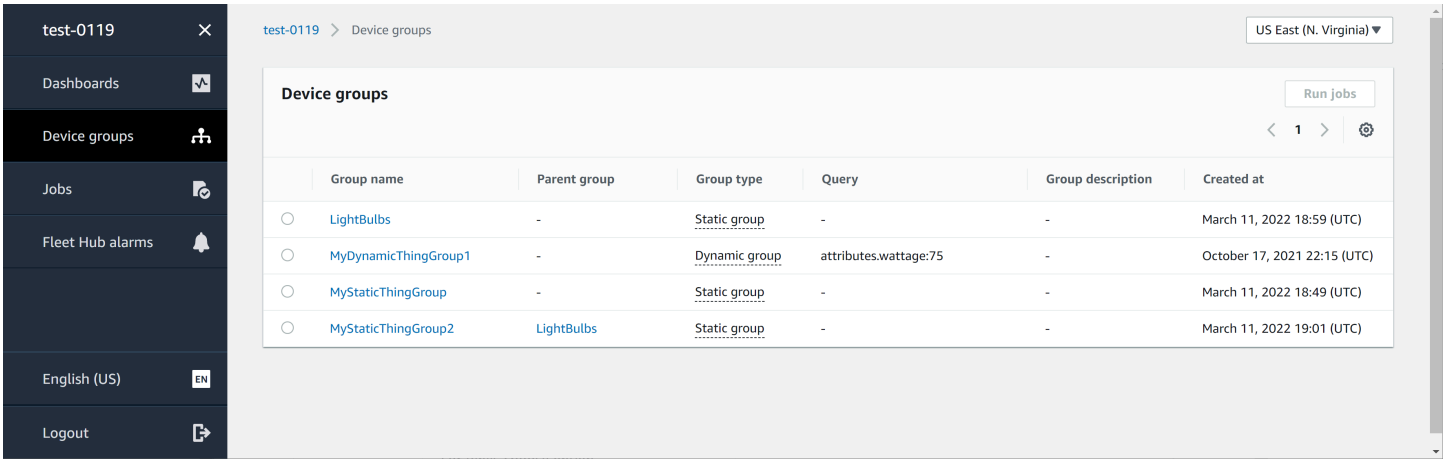
本主题将引导您完成查看有关设备组和设备的详细信息的步骤。

先决条件

- 与包含设备的 AWS IoT Core 账户关联的 Fleet Hub 应用程序。
- 组织中有权使用 Fleet Hub 应用程序的账户。

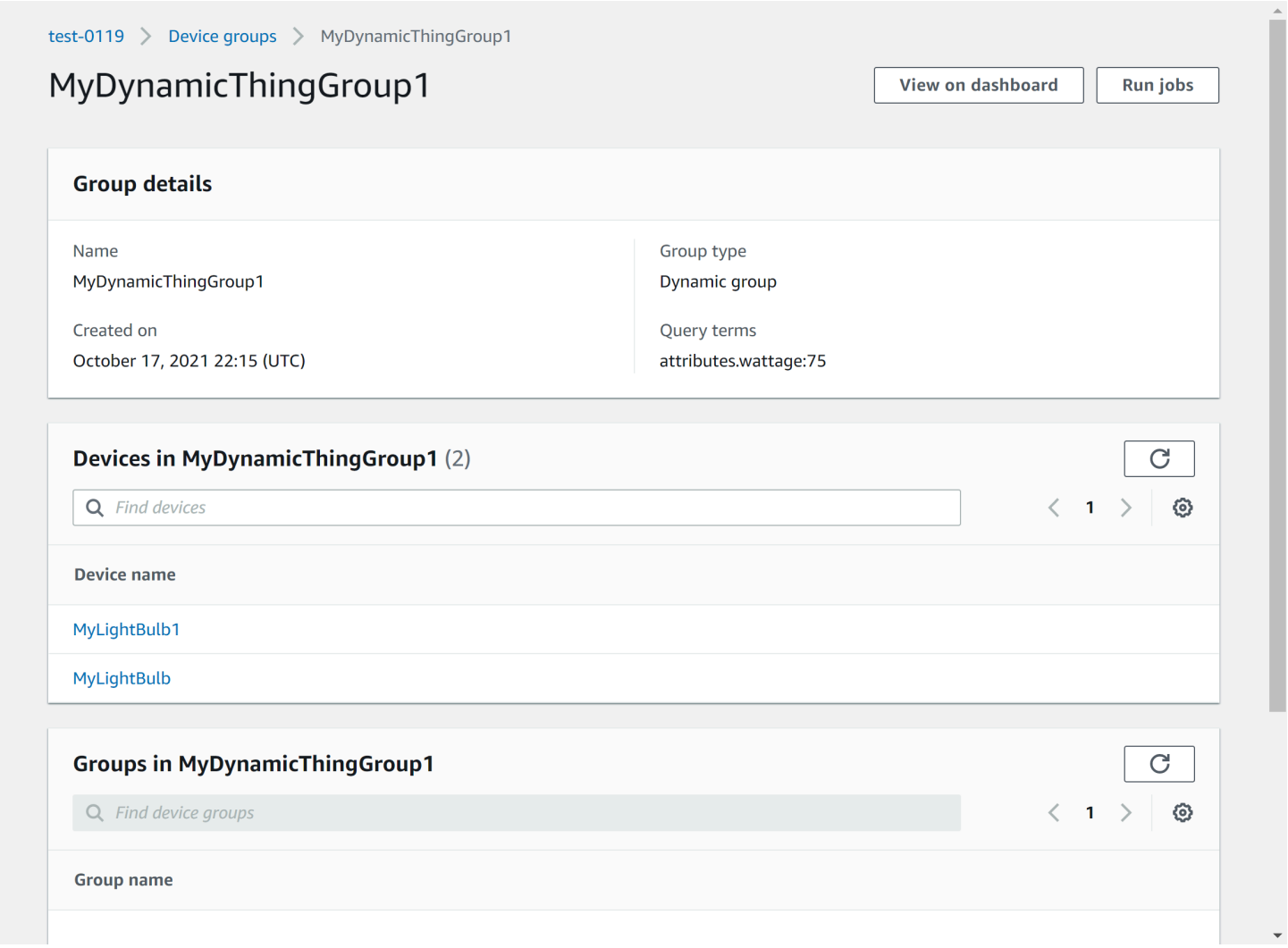
设备组

当您登录到 Fleet Hub Web 应用程序时，您会在左侧导航面板上看到 Device groups（设备组）。Device groups（设备组）页面列出了 Fleet Hub Web 应用程序中的所有设备组。要查看设备组的详细信息，请从 Device groups（设备组）列中选择特定的设备组。



设备组详细信息

Device group details（设备组详细信息）页面包含有关所选设备组的信息。要查看设备的详细信息，请从 Devices in ***XXX***（XXX 中的设备）部分的 Device name（设备名称）列中选择特定的设备。



设备详细信息

Device details（设备详细信息）页面包含有关所选设备的信息。

> **Note**
>
> 如果客户端在连接到 AWS IoT 时使用的客户端 ID 与事物名称不同，则实例集索引不会为您的“事物”的连接状态编制索引。

详细信息

Details（详细信息）部分包含以下有关您的设备的信息：

- Device name（设备名称）– 表示设备的事物资源的名称。有关更多信息，请参阅如何使用注册表管理事物。

- Thing type（事物类型）– 与您的设备关联的事物类型。您可以使用事物类型来存储具有相同事物类型的所有事物共有的信息。有关更多信息，请参阅事物类型。

- Last connection timestamp（上次连接时间戳）– 设备上次连接到 AWS IoT 的时间戳。

- Shareable device link（可共享设备链接）– 一个可共享的链接，指向所选设备的 Device details（设备详细信息）页面。

- Last connection status（上次连接状态）– 设备到 AWS IoT 的连接状态。如果您的设备已连接，则值为 *true*。如果未连接，则值为 *false*。

- Disconnect reason（断开连接原因）– 设备断开连接的原因。

报告的数据

Reported data（报告的数据）部分包含有关设备的注册表数据、设备影子数据和事物组的信息。

- Device fields（设备字段）– AWS IoT 机群索引中设备的索引字段。更多信息，请参阅管理机群索引。

- Device shadows（设备影子）– 与您的设备关联的影子。设备影子可以包含经典未命名影子和命名影子。有关更多信息，请参阅 AWS IoT 设备影子。

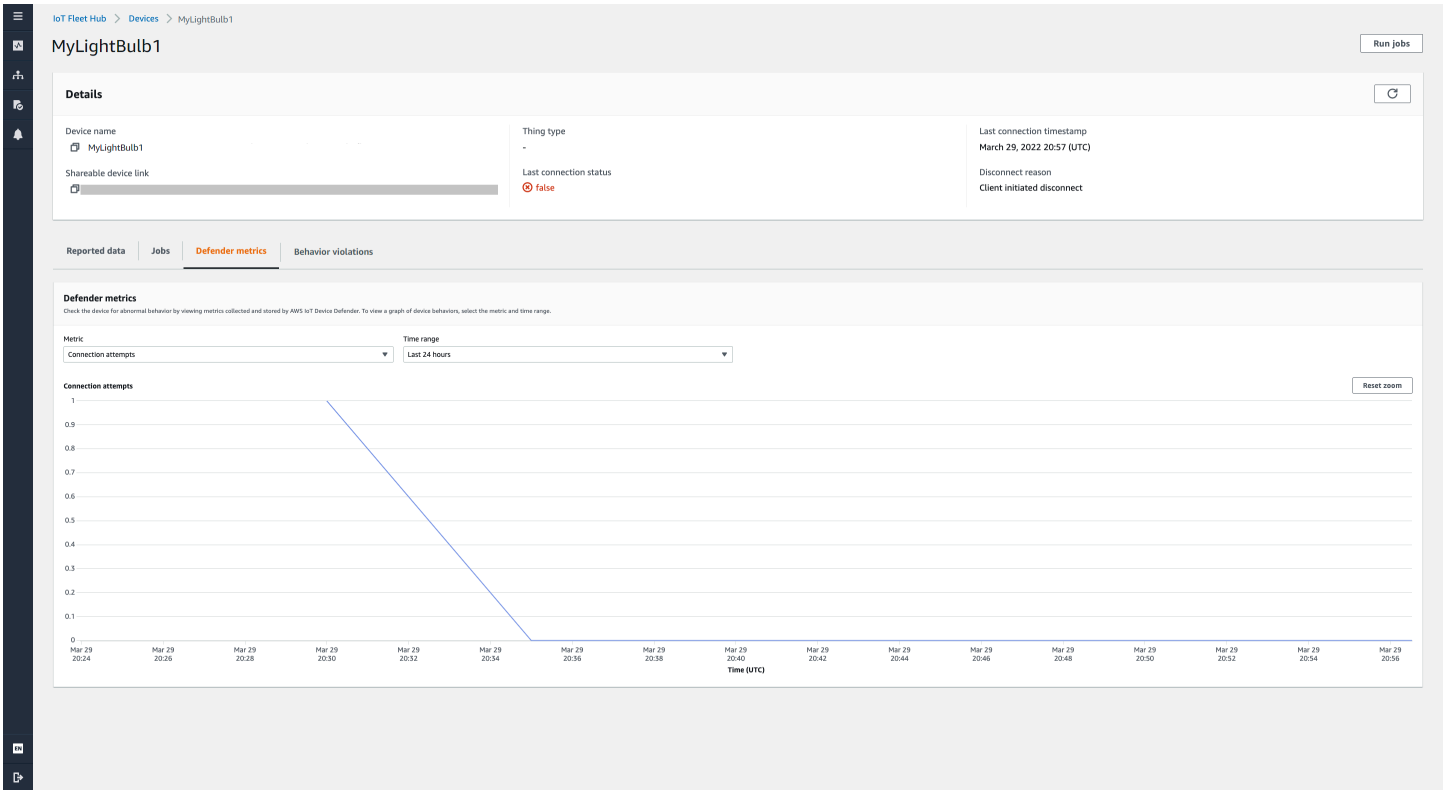
- Device groups（设备组）– 与您的设备关联的设备组。设备组可以包括静态事物组和动态事物组。有关更多信息，请参阅静态事物组和动态事物组。

任务

Jobs（任务）部分显示设备上运行的所有任务。每个任务都有一个详细信息页面，其中显示有关任务的摘要信息，包括目标和运行时信息。有关更多信息，请参阅为 AWS IoT Device Management 在 Fleet Hub 中使用任务和任务模板和任务。

Defender 指标

Defender metrics（Defender 指标）部分显示与当前所选设备关联的 AWS IoT Device Defender 指标。您可以使用显示的指标数据在您选择的时间范围内可视化设备运行情况。要查看 Fleet Hub 应用程序中的 Defender 指标数据，您的 Fleet Hub 管理员必须首先设置与选定设备关联的 AWS IoT Device Defender 指标。有关如何创建和设置设备的 AWS IoT Device Defender 指标的更多信息，请参阅自定义指标、设备端指标和 云端指标。



行为违规

Behavior violations（行为违规）部分显示已索引的 AWS IoT Device Defender 检测到与当前所选设备关联的违规数据。行为违规数据可以包括违规计数、上次违规时间和上次违规指标值。要查看 Fleet Hub 应用程序中的行为违规数据，Fleet Hub 管理员应该在安全配置文件中设置 AWS IoT Device Defender 行为违规，并在机群索引中配置 AWS IoT Device Defender 违规。有关如何在 AWS IoT Device Defender 安全配置文件中设置行为违规的更多信息，请参阅 AWS IoT Device Defender 检测。有关如何配置 AWS IoT Device Defender 违规的更多信息，请参阅管理 Fleet Hub 应用程序的机群索引和管理事物索引。

查询和筛选条件

您可以使用 Fleet Hub for AWS IoT Device Management 查询来创建和查看设备机群中的事物列表。编制了索引的数据来源中的所有 AWS 托管式字段、自定义字段和任何属性都可用作查询筛选条件。您还可以使用 AWS IoT 实例集索引创建自定义字段来针对 the section called “告警”激活聚合。有关机群索引的更多信息，请参阅 Fleet 索引服务。

主题

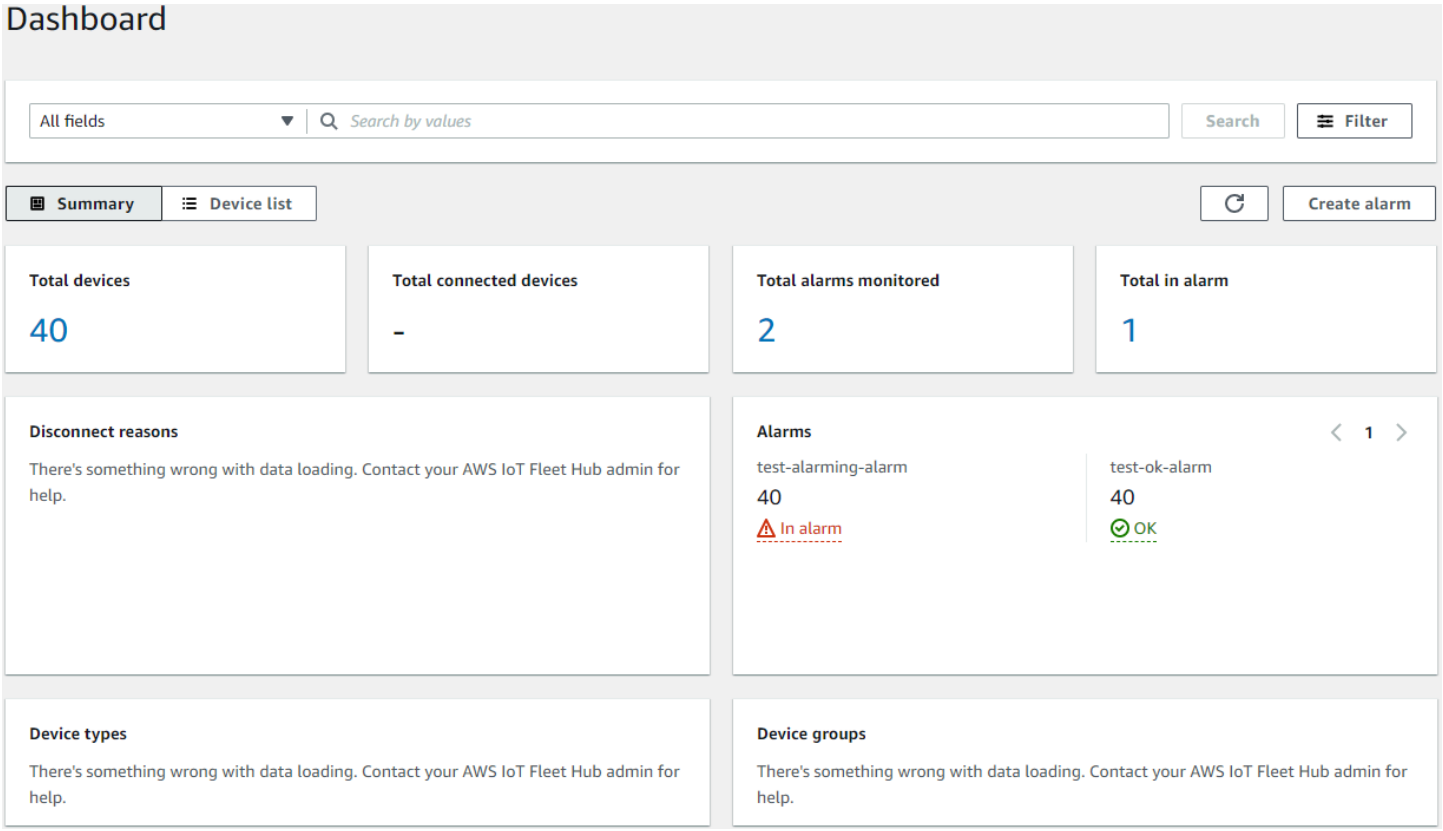
查看控制面板

当您登录 AWS IoT Device Management Web 应用程序的实例集中心时，您将看到一个控制面板，其中显示有关实例集中设备的两个数据视图。

摘要

摘要视图显示有关您机群中所有设备数据的汇总视图。其中提供以下信息。

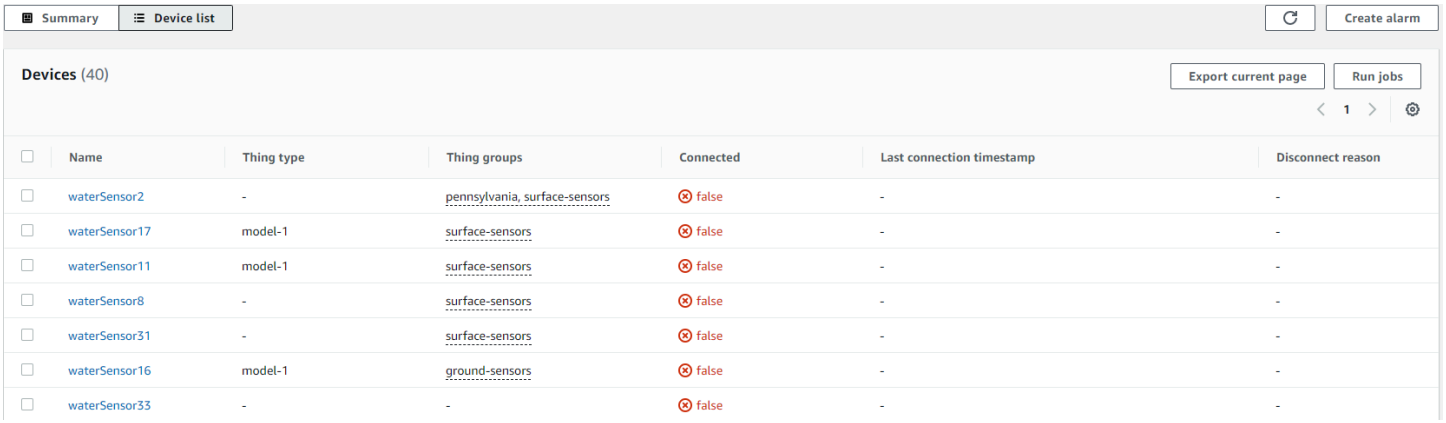
- 设备总数
- 互联设备数
- 设备断开连接的原因列表
- 您为机群创建的事物类型以及每种类型的设备数量
- 您为机群创建的事物组以及每个组中的设备数量



设备列表

设备列表视图显示一个表，列出了机群中的设备。该表为列表中的每个设备提供以下信息。

- 设备名称
- 设备的连接状态
- 设备上次连接的时间戳
- 对于未连接的设备，其断开连接的原因
- 设备的事物类型
- 设备的事物组
- 您在机群索引服务中创建的自定义字段



要下载包含页面上显示的设备的 CSV 文件，请在设备列表中选择导出当前页面。请注意，如果列表是分页的，则这仅下载当前页面上显示的数据，而不会下载后续页面上显示的数据。

您可以使用查询和筛选条件来缩小在第一个视图中生成摘要数据并显示在设备列表中的设备数量。有关使用查询和筛选条件获取有关机群中设备的更多具体信息的详细信息，请参阅 the section called “创建查询”。

使用筛选条件创建查询

本主题介绍 Fleet Hub for AWS IoT Device Management 查询的工作原理并将指导您完成使用筛选条件创建查询的所需步骤。

您可以使用查询控制控制面板摘要和列表视图上显示的设备数量和类型。您可以从 AWS IoT 实例集索引中使用 AWS 托管式字段、自定义字段以及编制了索引的数据来源中的任何属性来筛选查询。有关机群索引的更多信息，请参阅 机群索引。

您还可以将关键字添加到查询。关键字适用于所有可搜索字段。它们还会计入您可以在单个查询中应用的三个筛选条件的限制。

以下部分介绍创建典型查询所需的步骤。

创建查询

以下步骤介绍如何创建典型查询。

先决条件

- 连接到 AWS IoT Core 包含多个设备（事物）的账户的 Fleet Hub 应用程序
- 有权使用 Fleet Hub 应用程序的账户

在控制台中使用筛选条件创建您的第一个 Fleet Hub 查询

1. 导航到您的 Fleet Hub 应用程序。
2. 在默认控制面板上，验证您是否可以看到 Device list（设备列表）选项卡以及关联 AWS IoT Core 账户中的设备（事物）总数。

   默认仪表板包含导航选项卡，包括一个适用于设备列表的选项卡。它显示了关联 AWS IoT Core 账户中的设备总数以及互联设备的总数。
3. 在默认控制面板上，选择 Device list（设备列表）选项卡。验证您是否能看到包含托管属性和自定义属性的所有设备的列表。自定义属性包含 attributes（属性）前缀。

   默认情况下，设备列表控制面板显示关联 AWS IoT Core 账户中的所有设备的自定义和托管式属性。
4. 在页面顶部，输入要包含在查询中的任何关键字。关键字查询适用于所有字段。
5. 在页面顶部，选择 Filter（筛选条件）。
6. 在 Filter（筛选条件）模态，在 Field（字段）中，选择要用作筛选条件的字段。在 Operator（运算符）项下，选择一个选项。最后，对于 Value（值），选择要在筛选条件中使用的字段值。

   您最多可以添加三个筛选条件。关键字查询将计入此数量。
7. 要执行查询，请选择 Apply filters（应用筛选条件）。结果将显示与查询匹配的所有设备。

使用 Fleet Hub for AWS IoT Device Management 中的任务和任务模板

> **Note**
>
> 任务模板功能为预览版，可能会发生变化。

任务是被发送到一台或多台连接到 AWS IoT 的设备并在这些设备上运行的远程操作。例如，您可以定义一个任务，该任务指示一组设备下载并安装应用程序或固件更新、重启、轮换证书或执行远程故障排除操作。您可以从 Fleet Hub for AWS IoT Device Management Web 应用程序中运行预配置的任务。组织的管理员在 AWS IoT 控制台中创建任务模板并附加使策略以便模板可供 Fleet Hub 用户使用。在 Fleet Hub 应用程序中，您可以指定运行任务的设备或设备组。

管理员还创建设备组，可供您在应用程序中查看。要查看这些组，请在导航窗格中选择 Device groups（设备组）。将设备组指定为目标时，可以指定以下两种类型的选项之一，从而指定任务的运行方式。

- 快照：任务运行一次。
- 持续性：首次运行后，任务还将在添加到组中的任何设备上运行。

有关创建和管理任务模板的更多信息，请参阅任务模板。有关任务如何工作的更多信息，请参阅任务。

运行任务

您可以从 Fleet Hub 应用程序中的多个位置运行任务，但以下步骤始终保持相同。

1. 选择一个组或一个或多个设备作为目标。
2. 选择 Run job（运行任务）。
3. 在 Job target selection（任务目标选择）中，选择 continous（持续性）或者 snapshot（快照）。
4. 选择一个任务模板。确认 Job summary（任务摘要）下的文本描述了要运行的任务类型。
5. （可选）输入任务的名称。
6. 选择 运行。

您可以在 Fleet Hub 应用程序中以下位置选择目标并按照以下步骤操作。

- 控制面板上的设备列表选项卡。
- 特定设备的详细信息页面。
- 设备组页面。
- 特定设备组的详细信息页面。

查看和管理任务

您可以在以下位置查看机群中正在运行的任务。

- 任务列表页面 — 此页显示机群中运行的所有任务。要查看此页面，请在导航窗格中选择 Jobs（任务）导航窗格中。
- 特定设备的详细信息页面 — 此页显示设备上运行的所有任务。

每个任务都有一个详细信息页面，其中显示有关任务的摘要信息，包括目标和运行时信息。此页显示每台设备上任务的运行时状态。此外还会显示以下总计数目。

- 运行的数量。
- 已取消的运行数量。
- 成功的运行数量。
- 失败的运行数量。
- 拒绝的运行数量。
- 排队的运行数量。
- 正在运行的数量。
- 已删除的运行数量。
- 超时的运行数量。

要取消任务，请选择该任务，然后选择 Cancel（取消）。

告警

本部分介绍了 Fleet Hub for AWS IoT Device Management 告警的工作原理及其如何引导您完成创建告警所需的步骤。

当您创建 Fleet Hub 告警时，它将应用于当前显示在控制面板中的所有设备。如果您未应用任何查询，则告警将应用于机群中的所有设备。有关使用控制面板和创建查询的信息，请参阅 the section called “查询和筛选条件”。

告警使用 Amazon CloudWatch (CloudWatch) 指标与 AWS IoT 机群索引服务里的可搜索字段搭配来创建 CloudWatch 告警。例如，您可创建在机群中的设备平均电池电量低于 50% 时生成 Amazon Simple Notification Service (Amazon SNS) 消息的告警。

Fleet Hub 告警使用机群索引服务中的 GetStatistics 和 GetPercentiles 功能来查询聚合数据。例如，当您创建跟踪自定义数值字段的告警时，您可以创建应用于指定属性的以下值的告警阈值。

- 最高
- 计数
- 总计
- 最低

- 平均值
- 第 10、第 50、第 90、第 95 或第 99 位百分数中的值

有关在机群索引服务中查询聚合数据的更多信息，请参阅查询聚合数据。

下表列出了可用于AWS托管和自定义字段的聚合类型示例。

Field	Aggregation type（聚合类型）
事物类型（AWS托管字符串字段）	计数
事物组（AWS托管字符串字段）	计数
已连接（AWS托管的布尔字段） `true` 的值为 1。`false` 的值为 0。	• 最高 • 计数 • 总计 • 最低 • 平均值
shadow.reported.batterylevel（在机群索引服务中创建的数值聚合字段）	• 最高 • 计数 • 总计 • 最低 • 平均值 • p10 (10th percentile) • p50 (50th percentile) • p90 (90th percentile) • p95 (95th percentile) • p99 (99th percentile)

除了指定聚合字段和类型之外，还可以指定以下值。

- 指定的告警阈值触发告警所需的持续时间（1 分钟或 5 分钟）。
- 要应用于指定的聚合字段和类型的以下比较运算符之一。

- 大于
- 大于/等于
- 小于
- 小于/等于

- 要与指定的比较运算符一起使用的值。
- 您的组织中每当您的告警被触发时接收 Amazon SNS 消息的人员的电子邮件地址列表。
- 告警名称。

要创建 Fleet Hub 告警，请参阅 the section called “创建警报”。

创建警报

本主题将引导您完成创建 Fleet Hub for AWS IoT Device Management 告警所需的步骤。它假定您的管理员已从名为 shadow.reported.batterylevel 的设备影子字段中创建聚合字段。此自定义字段指示设备的电池电量。您需要请管理员在 AWS IoT 机群索引服务中创建可搜索的自定义字段。

当您机群中设备的平均电池电量处于 50% 以下时，您创建的告警会在 1 分钟内向您组织的人员列表发送 Amazon Simple Notification Service (Amazon SNS) 消息。

创建 Fleet Hub 查询

1. 导航到您的 Fleet Hub 应用程序。
2. 如果要针对特定的一组设备，请创建查询。有关如何创建简单查询的说明，请参阅 the section called “使用筛选条件创建查询”。如果您没有创建查询，您的告警将应用于您机群中的所有设备。
3. 在默认的控制面板页面上，选择 Create alarm（创建告警）。
4. 在 Build aggregation metric（构建聚合指标）页面上，验证您的查询是否显示在 Target query（目标查询）中。在 Configure fleet metric aggregation（配置机群指标聚合）部分，对于 Choose field（选择字段），选择 shadow.reported.batterylevel。此菜单包含AWS托管字段和管理员在 AWS IoT机群索引服务中创建的自定义字段。
5. 对于 Choose aggregation type（选择聚合类型），选择 Average（平均）。此选项基于设备机群中的平均电池电量值告警。
6. 对于 Choose period（选择周期），请选择 1 minute（1 分钟）。当您的设备机群保持指定的告警状态一分钟时，这就将触发告警。

   选择 Next（下一步）。

7. 在 Set threshold（设置阈值）页面上，在的 Trigger the alarm whenever…（每当…时触发告警）部分，选择 Lower/Equal（小于/等于）。当平均电池电量值低于您指定的值时，就会触发告警。
8. 在 Than（目标数值）文本框中，输入 50。

   选择 Next（下一步）。
9. 在 Notify user（通知用户）页面上，在 Notify — optional（通知 - 可选）部分中，输入电子邮件列表的名称，该列表应包含当告警被激活时组织中将接收通知的用户。输入以逗号分隔的电子邮件地址列表以填充此列表。
10. 在 Alarm details（告警详细信息）部分，输入告警的名称，并可选择是否输入告警的描述。选择 Next（下一步）。
11. 在 Review（审核）页面上，审核您在之前页面输入的信息。选择提交。返回到默认控制面板。
12. 在默认控制面板上，在左侧导航窗格中，选择 Fleet Hub alarm（Fleet Hub 告警）。验证是否能看到您创建的告警。

故障排除

本部分提供故障排除信息和可能的解决方案，以帮助用户解决 Fleet Hub 的问题。

症状	解决方案
我无法为我的查询添加更多的筛选条件或术语。	请确保您没有达到四个查询术语和筛选条件的限制。
我找不到自定义指标。	要求管理员在机群索引服务中创建指标。
我的告警没有显示任何数据。	告警数据需要几分钟才能加载完成。
我需要更改我的告警针对的设备。	请前往您的控制面板并更改查询。
我在控制面板中更改区域时看到了错误。	请您的管理员确保在您选择的区域中激活了机群索引。
实例集索引未对我的“事物”的连接状态编制索引。	确保客户端在连接到 AWS IoT 时使用的客户端 ID 与事物名称相同。如果客户端在连接到 AWS IoT 时使用的 ID 与事物名称不同，则实例集索引不会对您的“事物”的连接状态编制索引。

监控 Fleet Hub for AWS IoT Device Management

监控是保持 Fleet Hub 和您的其它 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下一些监控工具来监控 Fleet Hub、在出现错误时进行报告并适时自动采取措施。

- AWS CloudTrail 捕获由您的AWS账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

主题

使用 AWS CloudTrail 记录 Fleet Hub for AWS IoT Device Management API 调用

Fleet Hub for AWS IoT Device Management 已与 AWS CloudTrail 整合。CloudTrail 服务提供用户、角色或AWS服务在 Fleet Hub 中所执行的操作记录。CloudTrail 将 Fleet Hub 的所有 API 调用作为事件捕获。捕获的调用包括来自 Fleet Hub 控制台的调用，并且包含 Fleet Hub API 操作的代码调用。

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Fleet Hub 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录） 中查看最新事件。

使用 CloudTrail 收集的信息，您可以确定向 Fleet Hub 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其它详细信息。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 Fleet Hub 信息

在您创建 AWS CloudTrail 账户时，即针对该账户启用了 AWS。当 Fleet Hub 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其它 AWS 服务事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录AWS账户中的事件（包括 Fleet Hub 的事件），请创建跟踪记录。跟踪记录让 CloudTrail 可以将日志文件发送至 Amazon Simple Storage Service (Amazon S3) 存储桶。预设情况下，在控制

台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。

您还可以配置其它 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取措施。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件
- 从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 Fleet Hub 操作。它们记录在 AWS IoT API 引用中。例如，对 `CreateApplication` 和 `UpdateApplication` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management 用户凭证发出的
- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其它 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Fleet Hub for AWS IoT Device Management 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。

CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。

CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

Example

以下 CloudTrail 日志条目显示有关 `CreateApplication` 操作的信息。

```
{
    "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 中用于 AWS IoT 设备管理的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Fleet Hub 的合规计划，请参阅AWS 按合规计划划分的范围内AWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Fleet Hub 进行 AWS IoT 设备管理时如何应用分担责任模型。以下主题说明如何配置 Fleet Hub 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Fleet Hub 资源。

主题

- Fleet Hub 中的数据保护
- 适用于 Identity and Access Managem Fleet Hub for AWS IoT Device Management
- 用于 AWS IoT 设备管理的 Fleet Hub 的合规性验证
- Fleet Hub 中用于 AWS IoT 设备管理的弹性
- AWS 用于 AWS IoT 设备管理的 Fleet Hub 的托管策略
- Fleet Hub 中用于 AWS IoT 设备管理的基础设施安全
- 防止跨服务混淆代理

Fleet Hub 中的数据保护

AWS 分担责任模式适用于 AWS IoT 设备管理的 Fleet Hub 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API 或 AWS SDK 与 Fleet Hub 或其他人合作时。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

Fleet Hub 可通过服务器端加密保护静态数据。有关更多信息，请参阅 AWS IoT 开发人员指南中的AWS IoT中的数据加密。

传输中加密

在流的云部署中，Fleet Hub 使用传输层安全性 (TLS) 协议保护传输中的数据。有关更多信息，请参阅 AWS IoT 开发人员指南中的 AWS IoT的传输安全。

适用于 Identity and Access Managem Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用 Fleet Hub 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Fleet Hub 中所做的工作。

服务用户 - 如果您使用 Fleet Hub 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Fleet Hub 特征来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Fleet Hub 中的一项特征，请参阅 对 Fleet Hub for AWS IoT Device Management 身份和访问进行故障排除。

服务管理员 - 如果您在公司负责管理 Fleet Hub 资源，则您可能具有 Fleet Hub 的完全访问权限。您有责任确定您的服务用户应访问哪些 Fleet Hub 特征和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Fleet Hub 搭配使用的更多信息，请参阅 如何 Fleet Hub for AWS IoT Device Management 与 IAM 配合使用。

IAM 管理员 - 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Fleet Hub 的访问的详细信息。要查看您可在 IAM 中使用的 Fleet Hub 基于身份的策略示例，请参阅 基于身份的策略示例 Fleet Hub for AWS IoT Device Management。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅 IA M 用户指南中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的

策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Fleet Hub for AWS IoT Device Management 与 IAM 配合使用

在使用 IAM 管理对 Fleet Hub 的访问之前，请了解哪些 IAM 特征可与 Fleet Hub 协同工作。

您可以搭配使用的 IAM 功能 Fleet Hub for AWS IoT Device Management

IAM 功能	Fleet Hub 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	否

要全面了解 Fleet Hub 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

适用于 Fleet Hub 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解在 JSON 策略中可以使用的所有元素，请参阅 IAM 用户指南中的 IAM JSON 策略元素引用。

适用于 Fleet Hub 的基于身份的策略示例

要查看 Fleet Hub 基于身份的策略的示例，请参阅 基于身份的策略示例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 中的基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的跨账户访问 IAM 中的资源。

Fleet Hub 的策略操作

> **Note**
>
> Fleet Hub 应用程序使用 `AWSIoTFleetHubFederationAccess` 托管策略。有关更多信息，请参阅 ???。

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Fleet Hub 系统操作的列表，请参阅服务授权参考中的由 Fleet Hub for AWS IoT Device Management定义的操作。

Fleet Hub 中的策略操作在操作前使用以下前缀：

```
iotfleethub
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Fleet Hub 基于身份的策略的示例，请参阅 基于身份的策略示例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 的策略资源

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 Fleet Hub 的资源类型及其 ARN 的列表，请参阅服务授权参考中的 Fleet Hub for AWS IoT Device Management定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Fleet Hub for AWS IoT Device Management定义的操作。

要查看 Fleet Hub 基于身份的策略的示例，请参阅 基于身份的策略示例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 的策略条件密钥

支持特定于服务的策略条件键	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Fleet Hub 状态键的列表，请参阅服务授权参考中的 Fleet Hub for AWS IoT Device Management的条件键。要了解可以使用条件键的操作和资源，请参阅由定义的操作 Fleet Hub for AWS IoT Device Management。

要查看 Fleet Hub 基于身份的策略的示例，请参阅 基于身份的策略示例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 中的权限管控列表 (ACL)

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Fleet Hub 基于属性的访问控制 (ABAC)

支持 ABAC（策略中的标签）	是

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看包含设置 ABAC 步骤的教程，请参阅 IAM 用户指南中的使用基于属性的访问控制 (ABAC)。

将临时凭证用于 Fleet Hub

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Fleet Hub 的跨服务委托人权限

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Fleet Hub 的服务角色

支持服务角色	是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 Fleet Hub 功能。仅当 Fleet Hub 提供相关指导时才编辑服务角色。

Fleet Hub 的服务相关角色

支持服务相关角色	否

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

基于身份的策略示例 Fleet Hub for AWS IoT Device Management

默认情况下，用户和角色没有创建或修改 Fleet Hub 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

有关 Fleet Hub 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 Fleet Hub for AWS IoT Device Management的操作、资源和条件键。

主题

- 策略最佳实践
- 使用 Fleet Hub 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Fleet Hub 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略 或 工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件 。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 Fleet Hub 控制台

要访问 Fleet Hub for AWS IoT Device Management 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Fleet Hub 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Fleet Hub 控制台，还需要将 Fleet Hub `ConsoleAccess` 或`ReadOnly` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

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

对 Fleet Hub for AWS IoT Device Management 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Fleet Hub 和 IAM 时可能遇到的常见问题。

主题

我无权在 Fleet Hub 中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

> **Note**
>
> Fleet Hub 应用程序使用 `AWSIoTFleetHubFederationAccess` 托管策略。有关更多信息，请参阅 ???。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不具有虚构 `iotfleethub:`*`GetWidget`* 权限时，会发生以下示例错误。

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

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `iotfleethub:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Fleet Hub。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Fleet Hub 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的人访问我的 Fleet Hub 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Fleet Hub 是否支持这些特征，请参阅 如何 Fleet Hub for AWS IoT Device Management 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅 IA M 用户指南中的跨账户资源访问。

用于 AWS IoT 设备管理的 Fleet Hub 的合规性验证

作为多项合规计划的一部分，第三方审计师评估 Fleet Hub 的安全 AWS 性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。

- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Fleet Hub 中用于 AWS IoT 设备管理的弹性

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

AWS 用于 AWS IoT 设备管理的 Fleet Hub 的托管策略

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些政策涵盖常见用例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 管理型策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 管理型策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnly访问 AWS 管理策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 管理型策略。

AWS 托管策略： AWSIoTFleetHubFederationAccess

您可以将 `AWSIoTFleetHubFederationAccess` 策略附加到 IAM 身份。

此政策向用于 AWS IoT 设备管理的 Fleet Hub 联合用户授予在 Fleet Hub Web 应用程序中执行操作 AWS IoT 和其他 AWS 服务所需的权限。

有关将用户添加到 Fleet Hub Web 应用程序的更多信息，请参阅 ???。

您可以在AWS 控制台中查看此策略。

权限详细信息

该策略包含以下权限：

- `iot`-检索 AWS IoT 设备数据并执行舰队级别的操作。
- `iotfleethub`-检索 Fleet Hub 应用程序元数据。
- `cloudwatch`-检索 CloudWatch 警报和指标数据。还允许创建和删除适用于 Fleet Hub 警报的操作。
- `sns`-执行创建、读取、删除、订阅和取消订阅操作。这些操作适用于 Fleet Hub SNS 主题。

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

舰队中心对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来 Fleet Hub AWS 托管策略更新的详细信息。有关更多信息，请参阅 Fleet Hub 文档历史记录页面。

更改	描述	日期
AWSIoTFleetHubFederationAccess – 对现有策略的更新	Fleet Hub 添加了新的权限，以允许应用程序用户检索 Fleet	2022 年 4 月 22 日

更改	描述	日期
	Hub 应用程序中的 AWS IoT Device Defender 指标数据。	
AWSIoTFleetHubFederationAccess – 更新了现有策略	Fleet Hub 添加了新的权限，允许应用程序用户检索其他数据源进行索引。还添加了允许应用程序用户取消应用程序内 AWS IoT 任务执行的权限。	2021 年 11 月 15 日
AWSIoTFleetHubFederationAccess – 对现有策略的更新	Fleet Hub 为应用程序用户增加了检索事物组数据和对 AWS IoT 任务执行 CRUD 操作的新权限。	2021 年 5 月 24 日
AWSIoTFleetHubFederationAccess – 更新了现有策略	Fleet Hub 删除了对不受支持的 Fleet Hub 控制面板 API 的权限	2021 年 4 月 12 日
AWSIoTFleetHubFederationAccess：新策略	Fleet Hub 添加了一项新政策，授予 Fleet Hub 应用程序用户检索设备数据和执行 AWS IoT 操作所需的权限。	2021 年 4 月 12 日
Fleet Hub 开启跟踪变更	Fleet Hub 开始跟踪其 AWS 托管策略的变更。	2021 年 4 月 12 日

Fleet Hub 中用于 AWS IoT 设备管理的基础设施安全

作为一项托管服务，用于 AWS IoT 设备管理的 Fleet Hub 受《亚马逊网络服务：安全流程概述》白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Fleet Hub。客户端必须支持传输层安全性（TLS）1.2 或更高版本。我们建议使用 TLS 1.3。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Ephemeral Diffie-Hellman（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务)时，可能会发生跨服务模拟。可以操纵调用服务以使用其权限对另一个客户的资源进行操作，否则该服务不应有访问权限。为了防止这种情况， AWS 提供可帮助您保护所有服务的服务委托人数据的工具，这些服务委托人有权限访问账户中的资源。

要限制 Fleet Hub 为资源提供另一项服务的权限，我们建议使用 `aws:SourceArn` 和 `aws:SourceAccount` 资源策略中的全局条件上下文键。如果使用两个全局条件上下文键，在同一策略语句中使用时，`aws:SourceAccount` 值和 `aws:SourceArn` 值中的账户必须使用相同的账户 ID。

防止混淆代理问题最有效的方法是使用具有资源完整 Amazon Resource Name (ARN) 的 `aws:SourceArn` 全局条件上下文键。对于 Fleet Hub，`aws:SourceArn` 必须符合以下格式：`arn:aws:iot:`*`region`*`:`*`account-id`*`:*`。确保 *`region`* 与您的 Fleet Hub 区域匹配，*`account-id`* 与您的客户账户 ID 相匹配。

以下示例说明了如何通过使用 Fleet Hub 角色信任策略中的 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键防止混淆代理问题。要查找您的 Fleet Hub 角色 ARN，请前往 AWS IoT 控制台中的 Fleet Hub 部分，然后选择您的 Fleet Hub 应用程序以查看应用程序详情页面。

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

文档历史记录

下表介绍对 Fleet Hub 文档的更新。对于AWS Fleet Hub 的托管策略中的更改，请参阅 AWS Fleet Hub for AWS IoT Device Management。

更改	说明	日期
Fleet Hub for AWS IoT Device Management 公开发行版本	更新内容以反映预览期间对 Fleet Hub for AWS IoT Device Management 做出的改进。	2021 年 5 月 25 日
Fleet Hub for AWS IoT Device Management 的预览版	发布了 Fleet Hub for AWS IoT Device Management 用户指南的预览版。	2020 年 12 月 16 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。