Fleet Hub for AWS IoT Device 管理指南

Fleet Hub for AWS IoT Device Management

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Fleet Hub for AWS IoT Device Management: Fleet Hub for AWS IoT Device 管理指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 Fleet Hub for AWS IoT Device Management？

利用 Fleet Hub for AWS IoT Device Management (Fleet Hub)，您可建置獨立的 Web 應用程式，監控裝置機群的運作狀態。您可將這些應用程式提供給組織內的使用者，即使他們沒有 AWS 帳戶。使用 Fleet Hub 來管理常見的整個機群任務，例如調查和補救作業和安全性問題。

Fleet Hub 提供下列功能。

- 近即時監控裝置機群。
- 設定警示，通知您的技術人員異常行為的訊息。
- 執行任務

> **Note**
>
> 若要為 Fleet Hub 編製連線狀態資料索引，您的物件必須連接到 AWS IoT Core，用户端 ID 等於物件名稱。

Fleet Hub for AWS IoT Device Management 的運作方式

系統管理員可使用 Fleet Hub for AWS IoT Device Management，在幾分鐘內建立安全的 Web 應用程式，無需佈建任何資源或編寫任何程式碼。您使用 Fleet Hub 建立的 Web 應用程式會與您現有的身分識別系統 (例如 Active Directory) 進行整合。這可讓您的管理員套用其自己的驗證和授權模型。

Fleet Hub Web 應用程式與 AWS IoT Core 機群索引和裝置監控進行整合。這些整合提供監控裝置運作狀態資料並在您機群中的裝置達到指定狀態時建立警示的能力。

Fleet Hub 應用程式會使用 `AWSIoTFleetHubFederationAccess` 受管政策。如需更多詳細資訊，請參閱 ???。

範例使用案例：

- 視覺化裝置連線問題 - 您可以查看機群中，中斷連線的裝置數量、裝置的上次連線狀態，及裝置中斷連線的原因。
- 設定警示 - 您可以設定在特定數量的裝置中斷連線時觸發警報的閾值。當裝置或裝置因特定原因而中斷連線時，警示也會通知您。接著，您可以查看詳細的裝置資料，進行調查和疑難排解。
- 執行任務 - 您可在多一或多部裝置上執行遠端作業 (例如韌體更新)。

Fleet Hub 資料索引的運作方式

您可以使用 Fleet Hub 主控台來啟動裝置機群的機群索引。當您啟動 Fleet Hub 中的機群索引時，您對整個機群啟動該索引，並將其提供給所有 Fleet Hub 應用程式。

啟用時，機群索引會自動對所有的 AWS IoT Core 受管欄位編製索引。您還可使用機群索引來新增自訂資料，以用來查詢和彙總 Fleet Hub 應用程式中的資料。

Fleet Hub 警示的運作方式

Fleet Hub Web 應用程式提供一個可讓您的使用者建立警示的介面。下列步驟顯示使用者如何在 Fleet Hub 中建立警示。

1. 建立查詢以彙總資料 - 指定一個查詢，透過使用可搜索欄位彙總您的用戶想要設定目標的裝置。
2. 配置閾值 - 設定閾值，在達到索引資料中的條件 (例如指定時間間隔內的連線狀態) 時觸發警示。
3. 配置通知 - 指定一組收件人，當指定的裝置處於警示狀態時，Fleet Hub 會通知這些收件人。

Fleet Hub 任務的運作方式

您可以使用 Fleet Hub 主控台，在裝置上執行遠端作業。

啟用工作範本後，您可從您 Fleet Hub 應用程式中的範本建立特定任務。

適用於管理員 AWS IoT 裝置管理的叢集中樞

本節包含系統管理員如何為 AWS IoT 裝置管理 Web 應用程式建立和管理叢集中樞的指引。

主題

開始使用

本節說明如何為 AWS IoT 裝置管理 Web 應用程式建立和設定叢集中樞。

主題

建立您的第一個 Fleet Hub 應用程式

必要條件

下方清單包含您建立 Fleet Hub Web 應用程式所需的資源。

- AWS 帳戶。
- 在您的帳戶中開啟的 AWS IAM Identity Center。(若您尚未啟用此服務， AWS IoT Core 主控台 (https://console.aws.amazon.com/iot/) 會提示您啟用。)

建立您的第一個 Fleet Hub Web 應用程式

下列步驟說明如何為 AWS IoT 裝置管理 Web 應用程式建立叢集中樞。

1. 瀏覽至 AWS IoT Core 主控台 (https://console.aws.amazon.com/iot/)，然後在左側面板中選擇 [叢集中心]，然後選擇 [應用程式]。

2. 在 Applications (應用程式) 頁面上，選擇 Create application (建立應用程式)。
3. 在 [設定 IAM 身分中心] 頁面上，如果您尚未啟用 AWS IAM Identity Center (IAM 身分中心)，請依照步驟啟用它。 AWS 組織會傳送電子郵件給您。選擇電子郵件中的連結，完成啟用 IAM Identity Center。

> **Note**
>
> 您可將自己的身分提供者連線至 IAM Identity Center。如需詳細資訊，請參閱什麼是 AWS IAM Identity Center？ 並 Connect 至您的外部身分識別提供者。
> 建立 Fleet Hub 應用程式時，您必須建立 IAM 身分中心的組織執行個體 (如果您還沒有執行個體)。您建立的 Fleet Hub 應用程式也必須與 IAM 身分中心 AWS 區域 的組織執行個體相同。如需詳細資訊，請參閱啟用 IAM 身分中心和 IAM 身分中心的組織執行個體。

該頁面會告訴您是否啟用了 IAM Identity Center。

選擇下一步。

4. 在 [索引資 AWS IoT 料] 頁面上，檢閱資料流程如何運作 AWS IoT 至叢集中心區段中的資訊。此頁面會將您連結至主 AWS IoT Core 控台中的頁面，您可以在其中啟動和管理 AWS IoT Core 叢集索引。您可使用此服務來索引、搜尋和彙總登錄檔資料、影子資料、裝置連線資料 (裝置生命週期事件) 和裝置違規資料。您還可以創建自定義字段，除了默認情況下對其進行索引 AWS IoT Core 編制索引的託管字段。

   - 如果您已啟用機群索引，此頁面會顯示機群索引設定值及自訂欄位。
   - 如果您尚未啟用物件索引和連線，您必須啟用才能使用 Fleet Hub。

   當您完成機群索引設定的管理和檢閱時，請選擇 Next (下一步)。

   如需有關如何啟用機群索引的詳細資訊，請參閱管理 Fleet Hub 應用程式的機群索引。
5. 在 Configure application (配置應用程式) 頁面的 Application role (應用程式角色) 區段中，建立新的服務角色或選取現有的服務角色。您的 Fleet Hub Web 應用程式會在其使用 Fleet Hub 資源時擔任此角色。聯合身分使用者在使用 Web 應用程式時，具有與角色相同的權限。

   - 若您建立新角色，角色名稱必須以下列字串開頭：`AWSIotFleetHub_`*`random_string`*。

- 若您選取現有的角色，請確定其具有此政策文件中的權限。如要查看您的 Fleet Hub Web 應用程式所需的權限，請選擇 View role details (檢視角色詳細資訊)。這會開啟一個視窗，顯示該服務適用於您從此頁面建立的任何新角色的政策文件。

6. 在 Configure application (配置應用程式) 頁面的 Application properties (應用程式屬性) 區段中，輸入應用程式的名稱。或者，您也可以選擇輸入應用程式說明。

   選擇 Create application (建立應用程式)。

7. 在 Applications (應用程式) 頁面上，選擇您建立的應用程式，然後選擇 View details (檢視詳細資料)。檢閱應用程式的詳細資訊。

> **Note**
>
> 若要進一步了解如何以 Fleet Hub 的管理員身分解決問題，請參閱疑難排解。

管理 Fleet Hub 應用程式的機群索引

您可以使用 AWS IoT Core 主控台或啟動叢集索引，並 AWS CLI 將下列資料來源設定為索引：AWS IoT 登錄資料、 AWS IoT Device Shadow 資料、AWS IoT 連線資料和AWS IoT Device Defender 違規資料。下列步驟說明如何在 AWS IoT Core 主控台中針對 AWS IoT 裝置管理應用程式啟用叢集中樞的叢集索引。欲使用檢視步驟 AWS CLI，請參閱管理物件索引。

> **Important**
>
> 2022 年 7 月 20 日是 AWS IoT 裝置管理叢集索引與 AWS IoT Core 命名陰影整合並 AWS IoT Device Defender 偵測違規的正式發行版本。使用此 GA 版本，您可以透過指定影子名稱來索引特定的已命名影子。如果您在 2021 年 11 月 30 日至 2022 年 7 月 19 日期間，即在此功能的公開預覽期間新增了要編製索引的已命名影子，我們建議您重新設定機群索引設定，並選擇特定的影子名稱，以降低索引成本並最佳化效能。如需如何重新設定機群索引設定的詳細資訊，請參閱管理機群索引。

1. 瀏覽至主 AWS IoT Core 控台 (https://console.aws.amazon.com/iot/)，然後在左側面板中選擇 [設定]。

2. 在 Settings (設定) 頁面上，導覽至 Fleet indexing (機群索引) 區段，然後選擇 Manage indexing (管理索引)。
3. 在 [管理叢集索引] 頁面的 [組態] 區段中，選擇 [物件索引] 和您要 AWS IoT 索引的資料來源。必須啟用使用 Fleet Hub 的物件索引和物件連線。
4. (選用) 在 Manage fleet indexing (管理機群索引) 頁面的 Custom fields for aggregation-optional (彙總的自訂欄位 – 選用) 區段中，除了機群索引預設編製索引的受管欄位之外，還可建立自訂欄位。

   當您完成機群索引設定的管理和檢閱時，請選擇 Next (下一步)。

   機群索引可能需要一些時間才能更新設定。如需有關如何管理機群索引的詳細資訊，請參閱機群索引。

新增使用者至 Fleet Hub 應用程式

AWS IoT 裝置管理的叢集中樞 Web 應用程式在新建立時不會包含任何使用者。您必須先新增使用者，才能讓自己及組織成員使用應用程式。本主題中的步驟說明如何將使用者新增至您的應用程式。

您可以透過為帳戶設定 AWS IAM Identity Center (IAM 身分中心)，從現有的身分系統新增使用者。您可將自己的身分提供者連線至 IAM Identity Center。如需詳細資訊，請參閱什麼是 IAM Identity Center？。

1. 在 Applications (應用程式) 頁面上，從 Fleet Hub applications (Fleet Hub 應用程式) 清單中選擇您的 Web 應用程式。請選擇 View Details (檢視詳細資訊)。
2. 在應用程式詳細資訊頁面上，選擇 Add user (新增使用者)。
3. 在 Add Fleet Hub users (新增 Fleet Hub 使用者) 視窗中，從您的組織選取 您想存取應用程式的使用者。選擇 Add selected users (新增選取的使用者)。
4. 在應用程式詳細資訊頁面上，確認您看到所選取的使用者在 Fleet Hub 使用者清單中。

與 Fleet Hub for AWS IoT Device Management 互動的 AWS 和 AWS IoT Core 服務

本主題說明 Fleet Hub for AWS IoT Device Management 中的功能如何與其他 AWS 服務互動，以於您 Fleet Hub Web 應用程式中提供功能。

下表指出 Fleet Hub for AWS IoT Device Management 使用那些 AWS 服務來實作每個功能。

功能	AWS 服務	描述
整合現有的身分系統，例如 Active Directory。	AWS IAM Identity Center (IAM Identity Center)	您可設定您帳戶的 AWS IAM Identity Center (IAM Identity Center)，從現有的身分系統新增使用者。您可將自己的身分提供者連線至 IAM Identity Center。 如需詳細資訊，請參閱什麼是 AWS IAM Identity Center？和人力身分。
使用 AWS 受管欄位、自訂欄位和索引資料來源中的任何屬性來建立查詢。	AWS IoT 機群索引	使用機群索引服務，來編製索引、搜尋和彙總您的登錄資料、影子資料，及裝置連線能力資料 (裝置生命週期事件)。除了依預設，AWS IoT 機群索引對受管欄位編製索引之外，您還可建立彙總自訂欄位。 如需機群索引的詳細資訊，請參閱機群索引。
為查詢指定的一組裝置建立警示。	Amazon CloudWatch (CloudWatch)	Fleet Hub 儀表板會公開 CloudWatch 指標，您可搭配可搜尋欄位使用，建立警示性閾值。例如，每當連線的裝置數量低於指定數量時，您可以建立 CloudWatch 警示，產生 Amazon Simple Notification Service (Amazon SNS) 通知。 如需 CloudWatch 的資訊，請參閱什麼是 Amazon CloudWatch？ 如需如何 AWS IoT Core 與 CloudWatch 搭配使用，以建立指標和警示

功能	AWS 服務	描述
		的詳細資訊，請參閱使用 CloudWatch 來監控 AWS IoT 警示和指標。

故障診斷

本節提供疑難排解資訊及可能的解決方案，協助 Fleet Hub 管理者解決問題。

徵狀	解決方案
我的 Web 應用程式連結無法運作。	建立應用程式後，可能需要幾個小時才能使連結生效。
我無法登入我的 Web 應用程式。	請確保您至少已將一個使用者新增至應用程式。 請確認角色具有適當的信任關係，如下所示： `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` 如需有關如何編輯 IAM 信任關係的詳細資訊，請參閱編輯現有角色的信任關係。
我無法建立 Web 應用程式。	請確保您尚未達到 Web 應用程式總數的限制。
我沒有看到我想看到的自訂欄位。	查看確認您已正確地設定機群索引。

徵狀	解決方案
	如需機群索引的詳細資訊，請參閱機群索引。

適用於使用者的 Fleet Hub for AWS IoT Device Management

本節包含 Fleet Hub for AWS IoT Device Management Web 應用程式使用者的資訊。如需建立 Fleet Hub 應用程式及將使用者新增至其中的詳細資訊，請參閱 適用於管理員 AWS IoT 裝置管理的叢集中樞。

主題

入門

本節包含開始使用 Fleet Hub for AWS IoT Device Management Web 應用程式功能的詳細資訊。

主題

建立您的第一個查詢

本主題會逐步說明建立一個簡單的 Fleet Hub for AWS IoT Device Management 查詢步驟。查詢是使用搜尋查詢語法指定的。

先決條件

- 與包含裝置 (物件) 之 AWS IoT Core 帳戶關聯的 Fleet Hub 應用程式。
- 您組織中有權使用 Fleet Hub 應用程序的帳戶。

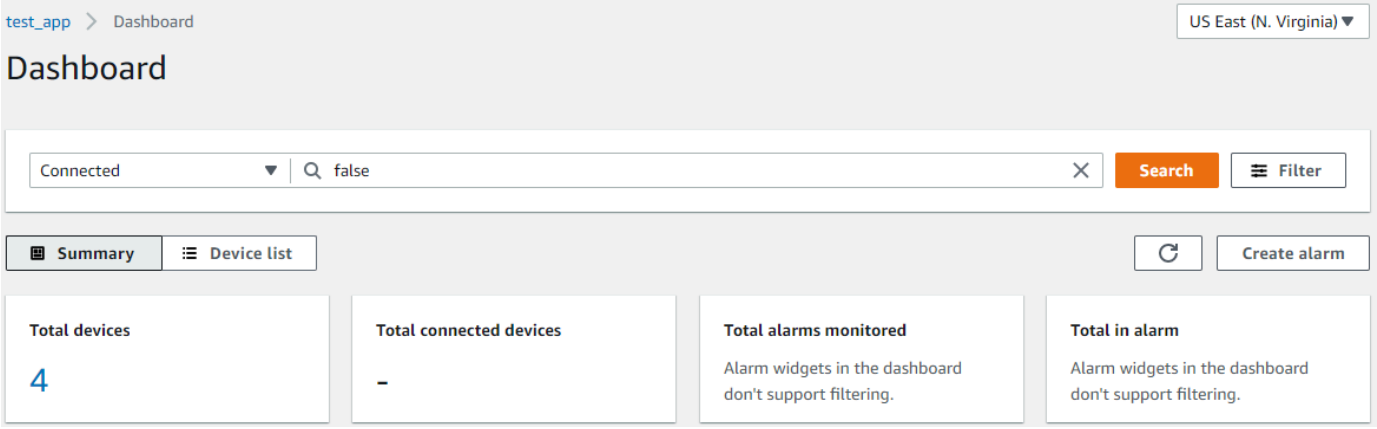
建立您的第一個 Fleet Hub 查詢

建立您的第一個 Fleet Hub 查詢

1. 瀏覽至您的 Fleet Hub 應用程式。

   預設儀表板檢視會顯示包含受管和自訂屬性的所有裝置清單。包含屬性字首的屬性是自訂屬性。

2. 在頁面頂端的選單中，從 All fields (所有欄位) 選擇 Connected (已連線)。在下拉式選單旁的文字方塊中輸入 **`false`**。



3. 如要執行搜尋，請選擇 Search (搜尋)。您會看到未連線至 AWS IoT Core 的所有裝置清單。

如需查詢語法和查詢範例的詳細資訊，請參閱查詢語法、物件查詢範例以及物件群組查詢範例。

建立您的第一個警示

本主題會逐步說明建立一個簡單的 Fleet Hub for AWS IoT Device Management 警示步驟。

先決條件

- 與包含裝置 (物件) 之 AWS IoT Core 帳戶關聯的 Fleet Hub 應用程式。
- 您組織中有權使用 Fleet Hub 應用程序的帳戶。

建立您的第一個警示

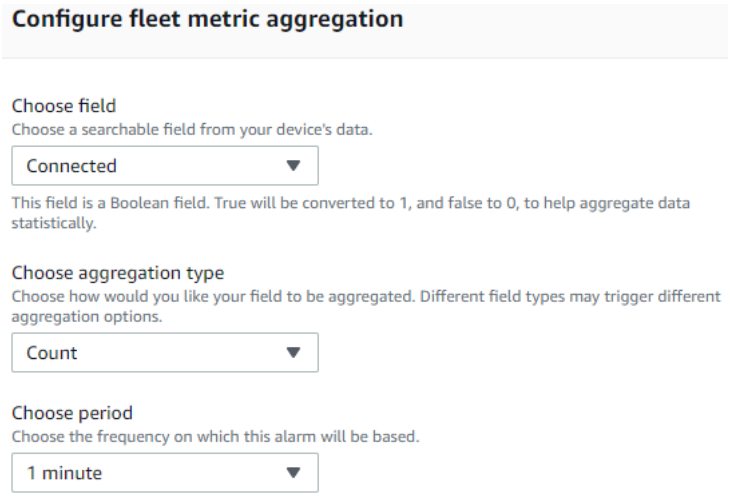
建立您的第一個 Fleet Hub 警示

1. 瀏覽至您 Fleet Hub 應用程式。

2. 若您想要鎖定特定的裝置組合，請建立查詢。如需如何建立簡單查詢的指示，請參閱 the section called “建立您的第一個查詢”。若您並未建立查詢，您的警示將會套用至您機群中的所有裝置。
3. 在預設儀表板頁面上，選擇 Create alarm (建立警示)。
4. 在 Build aggregation metric (建立彙整指標) 頁面上，請確認您於 Target query (目標查詢) 之下顯示查詢。在 Configure fleet metric aggregation (配置機群指標彙整) 區段中的Choose field (選擇欄位) 選單上，選擇 Connected (已連線)。此 AWS 受管欄位會指出裝置是否連線至 AWS IoT Core。Choose field (選擇欄位) 選單包含 AWS 受管欄位以及系統管理員在 AWS IoT 機群索引中建立的自訂欄位。
5. 若為選擇彙總類型，選擇下列其中一個選項。

   - 上限：配置一個最大閾值。
   - 計數：將特定計數配置為閾值。
   - 總和：將總和配置為閾值。
   - 下限：配置一個最小閾值。
   - 平均數：配置平均閾值。
6. 如為 Choose period (選擇期間)，選擇先前選單中指定的條件持續時間，以觸發警示。

   設定機群指標彙總的範例設定如下所示：

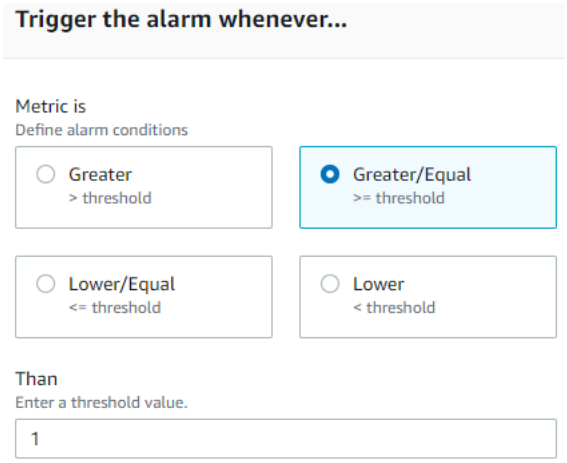
   選擇 Next (下一步)。
7. 在 Set threshold (設定閾值) 頁面的 Trigger the alarm whenever... (觸發警報...) 區段中，選擇下列其中一個選項。

   - 大於：當彙總指標和類型超過指定值時發出警示。
   - 大於/等於：當彙總指標和類型等於或超過指定值時發出警示。

- 小於：當彙總指標和類型低於指定值時發出警示。
- 小於/等於：當彙總指標和類型等於或低於指定值時發出警示。

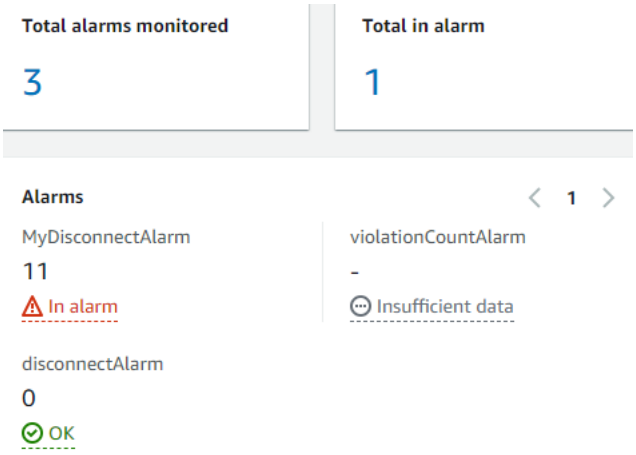
8. 在 Than (比) 文字方塊中，指定要用來作為警示閾值的值。

   設定閾值的範例設定看起來可能如下所示：

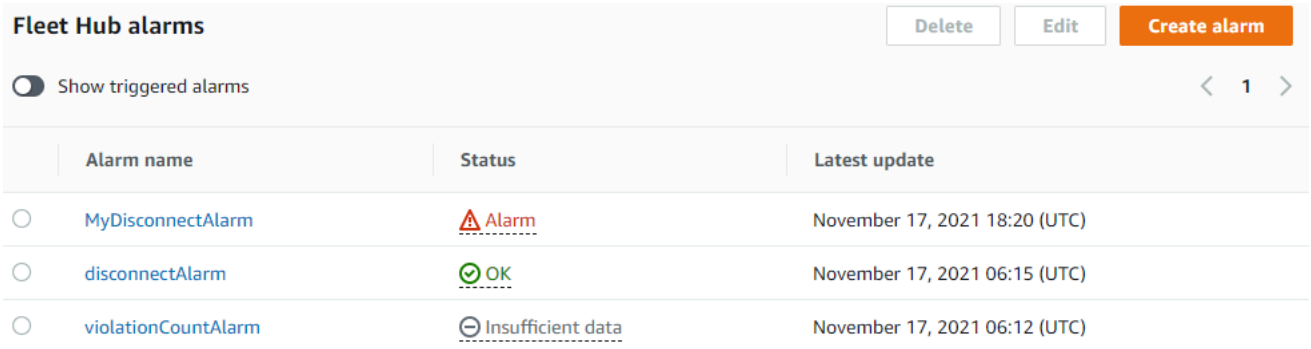


   選擇 Next (下一步)。

9. 在 Notify user (通知使用者) 頁面的 Notify – optional (通知 – 選用) 區段中，輸入電子郵件清單的名稱，其中包含您組織中在警示處於作用中狀態時收到通知的使用者。輸入電子郵件地址清單 (以逗號分隔)，填入此清單。
10. 在 Alarm details (警示詳細資料) 區段中，輸入警示的名稱，然後選擇性地輸入警示的說明。選擇 Next (下一步)。
11. 於 Review (檢閱) 頁面上，檢閱您在先前頁面上輸入的資訊。選擇 Submit (提交)。您會返回預設的儀表板。
12. 在預設儀表板上，警示小工具會顯示您建立的所有警示的資訊。



若要查看所建立警示的詳細資訊，請在左側導覽面板中選擇 Fleet Hub alarms (Fleet Hub 警示)。



檢視裝置詳細資訊

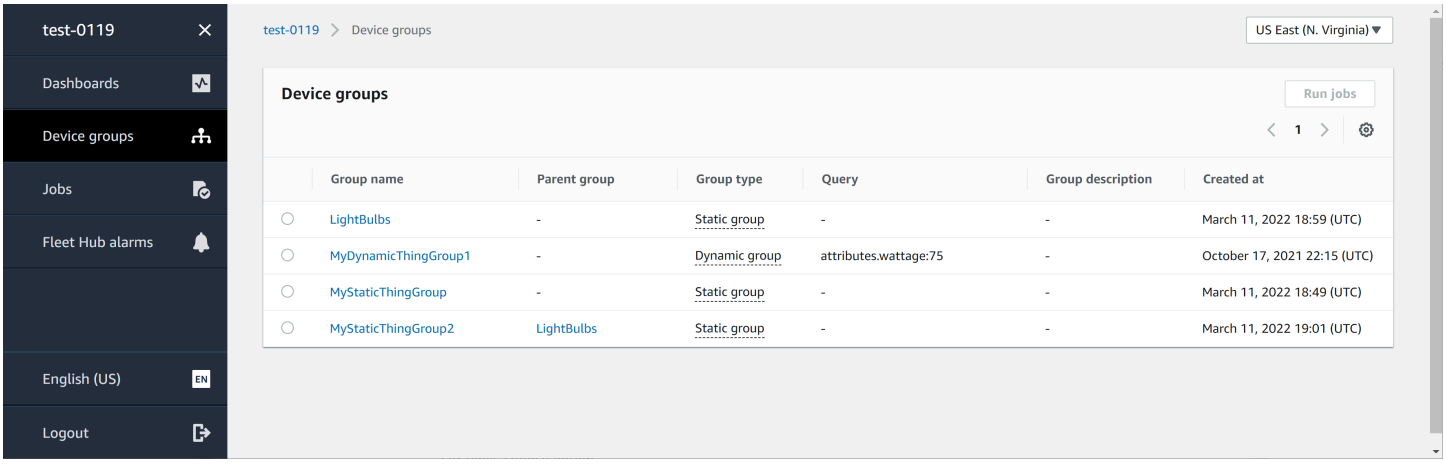
本主題將逐步說明檢視您的裝置群組和裝置詳細資訊的步驟。

先決條件

- 與包含裝置 (物件) 之 AWS IoT Core 帳戶關聯的 Fleet Hub 應用程式。
- 您組織中有權使用 Fleet Hub 應用程序的帳戶。

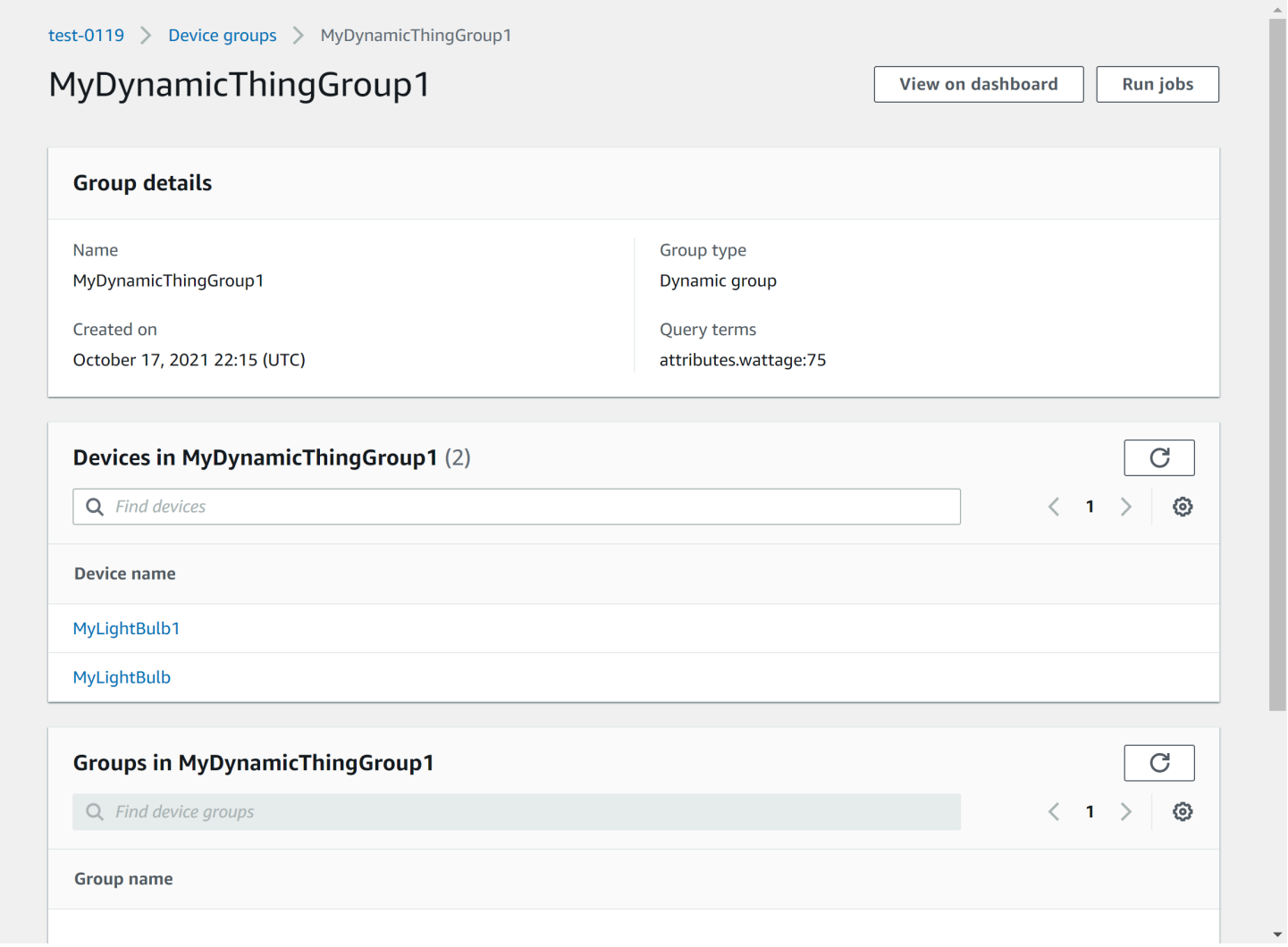
裝置群組

登入 Fleet Hub Web 應用程式時，您會看到左側導覽面板中的 Device groups (裝置群組)。Device groups (裝置群組) 頁面列出了您的 Fleet Hub Web 應用程式中的所有裝置群組。若要查看裝置群組的詳細資訊，請從 Group name (群組名稱) 欄位選擇特定裝置群組。



裝置群組詳細資訊

Device group details (裝置群組詳細資訊) 頁面包含有關所選裝置群組的資訊。若要檢視裝置的詳細資訊，請從 Devices in ***XXX*** (XXX 中的裝置) 的 Device name (裝置名稱) 欄位選擇指定的裝置。



裝置詳細資訊

Device details (裝置詳細資訊) 頁面包含有關所選裝置的資訊。

> **Note**
>
> 如果您的用戶端在連接至 AWS IoT 時使用與物件名稱不同的用戶端 ID，則「物件」的連線狀態將不會透過機群編製索引。

詳細資訊

Details (詳細資訊) 區段包含您裝置的下列資訊：

- Device name (裝置名稱)：代表裝置的物件資源名稱。如需詳細資訊，請參閱如何使用登錄檔管理物件。
- 物件類型：與您的裝置關聯的物件類型。您可以使用物件類型存放具有相同物件類型之所有物件的共通資訊。如需詳細資訊，請參閱物件類型。
- Last connection timestamp (上次連線時間戳記)：裝置上次連線到 AWS IoT 的時間戳記。
- 可共用裝置連結：指向 Device details (裝置詳細資訊) 頁面上所選裝置的可共用連結。
- Last connection status (上次連線狀態)：裝置到 AWS IoT 的連線狀態。如果您的裝置已連線，則值為 `true`。如果未連線，則值為 `false`。
- Disconnect reason (中斷連線原因)：裝置中斷連線的原因。

報告的資料

Reported data (報告的資料) 區段包含有關裝置登錄資料、裝置影子資料和物件群組的資訊。

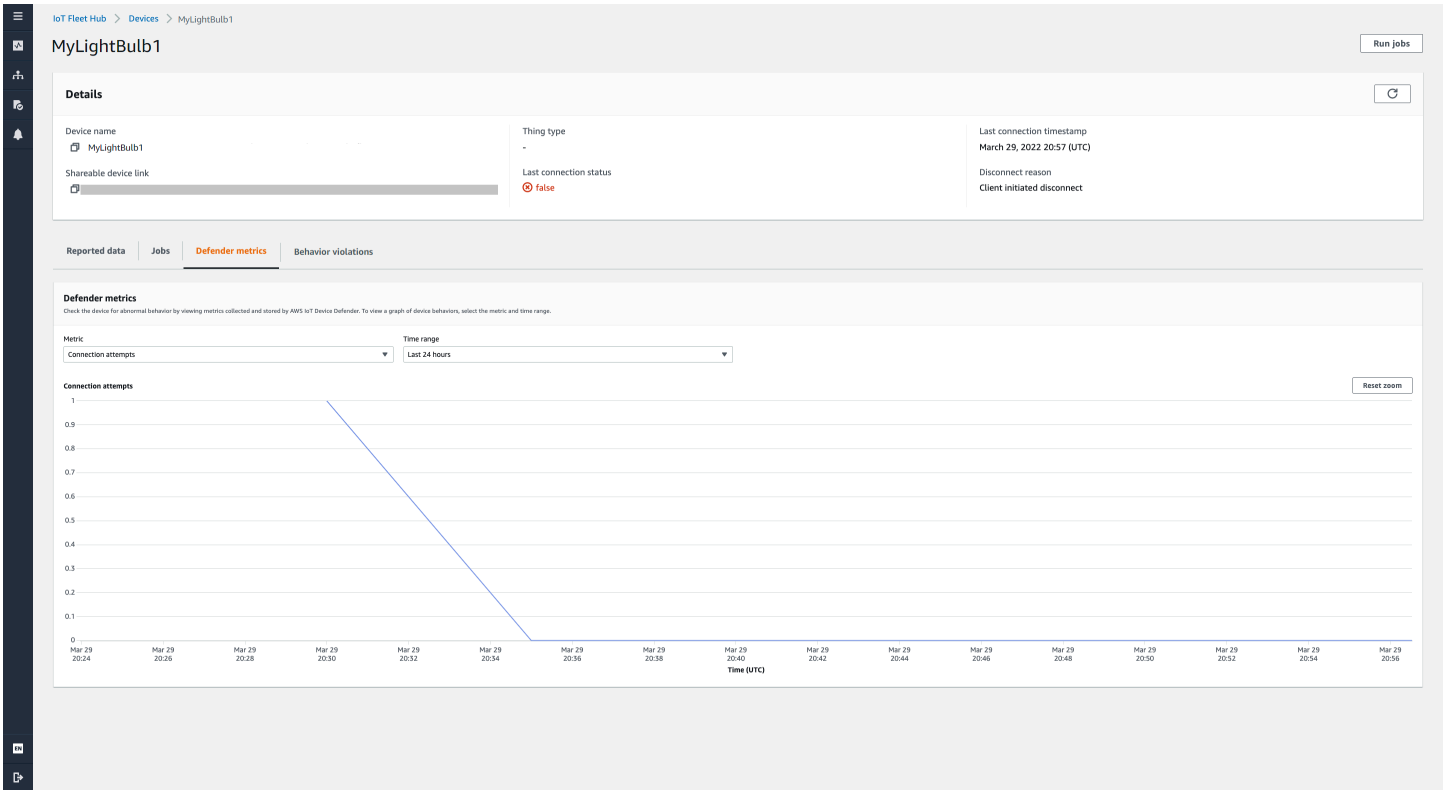
- Device fields (裝置欄位)：裝置在 AWS IoT 機群索引中的索引欄位。如需詳細資訊，請參閱管理機群索引。
- Device shadows (裝置影子)：與您的裝置關聯的影子。裝置影子可以同時包含傳統的未命名影子和已命名影子。如需詳細資訊，請參閱 AWS IoT 裝置影子。
- Device groups (裝置群組)：與您的裝置關聯的裝置群組。裝置群組可以同時包含靜態物件群組和動態物件群組。如需詳細資訊，請參閱靜態物件群組和動態物件群組。

任務

Jobs (任務) 區段會顯示裝置上執行的所有任務。每個任務都有一個詳細資訊頁面，可顯示任務的摘要資訊，包括目標和執行時間資訊。如需詳細資訊，請參閱使用 Fleet Hub for AWS IoT Device Management 中的任務和任務範本和任務。

Defender 指標

Defender metrics (Defender 指標) 區段顯示與您目前所選裝置關聯的 AWS IoT Device Defender 指標。您可以使用顯示的指標資料，將您選擇之時間範圍內的裝置操作視覺化呈現。要從 Fleet Hub 應用程式查看 Defender 指標資料，您的 Fleet Hub 管理員必須先設定與所選裝置關聯的 AWS IoT Device Defender 指標。如需更多關於如何建立和設定裝置 AWS IoT Device Defender 指標的資訊，請參閱自訂指標、裝置端指標和雲端指標。



行為違規

Behavior violations (行為違規) 區段顯示與您目前所選裝置相關聯、經過索引的AWS IoT Device Defender 偵測違規資料。行為違規資料可以包括違規計數、上次違規時間和上次違規度指標值。要從 Fleet Hub 應用程式檢視行為違規資料，您的 Fleet Hub 管理員應在安全設定檔中設定 AWS IoT Device Defender 行為違規，並在機群索引中設定 AWS IoT Device Defender 違規。如需更多關於如何在 AWS IoT Device Defender 安全設定檔中設定行為違規的資訊，請參閱 AWS IoT Device Defender

偵測。如需更多如何設定 AWS IoT Device Defender 違規的資訊，請參閱管理 Fleet Hub 應用程式的機群索引和管理物件索引。

查詢和篩選條件

您可以使用叢集中樞進行 AWS IoT 裝置管理查詢，以建立和檢視裝置叢集中的項目清單。所有 AWS 託管的欄位、自訂欄位和索引資料來源中的任何屬性都可作為查詢篩選器使用。您也可以建立自訂欄位，以使用 AWS IoT 叢集索引啟動彙總。the section called “警示”如需機群索引的詳細資訊，請參閱機群索引。

主題

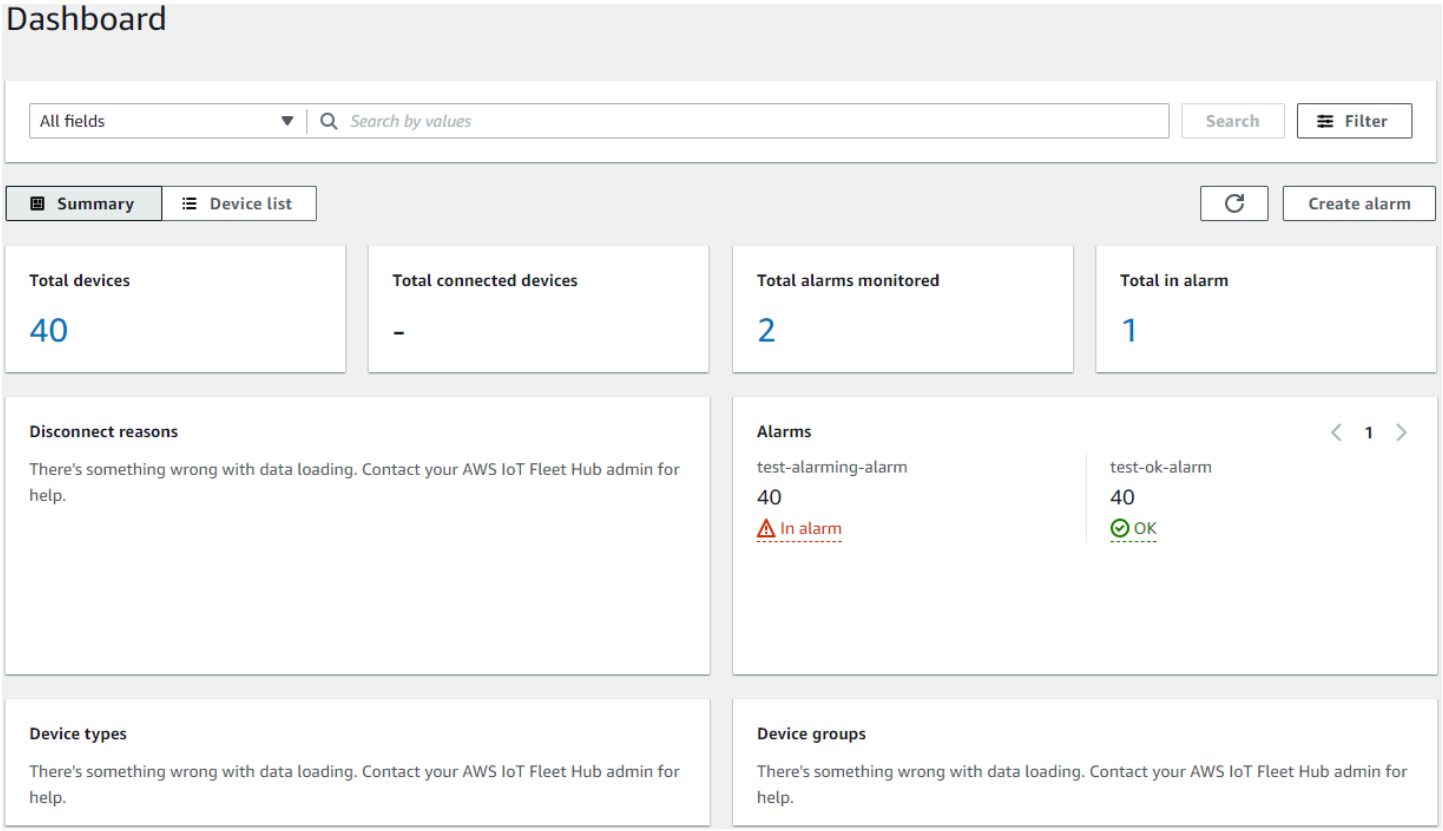
檢視儀表板

當您登入用於 AWS IoT 裝置管理的叢集中樞 Web 應用程式時，您會看到一個儀表板，其中顯示有關叢集中裝置的兩個資料檢視。

Summary

Summary (摘要) 檢視會顯示機群中所有裝置相關資料的彙總檢視。其會提供下列資訊：

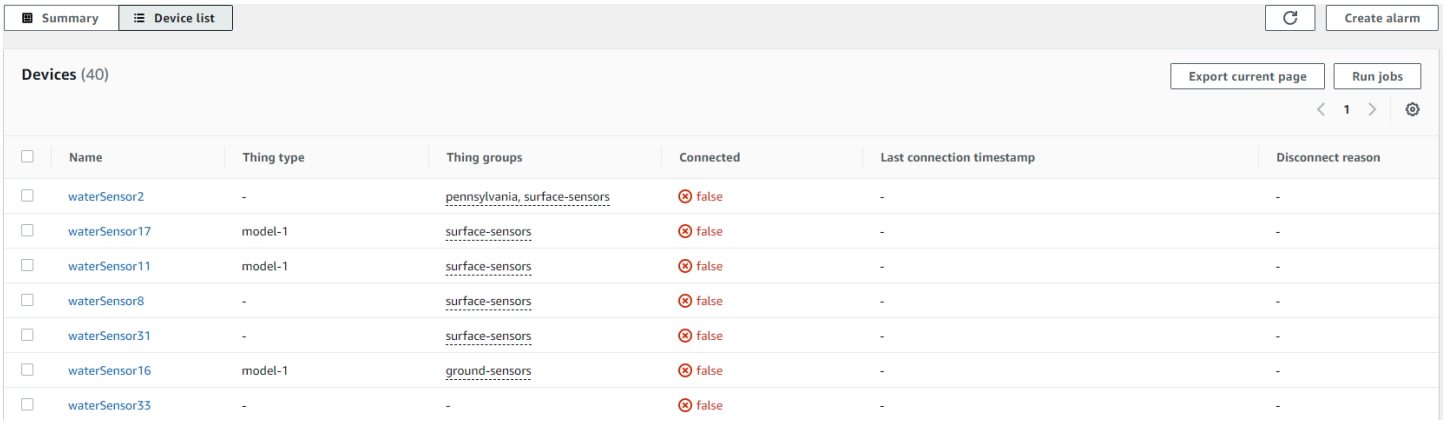
- 裝置總數量
- 連網裝置數量
- 裝置中斷連線的原因清單
- 您為機群所建立的物件類型和每個類型中的裝置數量
- 您為機群所建立的物件群組和每個群組中的裝置數量



裝置清單

Device list (裝置清單) 檢視會顯示列出機群裝置的表格。表格提供清單中每個裝置的下列資訊。

- 裝置名稱
- 裝置的連線狀態
- 裝置上次連線的時間戳記
- 裝置連線中斷的原因
- 裝置的物件類型
- 裝置的物件群組
- 您在機群索引服務中建立的自訂欄位



若要下載包含頁面上顯示之裝置的CSV檔案，請在裝置清單上選擇「匯出目前頁面」。請注意，若清單已分頁，這項動作只會下載目前頁面上顯示的資料，而不會下載後續頁面上的資料。

您可以使用查詢和篩選條件，縮小在第一個檢視中產生摘要資料並顯示於裝置清單中的裝置數目。如需使用查詢和篩選條件以取得機群中裝置的詳細資訊，請參閱 the section called “建立查詢”。

使用篩選條件建立查詢

本主題說明 AWS IoT 裝置管理查詢的叢集中心如何運作，並引導您完成使用篩選器建立查詢所需的步驟。

您可使用查詢，來控制顯示在儀表板摘要和清單檢視上的裝置數量和類型。您可以使用 AWS-managed 欄位、自訂欄位以及 AWS IoT 叢集索引中索引資料來源的任何屬性來篩選查詢。如需機群索引的詳細資訊，請參閱機群索引。

您也可將關鍵字新增至查詢。關鍵字適用於所有可搜尋的欄位。其還會計入您可在單一查詢中套用的三個篩選條件限制。

下一節說明建立典型查詢所需的步驟。

建立查詢

下列步驟說明如何建立典型查詢。

必要條件

- 綁定到包含多個設備（事物）的 AWS IoT Core 帳戶的 Fleet Hub 應用程序
- 有權使用 Fleet Hub 應用程式的帳戶

使用主控台中的篩選條件建立您第一個 Fleet Hub 查詢

1. 瀏覽至您的 Fleet Hub 應用程式。
2. 在預設儀表板上，確認您可以看到 [裝置清單] 索引標籤，以及關聯 AWS IoT Core 帳戶中裝置 (事物) 的總數。
3. 在預設儀表板上，選擇 Device list (裝置清單) 索引標籤。確認您看到包含受管理和自訂屬性的所有裝置清單。自訂屬性包含屬性字首。
4. 在頁面頂端，輸入您想要包含於查詢中的任何關鍵字。關鍵字查詢套用至所有欄位。
5. 請在頁面頂端，選擇 Filter (篩選條件)。
6. 在 Filter (篩選條件) 模式的 Field (欄位) 下，選擇您要用來作為篩選條件的欄位。在 Operator (運算子) 下，請選擇一個選項。最後，在 Value (值) 下，請選擇要用於您篩選條件中的欄位值。

   您最多可新增三個篩選條件。關鍵字查詢會計入此數字。
7. 如要執行查詢，請選擇 Apply filters (套用篩選條件)。結果會顯示符合您查詢的所有裝置。

使用 Fleet Hub for AWS IoT Device Management 中的任務和任務範本

> **Note**
>
> 任務範本功能目前為預覽狀態，可能會變更。

任務為傳送至連接至 AWS IoT 的一或多個裝置，並在其上執行的遠端作業。例如，您可以定義一個任務，指示一組裝置下載並安裝應用程式或韌體更新、重新啟動、輪換憑證，或者執行遠端故障排除操作。您可執行來自 Fleet Hub for AWS IoT Device Management Web 應用程式的預先配置任務。您組織的管理員會在 AWS IoT 主控台中建立任務範本，並連接可供 Fleet Hub 使用者使用範本的政策。在您的 Fleet Hub 應用程式中，您指定執行任務的裝置或裝置群組。

管理員還會建立您可在應用程式中檢視的裝置群組。如要查看這些群組，請選擇導覽窗格中的 Device groups (裝置群組)。當您指定裝置群組為目標時，您可為任務執行方式指定下列兩種選項之一。

- Snapshot (快照)：任務執行一次。
- Continuous (持續)：在其初次執行之後，任務會在新增至群組的任何裝置上執行。

如需建立及管理任務範本的詳細資訊，請參閱任務範本。如需任務運作方式的詳細資訊，請參閱任務。

執行任務

您可從 Fleet Hub 應用程式中的數個位置執行任務，但下列步驟始終相同。

1. 選取一個群組或一個或多個裝置作為目標。
2. 選擇 Run job (執行任務)。
3. 在 Job target selection (任務目標選項) 下，選擇 continuous (持續) 或 snapshot (快照)。
4. 選取任務範本。驗證 Job summary (任務摘要) 下的文字是否說明您想執行的任務類型。
5. 您可以選擇輸入任務的名稱。
6. 選擇 Run (執行)。

您可從 Fleet Hub 應用程式的下列位置選取目標，並遵循下列步驟。

- 儀表板上的裝置清單索引標籤。
- 特定裝置的詳細資訊頁面。
- 裝置群組頁面。
- 特定裝置群組的詳細資訊頁面。

檢視和管理任務

您可在下列位置查看機群中正在執行的任務。

- 任務清單頁面：此頁面顯示機群中執行的所有任務。如要查看此頁面，請在導覽窗格中選擇 Jobs (任務)。
- 特定裝置的詳細資訊頁面：此頁面會顯示裝置上執行的所有任務。

每個任務都有一個詳細資訊頁面，可顯示任務的摘要資訊，包括目標和執行時間資訊。此頁面會顯示每個裝置上任務的執行時間狀態。其還會顯示下列總數。

- 運行數量。
- 已取消的運行數量。
- 成功的運行數量。

- 失敗的運行數量。
- 遭拒的運行數量。
- 已排入佇列的運行數量。
- 進行中的運行數量。
- 遭移除的運行數量。
- 逾時的運行數量。

如要取消任務，請選擇 Cancel (取消)。

警示

本節說明 Fleet Hub for AWS IoT Device Management 警示如何運作，並引導您完成建立警示所需的步驟。

當您建立 Fleet Hub 警示時，其會套用至目前顯示於儀表板中的所有裝置。若您不套用任何查詢，則警示會套用至您機群中的所有裝置。如需使用儀表板和建立查詢的詳細資訊，請參閱 the section called “查詢和篩選條件”。

警示將 Amazon CloudWatch (CloudWatch) 指標與 AWS IoT 機群索引服務中的可搜尋欄位結合使用，來建立 CloudWatch 警示。例如，您可建立一則警示，其在您機群中裝置的平均電池電量低於 50% 時，會產生一則 Amazon Simple Notification Service (Amazon SNS)訊息。

Fleet Hub 警示會使用機群索引服務的 GetStatistics 和 GetPercentiles 功能，查詢彙總資料。例如，當您建立追蹤自訂數值欄位的警示時，您可建立套用至指定屬性之下列值得警示閾值。

- 最大
- 計數
- 總和
- 下限
- 平均數
- 在第 10 個、第 50 個、第 90 個，第 95 個或第 99 個百分位數的值

如需在機群索引服務中查詢彙整資料的詳細資訊，請參閱彙總資料的查詢。

下表列出一些可用於 AWS 受管欄位和自訂欄位之彙總類型的範例。

欄位	Aggregation Period (彙總期間)
事物類型 (AWS 受管字串欄位)	計數
事物群組 (AWS 受管字串欄位)	計數
已連線 (AWS 受管布林欄位) `true` 的值為 1。`false` 的值為 0。	• 最大 • 計數 • 總和 • 下限 • 平均數
shadow.reported.batterylevel (機群索引服務中建立的數字彙總欄位)	• 最大 • 計數 • 總和 • 下限 • 平均數 • p10 (第 10 百分位數) • p50 (第 50 百分位數) • p90 (第 90 百分位數) • p95 (第 95 百分位數) • p99 (第 99 百分位數)

除了指定彙總欄位和類型之外，您還可指定下列值。

- 您指定的警示閾值觸發警示所需的時間長度 (1 分鐘或 5 分鐘)。
- 下列其中一個要套用至您指定彙總欄位和類型的比較運算子。
  - 更大
  - 大於/等於
  - 較低
  - 低於/等於
- 與您指定的比較運算子搭配使用的值。
- 您組織中每次觸發警示時所收到 Amazon SNS 訊息之人員的電子郵件地址清單。

- 警示名稱。

如要建立 Fleet Hub 警示，請參閱 the section called “建立警示”。

建立警示

本主題會逐步說明建立一個 Fleet Hub for AWS IoT Device Management 警示所需的步驟。其假設您的系統管理員已從名為 shadow.reported.batterylevel 的裝置影子欄位建立一個彙總欄位。此自訂欄位指出裝置的電池電量。您必須要求管理員在AWS IoT 機群索引服務中建立可搜尋的自訂欄位。

只要您機群中裝置的平均電池電量於 1 分鐘內低於 50%，您所建立的警示就會將 Amazon Simple Notification Service (Amazon SNS) 訊息傳送至您組織中的人員清單。

建立 Fleet Hub 查詢

1. 瀏覽至您 Fleet Hub 應用程式。
2. 若您想要鎖定特定的裝置組合，請建立查詢。如需如何建立簡單查詢的指示，請參閱 the section called “使用篩選條件建立查詢”。若您並未建立查詢，您的警示會套用至您機群中的所有裝置。
3. 在預設儀表板頁面上，選擇 Create alarm (建立警示)。
4. 在 Build aggregation metric (建立彙整指標) 頁面上，請確認您於 Target query (目標查詢) 之下顯示查詢。在 Configure fleet metric aggregation (設定機群指標彙整) 區段中，於 Choose field (選擇欄位) 中，選擇 shadow.reported.batterylevel。此選單包含 AWS 受管欄位，及您的系統管理員建立於 AWS IoT 機群索引服務中的自訂欄位。
5. 若為 Choose aggregation type (選擇彙總類型)，請選擇 Average (平均)。此選擇根據裝置機群中的平均電池電量值設定警報。
6. 若為 Choose period (選擇期間)，請選擇 1 Minute (1 分鐘)。當您的裝置機群保持在指定的警示狀態一分鐘時，就會觸發警示。

   選擇 Next (下一步)。
7. 在 Set threshold (設定閾值) 頁面中的 Trigger the alarm whenever... (觸發警報...) 區段中，選擇 Lower/Equal (低於/等於)。當平均電池電量值低於您指定的值時，此會觸發警示。
8. 在 Than (比) 文字方塊中，輸入 50。

   選擇 Next (下一步)。
9. 在 Notify user (通知使用者) 頁面的 Notify – optional (通知 – 選用) 區段中，輸入電子郵件清單的名稱，其中包含您組織中在警示處於作用中狀態時收到通知的使用者。輸入電子郵件地址清單 (以逗號分隔)，填入此清單。

10. 在 Alarm details (警示詳細資料) 區段中，輸入警示的名稱，然後選擇性地輸入警示的說明。選擇 Next (下一步)。
11. 於 Review (檢閱) 頁面上，檢閱您在先前頁面上輸入的資訊。選擇 Submit (提交)。您會返回預設的儀表板。
12. 在預設儀表板左側的導覽面板中，選擇 Fleet Hub alarms (Fleet Hub 警示)。確認您看到您建立的警示。

疑難排解

本節提供疑難排解資訊及可能的解決方案，協助 Fleet Hub 使用者解決問題。

徵狀	解決方案
我無法將更多的篩選條件或術語新增至我的查詢。	請確定您尚未達到四個查詢術語和篩選條件的限制。
我找不到自訂指標。	請您的管理員在機群索引服務中建立指標。
我的警示並未顯示任何資料。	警示資料需要幾分鐘才能載入。
我需要變更我的警示設為目標的裝置。	移至您的儀表板並變更查詢。
我在儀表板中變更區域時看到錯誤訊息。	請您的管理員確認機群索引已啟用於您選取的區域中。
我的「物件」的連線狀態不是由機群索引編制索引。	連接至 AWS IoT 時，請確定您的用戶端正在使用與物件名稱相同的用戶端 ID。如果您的用戶端在連接至 AWS IoT 時使用與物件名稱不同的 ID，則「物件」的連線狀態將不會透過機群編製索引。

監控 Fleet Hub for AWS IoT Device Management

監控對維護 Fleet Hub 及您其他 AWS 解決方案的可靠性、可用性和效能至關重要。AWS 提供下列監控工具來監看 Fleet Hub，在出現問題時進行回報，並在適當的時候自動採取行動。

- AWS CloudTrail 擷取您 AWS 帳戶發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

主題

使用 AWS CloudTrail 記錄 Fleet Hub for AWS IoT Device Management API 呼叫

Fleet Hub for AWS IoT Device Management 與 AWS CloudTrail 進行整合。CloudTrail 服務提供使用者、角色或 AWS 服務在 Fleet Hub 中所採取動作的記錄。CloudTrail 會將 Fleet Hub 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Fleet Hub 主控台的呼叫，及對 Fleet Hub API 作業的程式碼呼叫。

若您建立追蹤，便可將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Fleet Hub 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。

您可以使用 CloudTrail 所收集的資訊來判斷向 Fleet Hub 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 Fleet Hub 資訊

當您建立帳戶時，系統會在您的 AWS 帳戶中啟用 AWS CloudTrail。此外，Fleet Hub 中發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他 AWS 服務事件記錄至事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

如需您 AWS 帳戶中正在進行事件的記錄 (包含 Fleet Hub 的事件)，請建立追蹤記錄。追蹤可讓 CloudTrail 將記錄檔案交付至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。根據預設，當

您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。

您可配置其他 AWS 服務，進一步分析和處理 CloudTrail 記錄中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Fleet Hub 動作。其會記載於 AWS IoTAPI 參考中。例如，對 `CreateApplication` 和 `UpdateApplication` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 AWS Identity and Access Management 使用者登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 該請求是否由另一項 AWS 服務提出

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 Fleet Hub for AWS IoT Device Management 記錄檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。

CloudTrail 日誌檔案包含一或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。

CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

Example

下列 CloudTrail 記錄項目顯示有關 `CreateApplication` 動作的資訊。

```
{
```

```
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "principal-id",
            "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user-name",
            "accountId": "123456789012",
            "accessKeyId": "access-key",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "principal-id",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2020-12-04T19:59:53Z"
                }
            }
        },
        "eventTime": "2020-12-04T20:02:38Z",
        "eventSource": "iotfleethub.amazonaws.com",
        "eventName": "CreateApplication",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "72.22.186.61",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
            "applicationDescription": "Test application description",
            "applicationName": "Test application name",
            "clientToken": "c9bc7f45-3737-4ee9-9b0f-5de1aab169b2"
        },
        "responseElements": {
            "applicationUrl": "https://application-id.app.iotfleethub.aws",
            "applicationArn": "arn:aws:iotfleethub:us-
east-1:123456789012:application/application-id",
            "applicationId": "application-id"
        },
        "requestID": "5456304e-31c5-4336-9bbe-a375e3728eee",
        "eventID": "9ffb5d72-9267-4f4e-88e6-d26051133c8c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "recipientAccountId": "123456789012"
```

```
}
```

Fleet Hub for AWS IoT Device Management 中的安全性

的雲端安全 AWS 是最高優先順序。作為 AWS 客戶，您受益於資料中心和網路架構，該架構旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，這是AWS 合規計畫 的一部分。若要了解適用於 Fleet Hub 的合規計劃，請參閱依AWS 合規計劃在 範圍內依合規計劃。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Fleet Hub for AWS IoT Device Management 時套用共同責任模型。下列主題將示範如何設定 Fleet Hub 以達到您的安全和合規目標。您也將了解如何使用 AWS 其他服務來協助您監控和保護 Fleet Hub 資源。

主題

Fleet Hub 中的資料保護

AWS 共同責任模型適用於 Fleet Hub for AWS IoT Device Management 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權。 FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和 GDPR部落格文章。

為了資料保護目的，我們建議您保護 AWS 帳戶 憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management （ ） 設定個別使用者IAM。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 （MFA）。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 使用 設定 API和使用者活動日誌 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 線索。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列介面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用FIPS端點。如需可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 （FIPS） 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Fleet Hub 或其他 AWS 服務 主控台API AWS CLI、 或 時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您將 URL提供給外部伺服器，強烈建議您在 中不要包含憑證資訊，URL以驗證您對該伺服器的請求。

靜態加密

Fleet Hub 經由伺服器端加密保護靜態資料。如需詳細資訊，請參閱《AWS IoT 開發人員指南》中AWS IoT中的靜態加密。

傳輸中加密

在流程的雲端部署中，Fleet Hub 會使用 Transport Layer Security （TLS） 通訊協定來保護傳輸中的資料。如需詳細資訊，請參閱 《AWS IoT 開發人員指南》中 AWS IoT中的傳輸安全性。

的身分和存取管理 Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management （IAM） 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 Fleet Hub 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

物件

使用 AWS Identity and Access Management （ IAM ） 的方式會有所不同，具體取決於您在 Fleet Hub 中執行的工作。

Service user (服務使用者)：若您使用 Fleet Hub 服務執行任務，您的管理員會為您提供您需要的憑證和許可。隨著您為了執行作業而使用的 Fleet Hub 功能數量變多，您可能會需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。若您無法存取 Fleet Hub 中的某項功能，請參閱對 Fleet Hub for AWS IoT Device Management 身分和存取權進行故障診斷。

Service administrator (服務管理員)：若您負責公司內的 Fleet Hub 資源，您可能具備 Fleet Hub 的完整存取權限。您的任務是判斷服務使用者應存取的 Fleet Hub 功能及資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念IAM。若要進一步了解您的公司如何IAM搭配 Fleet Hub 使用，請參閱 Fleet Hub for AWS IoT Device Management 如何使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 Fleet Hub 存取的詳細資訊。若要檢視您可以在 中使用的 Fleet Hub 身分型政策範例IAM，請參閱 的身分型政策範例 Fleet Hub for AWS IoT Device Management。

使用身分驗證

驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任IAM角色來驗證 （ 登入 AWS ）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center （ IAM Identity Center ） 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合來存取 時，您會間接擔任 角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 使用者指南 中的如何登入 AWS 帳戶您的 。 AWS 登入

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （SDK） 和命令列介面 （CLI），以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法來自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多因素身分驗證 （MFA） 來提高帳戶的安全性。若要進一步了解，請參閱 AWS IAM Identity Center 使用者指南 中的多重要素驗證和 使用者指南 中的使用多重要素驗證 （MFA） AWS。 IAM

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的需要根使用者憑證的任務。

聯合身分

作為最佳實務， 會要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證與身分提供者聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取 時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南 中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換需要長期憑證的使用案例存取金鑰。

IAM 群組是指定IAM使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 的群組IAMAdmins，並授予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者 （ 而非角色 ）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的擔任角色的方法。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 IAM 使用者指南 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人 （ 受信任的主體 ） 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用某些 AWS 服務，您可以將政策直接連接至資源 （ 而不是使用角色作為代理 ）。若要了解跨帳戶存取的角色與資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 （ FAS ） – 當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。

- 服務角色 – 服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行之應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用IAM角色或IAM使用者，請參閱 IAM 使用者指南 中的建立IAM角色 （ 而非使用者 ）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是其中的物件，AWS 當與身分或資源相關聯時， 會定義其許可。當主體 （ 使用者、根使用者或角色工作階段 ） 發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策都以JSON文件 AWS 形式儲存在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南 中的JSON 政策概觀。

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 AWS 取得角色資訊API。

身分型政策

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在受管政策與內嵌政策之間進行選擇。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自 的 AWS 受管政策。

存取控制清單 （ ACLs ）

存取控制清單 （ ACLs ） 控制哪些主體 （ 帳戶成員、使用者或角色 ） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，請參閱 Amazon Simple Storage Service 開發人員指南 中的存取控制清單 （ ACL ） 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 （ IAM使用者或角色 ） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南 中的IAM實體許可界限。
- 服務控制政策 （ SCPs ） – SCPs是在 中指定組織或組織單位 （ OU ） 最大許可JSON的政策 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。如果您啟用組織中的所有功能，則可以將服務控制政策 （ SCPs ） 套用至任何或所有帳

戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南 中的政策評估邏輯。

Fleet Hub for AWS IoT Device Management 如何使用 IAM

在您使用 IAM 管理 Fleet Hub 的存取權之前，請先了解哪些IAM功能可與 Fleet Hub 搭配使用。

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

IAM 功能	Fleet Hub 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACLs	否
ABAC （政策中的標籤）	是
暫時性憑證	是
主體許可	是
服務角色	是

IAM 功能	Fleet Hub 支援
服務連結角色	否

若要取得 Fleet Hub 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱 IAM 使用者指南 中的 AWS 使用 的服務IAM。

適用於 Fleet Hub 的身分型政策

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的IAMJSON政策元素參考。

Fleet Hub 的身分型政策範例

如要檢視 Fleet Hub 身分型政策的範例，請參閱 的身分型政策範例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 內的資源型政策

支援資源型政策：否

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的 時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南 中的跨帳戶資源存取權IAM。

Fleet Hub 的政策動作

> **Note**
>
> Fleet Hub 應用程式會使用 `AWSIoTFleetHubFederationAccess` 受管政策。如需詳細資訊，請參閱???。

支援政策動作：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action`元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符API操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

如要查看 Fleet Hub 動作的清單，請參閱《服務授權參考》中的 Fleet Hub for AWS IoT Device Management定義的動作。

Fleet Hub 中的政策動作會在該動作前使用下列字首：

```
iotfleethub
```

如要在單一陳述式中指定多個動作，請以逗號進行分隔：

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

如要檢視 Fleet Hub 身分型政策的範例，請參閱 的身分型政策範例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name （ ARN ） 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 Fleet Hub 資源類型及其 的清單ARNs，請參閱服務授權參考 中由 定義的資源 Fleet Hub for AWS IoT Device Management。若要了解您可以使用哪些動作指定每個資源ARN的 ，請參閱 定義的動作 Fleet Hub for AWS IoT Device Management。

如要檢視 Fleet Hub 身分型政策的範例，請參閱 的身分型政策範例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者的使用者名稱加上標籤時，您才能授予IAM使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的AWS 全域條件內容索引鍵。

如要查看 Fleet Hub 條件索引鍵的清單，請參閱《服務授權參考》中的 Fleet Hub for AWS IoT Device Management的條件索引鍵。若要了解您可以使用條件金鑰的動作和資源，請參閱 定義的動作 Fleet Hub for AWS IoT Device Management。

如要檢視 Fleet Hub 身分型政策的範例，請參閱 的身分型政策範例 Fleet Hub for AWS IoT Device Management。

Fleet Hub 中的存取控制清單 （ACLs）

支援ACLs：否

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

使用 Fleet Hub 的屬性型存取控制 （ABAC）

支援 ABAC（政策中的標籤）：是

屬性型存取控制 （ABAC） 是一種根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至IAM實體 （使用者或角色） 和許多 AWS 資源。標記實體和資源是 的第一步 ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取的資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 的詳細資訊ABAC，請參閱 使用者指南 中的什麼是 ABAC？。 IAM 若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的使用屬性型存取控制 （ABAC）。

暫時性憑證與 Fleet Hub 搭配使用

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 IAM 使用者指南 中的 AWS 服務 與 搭配使用IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則表示您正在使用臨時憑證。例如，當您 AWS 使用公司的單一登入 （SSO） 連結存取 時，該程序會自動建立臨時憑

證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南 中的切換到角色（主控台）。

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時憑證來存取 AWS. AWS recommends，您動態產生臨時憑證，而不是使用長期存取金鑰。如需詳細資訊，請參閱 中的臨時安全憑證IAM。

Fleet Hub 的跨服務委託人許可

支援轉送存取工作階段（FAS）：是

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段。

Fleet Hub 的服務角色

支援服務角色：是

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

> **Warning**
>
> 變更服務角色的許可可能會中斷 Fleet Hub 功能。只有在 Fleet Hub 提供指引時，才能編輯服務角色。

Fleet Hub 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱AWS 使用 的服務IAM。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 Fleet Hub for AWS IoT Device Management

依預設，使用者和角色不具備建立或修改 Fleet Hub 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface （ AWS CLI ） 或 來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立IAM身分型JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

如需 Fleet Hub 定義的動作和資源類型的詳細資訊，包括ARNs每種資源類型的 格式，請參閱服務授權參考 中的 的動作、資源和條件索引鍵 Fleet Hub for AWS IoT Device Management。

主題

- 政策最佳實務
- 使用 Fleet Hub 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Fleet Hub 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用受AWS 管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 任務功能的受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （ JSON ） 和IAM最佳實務。IAM Access Analyzer

提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。

- 需要多因素身分驗證 （MFA） – 如果您有需要 IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

使用 Fleet Hub 主控台

若要存取 Fleet Hub for AWS IoT Device Management 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視 中 Fleet Hub 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其API嘗試執行的操作相符的動作。

為了確保使用者和角色仍然可以使用 Fleet Hub 主控台，也請將 Fleet Hub `ConsoleAccess`或`ReadOnly` AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南 中的新增許可給使用者。

允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 或 AWS CLI 以程式設計方式完成此動作的許可 AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

對 Fleet Hub for AWS IoT Device Management 身分和存取權進行故障診斷

使用下列資訊來協助您診斷和修正使用 Fleet Hub 和 時可能遇到的常見問題IAM。

主題

- 我未獲授權在 Fleet Hub 中執行動作
- 我無權執行 iam：PassRole
- 我想要允許 AWS 帳戶外的人存取我的 Fleet Hub 資源

我未獲授權在 Fleet Hub 中執行動作

如果 AWS Management Console 告訴您未獲授權執行動作，則必須聯絡管理員尋求協助。您的管理員是為您提供登入憑證的人員。

> **Note**
>
> Fleet Hub 應用程式會使用 `AWSIoTFleetHubFederationAccess` 受管政策。如需詳細資訊，請參閱???。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構*my-example-widget*資源的詳細資訊，但沒有虛構iotfleethub:*GetWidget*許可時，會發生下列錯誤範例。

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 iotfleethub:*GetWidget* 資源。

我無權執行 iam：PassRole

若您收到錯誤，告知您無權執行 iam:PassRole 動作，則您的政策必須更新，允許您將角色傳遞給 Fleet Hub。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor IAM的使用者嘗試使用主控台在 Fleet Hub 中執行動作時，會發生下列錯誤範例。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人存取我的 Fleet Hub 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援資源型政策或存取控制清單 （ACLs） 的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 如要了解 Fleet Hub 是否支援這些功能，請參閱 Fleet Hub for AWS IoT Device Management 如何使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的在您 AWS 帳戶 擁有的另一個資源中為IAM使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 使用者指南 中的提供存取權給第三方 AWS 帳戶 擁有。 IAM

- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的為外部驗證的使用者提供存取權（身分聯合）。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。

Fleet Hub for AWS IoT Device Management 的合規驗證

第三方稽核人員會在多個合規計畫中評估 Fleet Hub 的安全性和 AWS 合規性。其中包括 SOC、PCI、Fed RAMP、 HIPAA和其他。

若要了解 是否 AWS 服務 在特定合規計畫的範圍內，請參閱AWS 服務 依合規計畫然後選擇您感興趣的合規計畫。如需一般資訊，請參閱 AWS Compliance Programs 。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您在使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。 AWS 提供下列資源以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供以 AWS 安全與合規為重點的基準環境部署步驟。
- Amazon Web Services 上HIPAA安全和合規的架構 – 本白皮書描述了公司如何使用 AWS 來建立HIPAA合格的應用程式。

> **Note**
>
> 並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱HIPAA合格服務參考 。

- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明跨多個架構（包括國家標準和技術研究所（）NIST、支付卡產業安全標準委員會（PCI）和國際標準化組織（ISO））保護指南 AWS 服務 並映射至安全控制的最佳實務。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態是否符合內部實務、產業指導方針和法規。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視 內的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。

- Amazon GuardDuty – 這會透過監控環境是否有可疑和惡意活動來 AWS 服務 偵測 AWS 帳戶、工作負載、容器和資料的潛在威脅。 GuardDuty 可以透過滿足某些合規架構強制要求的入侵偵測需求，協助您解決各種合規要求DSS，例如 PCI 。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

Fleet Hub for AWS IoT Device Management 中的復原能力

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援的網路連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱AWS 全域基礎設施。

AWS Fleet Hub for AWS IoT Device Management 的 受管政策

若要將許可新增至使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立IAM客戶受管政策需要時間和專業知識，為您的團隊提供他們所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並且可在您的帳戶中使用 AWS 。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南 中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務的任務函數的受管政策。例如， ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。服務啟動新功能時， 會 AWS 新增新操作和資源的唯讀許可。如需任務函數政策的清單和說明，請參閱 IAM 使用者指南 中的AWS 任務函數的受管政策。

AWS 受管政策： AWSIoTFleetHubFederationAccess

您可以將AWSIoTFleetHubFederationAccess政策連接至身分IAM。

此政策授予 Fleet Hub for AWS IoT Device Management 聯合使用者從 Fleet Hub Web 應用程式對 AWS IoT 和其他 AWS 服務採取動作所需的許可。

如需將使用者新增至 Fleet Hub Web 應用程式的詳細資訊，請參閱 ???。

於 AWS 主控台中檢視此政策。

許可詳細資訊

此政策包含以下許可：

- iot - 擷取 AWS IoT 裝置資料並執行機群層級動作。
- iotfleethub：擷取 Fleet Hub 應用程式中繼資料。
- cloudwatch - 擷取 CloudWatch 警示和指標資料。也允許建立和刪除設定為 Fleet Hub 警示範圍的動作。
- sns：執行建立、讀取、刪除、訂閱及取消訂閱操作。這些操作範圍涵蓋 Fleet Hub SNS主題。

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

受 AWS 管政策的 Fleet Hub 更新

檢視自此服務開始追蹤這些變更以來，Fleet Hub 受 AWS 管政策更新的詳細資訊。如需詳細資訊，請參閱 Fleet Hub Documentation history (文件歷史記錄) 頁面。

變更	描述	日期
AWSIoTFleetHubFederationAccess – 更新現有政策	Fleet Hub 新增了新的許可，允許應用程式使用者擷取 Fleet Hub 應用程式中的 AWS IoT Device Defender 指標資料。	2022 年 4 月 4 日
AWSIoTFleetHubFederationAccess – 更新現有政策	Fleet Hub 新增了新的許可，允許應用程式使用者擷取其他資料來源來編製索引。也會新增許可，以允許應用程式使用者取消應用程式中 AWS IoT 的任務執行。	2021 年 11 月 15 日
AWSIoTFleetHubFederationAccess – 更新現有政策	Fleet Hub 新增了應用程式使用者擷取 Thing 群組資料和執行 AWS IoT 任務CRUD操作的新許可。	2021 年 5 月 24 日
AWSIoTFleetHubFederationAccess – 更新現有政策	Fleet Hub 已移除不支援的 Fleet Hub 儀表板 的許可 APIs。	2021 年 4 月 12 日
AWSIoTFleetHubFederationAccess – 新政策	Fleet Hub 新增了一項新政策，授予 Fleet Hub 應用程式使用	2021 年 4 月 12 日

變更	描述	日期
	者擷取裝置資料和執行 AWS IoT 動作所需的許可。	
Fleet Hub 開始追蹤變更	Fleet Hub 開始追蹤其 AWS 受管政策的變更。	2021 年 4 月 12 日

Fleet Hub for AWS IoT Device Management 中的基礎設施安全

作為受管服務，Fleet Hub for AWS IoT Device Management 受到 Amazon Web Services：安全程序概觀白皮書中所述 AWS 的全球網路安全程序保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取 Fleet Hub。用戶端必須支援 Transport Layer Security （ TLS ） 1.2 或更新版本。建議使用 TLS 1.3。用戶端還必須支援具有完美正向保密性 （ PFS ） 的密碼套件，例如 Ephemeral Diffie-Hellman （ DHE ） 或 Elliptic Curve Ephemeral Diffie-Hellman （ ECDHE ）。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，必須使用與IAM委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以使用 AWS Security Token Service (AWS STS) 產生臨時安全憑證來簽署請求。

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 中 AWS，跨服務模擬可能會導致混淆代理問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

若要限制 Fleet Hub 為資源提供另一項服務的許可，我們建議在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵。如果同時使用全域條件內容索引鍵，則在相同政策陳述式中使用`aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須使用相同的帳戶 ID。

防止混淆代理問題的最有效方法是使用具有完整 Amazon Resource Name （ ARN ） 資源的`aws:SourceArn`全域條件內容金鑰。對於 Fleet Hub，`aws:SourceArn` 必須符合以下格式：`arn:aws:iot:`*`region`*`:`*`account-id`*`:*`。請確定 *`region`* 符合您的 Fleet Hub 區域和 *`account-id`* 符合您的客戶帳戶 ID。

下列範例展示如何透過在 Fleet Hub 角色信任政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵，來預防混淆代理人問題。若要尋找您的 Fleet Hub 角色ARN，請前往 AWS IoT 主控台中的 Fleet Hub 區段，然後選取您的 Fleet Hub 應用程式以檢視應用程式詳細資訊頁面。

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

文件歷史記錄

下表說明對 Fleet Hub 文件的更新。如需了解 Fleet Hub 的 AWS 受管政策中的變更，請參閱 Fleet Hub for AWS IoT Device Management 的 AWS 受管政策。

變更	描述	日期
Fleet Hub for AWS IoT Device Management 正式版本	更新內容，反映 Fleet Hub for AWS IoT Device Management 在預覽期間的改善。	2021 年 5 月 25 日。
Fleet Hub for AWS IoT Device Management 預覽版	發佈《Fleet Hub for AWS IoT Device Management 使用者指南》的預覽版本。	2020 年 12 月 16 日。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。