Guía de administración de AWS IoT dispositivos de Fleet Hub

Fleet Hub para la gestión de AWS IoT dispositivos

Fleet Hub para la gestión de AWS IoT dispositivos: Guía de administración de AWS IoT dispositivos de Fleet Hub

Table of Contents

¿Qué es Fleet Hub para AWS IoT Device Management?

Con Fleet Hub para AWS IoT Device Management (Fleet Hub), puede crear aplicaciones web independientes para supervisar el estado de sus flotas de dispositivos. Puede poner estas aplicaciones a disposición de los usuarios de su organización, aunque no tengan cuentas AWS. Utilice Fleet Hub para gestionar las tareas más comunes en flotas, como investigar y solucionar problemas operativos y de seguridad.

Fleet Hub ofrece las siguientes funciones.

- Supervisar las flotas de dispositivos en tiempo casi real.
- Configurar alertas para notificar a los técnicos cuando haya un comportamiento inusual.
- Trabajos en ejecución.

> **Note**
>
> A fin de que Fleet Hub pueda indexar los datos del estado de la conectividad, los objetos deben conectarse al AWS IoT Core con un ID de cliente igual al nombre del objeto.

Funcionamiento de Fleet Hub para AWS IoT Device Management

Los administradores pueden usar Fleet Hub para AWS IoT Device Management a fin de crear aplicaciones web seguras en pocos minutos, sin aprovisionar recursos ni escribir código. Las aplicaciones web que crea con Fleet Hub se integran con sus sistemas de identidad existentes, como Active Directory. Gracias a esto, los administradores pueden aplicar sus propios modelos de autenticación y autorización.

Las aplicaciones web de Fleet Hub se integran con la indexación de flotas y la supervisión de dispositivos de AWS IoT Core. Estas integraciones permiten supervisar los datos de estado de los dispositivos y crear alarmas cuando los dispositivos de la flota lleguen a un determinado estado.

Las aplicaciones de Fleet Hub utilizan la política administrada `AWSIoTFleetHubFederationAccess`. Para obtener más información, consulte ???.

Ejemplos de casos de uso:

- Ver los problemas de conectividad de los dispositivos. Puede ver la cantidad de dispositivos desconectados de su flota, el estado de última conexión de cualquier dispositivo y el motivo o los motivos por los que se han desconectado.
- Configurar alarmas. Puede establecer umbrales que activen alarmas cuando un número determinado de dispositivos se desconecten. Las alarmas también pueden avisarle cuando uno o varios dispositivos se desconecten por un motivo concreto. Luego, puede consultar información detallada del dispositivo para investigar el problema y resolverlo.
- Ejecutar tareas. Puede ejecutar operaciones remotas (como actualizaciones de firmware) en uno o más dispositivos.

Cómo funciona la indexación de datos de Fleet Hub

Puede usar la consola de Fleet Hub para activar la indexación de flotas en su propia flota de dispositivos. Cuando active la indexación de flotas en Fleet Hub, esta se activará para toda la flota y estará disponible para todas las aplicaciones de Fleet Hub.

Cuando está habilitada, la indexación de flotas indexa automáticamente todos los campos administrados por AWS IoT Core. También puede usar la indexación de flotas para añadir datos personalizados con los que consultar y agregar datos en las aplicaciones de Fleet Hub.

Cómo funcionan las alarmas de Fleet Hub

Las aplicaciones web de Fleet Hub proporcionan una interfaz que permite a los usuarios crear alarmas. En los siguientes pasos, se muestra cómo pueden los usuarios crear alarmas en Fleet Hub.

1. Crear una consulta para agregar datos: especifique una consulta que añada los dispositivos a los que sus usuarios quieren dirigirse mediante campos con capacidad de búsqueda.
2. Configurar un umbral: establezca un umbral que active las alarmas cuando se alcance una condición en los datos indexados (por ejemplo, el estado de conectividad durante un intervalo específico).
3. Configure la notificación: especifique un grupo de destinatarios a los que Fleet Hub notifique cuando los dispositivos especificados estén en alarma.

Cómo funcionan los trabajos de Fleet Hub

Puedes usar la consola Fleet Hub para ejecutar operaciones remotas en los dispositivos.

Cuando las plantillas de trabajo están habilitadas, puede crear trabajos específicos desde las plantillas en sus aplicaciones de Fleet Hub.

Fleet Hub para la gestión de AWS IoT dispositivos para administradores

Esta sección contiene instrucciones para los administradores sobre cómo crear y administrar las aplicaciones web de Fleet Hub for AWS IoT Device Management.

Temas

Introducción

En esta sección se explica cómo crear y configurar Fleet Hub para las aplicaciones web de administración de AWS IoT dispositivos.

Temas

Cree su primera aplicación Fleet Hub

Requisitos previos

La siguiente lista contiene los recursos que necesita para crear una aplicación web de Fleet Hub.

- Una cuenta de AWS.
- El AWS IAM Identity Center debe estar activado en su cuenta. (Si aún no ha activado este servicio, la consola AWS IoT Core (https://console.aws.amazon.com/iot/) le pedirá que lo haga).

Cree su primera aplicación web de Fleet Hub

Los siguientes pasos describen cómo crear aplicaciones web de Fleet Hub para la administración de AWS IoT dispositivos.

1. Ve a la AWS IoT Core consola (https://console.aws.amazon.com/iot/) y, en el panel izquierdo, selecciona Fleet Hub y, a continuación, Aplicaciones.
2. En la página de aplicaciones, seleccione Crear aplicación.
3. En la página Configurar el centro de identidad de IAM, si no lo has activado AWS IAM Identity Center (Centro de identidad de IAM), sigue los pasos para activarlo. AWS Organizations le envía un correo electrónico. Siga el enlace del correo electrónico para terminar la activación del Centro de identidades de IAM.

   > **Note**
   >
   > Puede conectar su propio proveedor de identidades al Centro de identidades de IAM. Para obtener más información, consulte ¿Qué es AWS IAM Identity Center? y Conéctese a su proveedor de identidad externo.
   > Al crear una aplicación Fleet Hub, debe crear una instancia organizativa de IAM Identity Center si aún no tiene una. La aplicación Fleet Hub que cree también debe estar en la misma instancia Región de AWS de organización de IAM Identity Center. Para obtener más información, consulte Habilitar las instancias del Centro de Identidad de IAM y de la Organización del Centro de Identidad de IAM.

   La página le indica si ya ha activado el Centro de identidades de IAM.

   Elija Siguiente.
4. En la página de AWS IoT datos del índice, consulta la información de la sección Cómo funciona el flujo de datos desde AWS IoT Fleet Hub. Esta página te enlaza con las páginas de la AWS IoT Core consola en las que puedes activar y gestionar la indexación de la AWS IoT Core flota. Puede usar este servicio para indexar, buscar y agregar datos de registro, datos de sombras, datos de conectividad de los dispositivos (eventos de ciclo de vida de los dispositivos) y datos de infracciones de dispositivos. También puedes crear campos personalizados además de los campos gestionados que la indexación de AWS IoT Core flotas indexa de forma predeterminada.

   - Si ha activado la indexación de flotas, esta página muestra la configuración de indexación de su flota y los campos personalizados.

- Si no ha activado la indexación y la conectividad de los objetos, debe hacerlo para poder usar Fleet Hub.

Cuando haya terminado de gestionar y revisar la configuración de indexación de flota, seleccione Siguiente.

Para obtener más información sobre cómo activar la indexación de flotas para las aplicaciones de Fleet Hub, consulte Managing fleet indexing for Fleet Hub applications.

5. En la página Configurar aplicación, en la sección Rol de la aplicación, cree un nuevo rol de servicio o seleccione un rol de servicio existente. La aplicación web de Fleet Hub asume este rol cuando utiliza los recursos de Fleet Hub. Los usuarios federados tienen los mismos permisos que el rol cuando usan la aplicación web.

   - Si crea un rol nuevo, el nombre del rol debe comenzar con la siguiente cadena: `AWSIotFleetHub_random_string`.

   - Si selecciona un rol existente, asegúrese de que tenga los permisos que figuran en el documento de política. Para ver los permisos que necesita su aplicación web de Fleet Hub, seleccione Ver detalles del rol. Se abre una ventana que muestra el documento de política, que el servicio aplica a cualquier rol nuevo que cree desde esta página.

6. En la página Configurar aplicación, en la sección Propiedades de aplicación, introduzca un nombre para la aplicación. Si lo desea, puede introducir una descripción para la aplicación.

   Elija Crear aplicación.

7. En la pestaña Aplicaciones, elija la aplicación que ha creado y seleccione Ver detalles. Revise los detalles de la aplicación.

> **Note**
>
> Para obtener más información sobre las posibles soluciones para resolver problemas como administrador de Fleet Hub, consulte Troubleshooting.

Administrar la indexación de flotas para las aplicaciones de Fleet Hub

Puede utilizar la AWS IoT Core consola o el AWS CLI para activar la indexación de la flota y configurar las siguientes fuentes de datos para indexar: datos de AWS IoT registro, datos de AWS IoT Device Shadow, datos de AWS IoT conectividad y datos de AWS IoT Device Defender infracciones. Los siguientes pasos describen cómo activar la indexación de flotas para las aplicaciones Fleet Hub for AWS IoT Device Management en AWS IoT Core la consola. Para ver los pasos a seguir AWS CLI, consulta Cómo administrar la indexación de elementos.

> **Important**
>
> El 20 de julio de 2022 estará disponible para el público general de la integración de la indexación de flotas de AWS IoT Device Management con el uso de AWS IoT Core nombres ocultos y la AWS IoT Device Defender detección de infracciones. Con esta versión GA, puede indexar sombras con nombres específicos especificando nombres de sombras. Si ha agregado sombras con nombre para indexarlas durante el período de vista previa pública de esta característica, del 30 de noviembre de 2021 al 19 de julio de 2022, le recomendamos que vuelva a configurar los ajustes de indexación de su flota y elija nombres de sombras específicos para reducir los costes de indexación y optimizar el rendimiento. Para obtener más información sobre cómo reconfigurar los ajustes de indexación de flotas, consulte Managing fleet indexing.

1. Ve a la AWS IoT Core consola (https://console.aws.amazon.com/iot/) y, en el panel izquierdo, selecciona Configuración.
2. En la página de Configuración, vaya a la sección Indexación de flotas y, a continuación, seleccione Administrar la indexación.
3. En la página Gestionar la indexación de la flota, en la sección Configuración, selecciona la indexación de cosas y las fuentes de datos que quieres AWS IoT indexar. Debe activar la indexación y la conectividad de objetos para poder usar Fleet Hub.
4. (Opcional) En la página Administrar la indexación de flotas, en la sección Campos personalizados para la agregación (opcional), cree campos personalizados además de los campos gestionados que la indexación de flotas indexa de forma predeterminada.

   Cuando haya terminado de gestionar y revisar la configuración de indexación de flota, seleccione Siguiente.

La indexación de flotas puede tardar cierto tiempo en actualizar la configuración. Para obtener más información sobre cómo administrar la indexación de flotas, consulte Managing fleet indexing.

Agregar usuarios a las aplicaciones de Fleet Hub

Tu aplicación web Fleet Hub for AWS IoT Device Management no contiene ningún usuario cuando se acaba de crear. Debe agregar usuarios antes de que usted y los miembros de su organización puedan usar la aplicación. En los pasos de este tema se describe cómo añadir usuarios a la aplicación.

Puede añadir usuarios desde su sistema de identidad existente configurando AWS IAM Identity Center (IAM Identity Center) para su cuenta. Puede conectar su propio proveedor de identidades al Centro de identidades de IAM. Para obtener más información consulte What Is IAM Identity Center?

1. En la página de Aplicaciones, elija su aplicación web en la lista de aplicaciones de Fleet Hub. Elija Ver detalles.
2. En la página de detalles de la aplicación, seleccione Agregar usuario.
3. En la ventana Agregar usuarios de Fleet Hub, seleccione a los usuarios de su organización que desee que tengan acceso a la aplicación. Seleccione Agregar usuarios seleccionados.
4. En la página de detalles de la aplicación, compruebe que los usuarios que ha seleccionado aparecen en la lista de usuarios de Fleet Hub.

Los servicios AWS y AWS IoT Core que interactúan con Fleet Hub para AWS IoT Device Management.

En este tema, se explica la interacción de las características de Fleet Hub para AWS IoT Device Management con otros servicios AWS a fin de ofrecer las funciones de las aplicaciones web de Fleet Hub.

En la siguiente tabla, se indican cuáles son los servicios AWS que Fleet Hub para AWS IoT Device Management utiliza a fin de implementar cada característica.

Capability	Servicio de AWS	Descripción
Integrar los sistemas de identidad existentes, como Active Directory.	AWS IAM Identity Center (Centro de identidades IAM)	Puede añadir usuarios de su sistema de identidad existente configurando el AWS IAM Identity Center (Centro de identidades de IAM) para su cuenta. Puede conectar su propio proveedor de identidad es al Centro de identidades de IAM. Para obtener más informaci ón, consulte What Is AWS IAM Identity Center? y Workforce identities.
Crear consultas mediante campos administrados por AWS, campos personalizados y cualquier atributo de los orígenes de datos indexados.	Indexación de flotas de AWS IoT	Utilice el servicio de indexació n de flotas para indexar, buscar y agregar datos de registro, datos de sombras y datos de conectividad de los dispositivos (eventos de ciclo de vida de los dispositi vos). También puede crear campos personalizados para su agregación, además de los campos gestionados que la indexación de flotas de AWS IoT indexa de forma predeterminada. Para obtener más información sobre la indexación de flotas, consulte Fleet indexing.

Capability	Servicio de AWS	Descripción
Crear alarmas para un conjunto de dispositivos especificados en una consulta.	Amazon CloudWatch (CloudWatch)	Los paneles de Fleet Hub muestran las métricas de CloudWatch que puede utilizar en combinación con campos en los que se pueden realizar búsquedas para crear umbrales de alarma. Por ejemplo, puede crear una alarma de CloudWatch que genere una notificación de Amazon Simple Notificat ion Service (Amazon SNS) cada vez que la cantidad de dispositivos conectados sea inferior a una cantidad especificada. Para obtener más información sobre CloudWatch, consulte ¿Qué es Amazon CloudWatc h? Para obtener más informaci ón sobre el funcionamiento de AWS IoT Core con CloudWatc h para crear métricas y alarmas, consulte Monitor AWS IoT alarms and metrics using CloudWatch.

Solución de problemas

En esta sección, encontrará información relacionada con la resolución de problemas como administrador de Fleet Hub.

Síntoma	Solución
El enlace de mi aplicación web no funciona.	Después de crear su aplicación, pueden pasar unas horas hasta que el enlace funcione.
No puedo iniciar sesión en mi aplicación web.	Asegúrese de que ha agregado al menos un usuario a su aplicación. Asegúrese de que su rol tenga la relación de confianza adecuada, como la siguiente: `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` Para obtener información sobre cómo editar la relación de confianza de IAM, consulte Editing the trust relationship for an existing role.
No puedo crear una aplicación web.	Asegúrese de no haber alcanzado el límite de número total de aplicaciones web.
No veo el campo personalizado que esperaba.	Asegúrese de que ha configurado la indexación de flotas de forma correcta. Para obtener más información sobre la indexación de flotas, consulte Fleet indexing.

Fleet Hub para AWS IoT Device Management para usuarios

Esta sección contiene información para los usuarios de las aplicaciones web de Fleet Hub para AWS IoT Device Management. Para obtener información sobre cómo crear aplicaciones de Fleet Hub y cómo agregar usuarios en esas aplicaciones, consulte Fleet Hub para la gestión de AWS IoT dispositivos para administradores.

Temas

Introducción

Esta sección contiene información sobre cómo empezar a utilizar las características de las aplicaciones web de Fleet Hub para AWS IoT Device Management.

Temas

Crear la primera consulta

En este tema, se explican los pasos necesarios para crear una consulta sencilla de Fleet Hub para AWS IoT Device Management. Las consultas se especifican mediante una sintaxis de consulta de búsqueda.

Requisitos previos

- Una aplicación de Fleet Hub vinculada a una cuenta de AWS IoT Core que contenga varios dispositivos (objetos).

- Una cuenta en su organización que tenga permisos para usar la aplicación Fleet Hub.

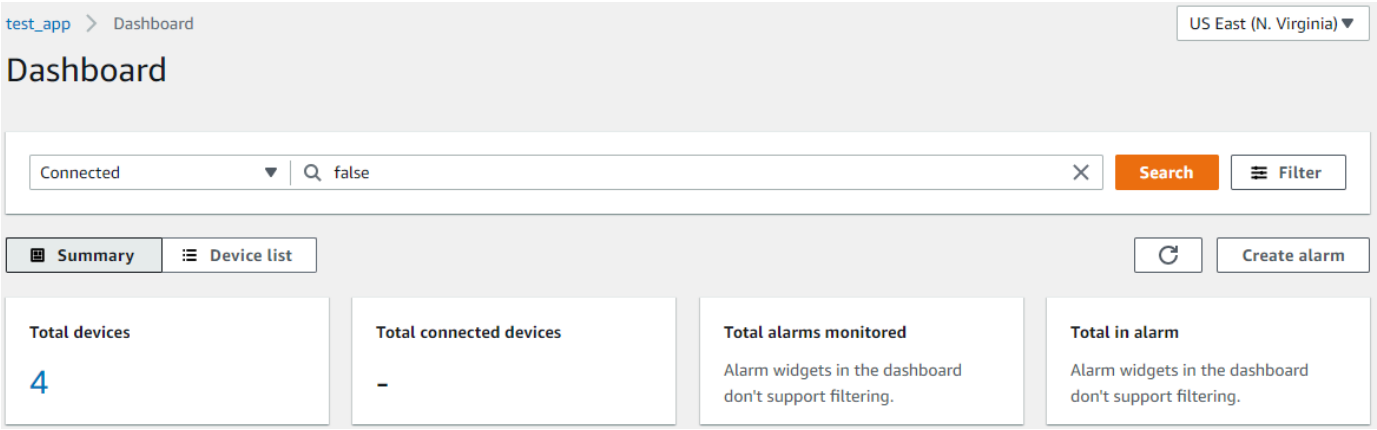
Crear la primera consulta de Fleet Hub

Crear la primera consulta de Fleet Hub

1. Vaya a su aplicación de Fleet Hub.

   La vista del panel de control predeterminado muestra una lista de todos los dispositivos con los atributos administrados y personalizados. Los atributos que contienen el prefijo atributos son atributos personalizados.

2. En el menú de la parte superior de la página, seleccione Conectado en Todos los campos. Introduzca **`false`** en el cuadro de texto situado junto al menú desplegable.



3. Para realizar la búsqueda, seleccione Buscar. Aparecerá una lista de todos los dispositivos que no están conectados a AWS IoT Core.

Para obtener más información sobre la sintaxis de las consultas y las consultas de ejemplo, consulte Query syntax, Example thing queries y Example thing group queries.

Crear la primera alarma

En este tema, se explican los pasos necesarios para crear una alarma sencilla de Fleet Hub para AWS IoT Device Management.

Requisitos previos

- Una aplicación de Fleet Hub vinculada a una cuenta de AWS IoT Core que contenga varios dispositivos (objetos).

- Una cuenta en su organización que tenga permisos para usar la aplicación Fleet Hub.

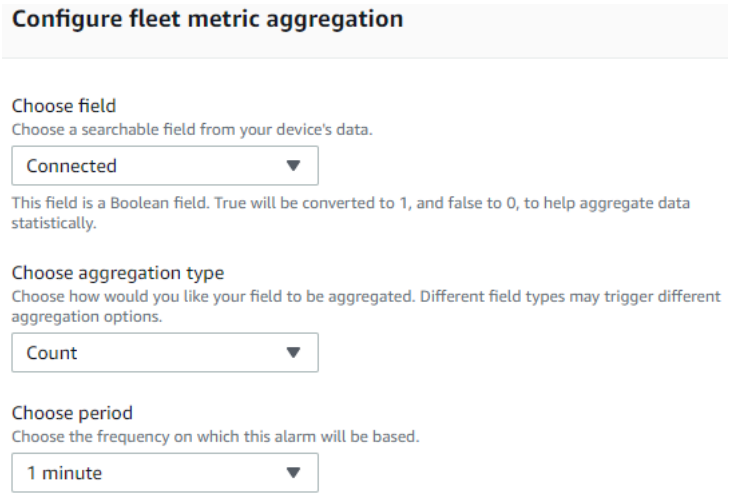
Creación de la primera alarma

Crear la primera alarma de Fleet Hub

1. Vaya a su aplicación de Fleet Hub.
2. Si quiere gestionar un conjunto específico de dispositivos, cree una consulta. Para obtener instrucciones sobre cómo crear una consulta sencilla, vaya a the section called “Crear la primera consulta”. Si no crea una consulta, la alarma se aplicará a todos los dispositivos de su flota.
3. En la página del panel de control predeterminado, seleccione Crear alarma.
4. En la página Crear métrica de agregación, compruebe que la consulta se encuentre bajo Consulta de destino. En la sección Configurar la agregación de métricas de flota, en el menú Elegir campo, seleccione Conectado. Este campo administrado por AWS indica si un dispositivo está conectado a AWS IoT Core. El menú Elegir campo contiene los campos administrados por AWS y los campos personalizados que el administrador ha creado en el servicio de indexación de flotas de AWS IoT.
5. En Elegir el tipo de agregación, elija una de las siguientes opciones.

   - Máximo: configure un umbral máximo.
   - Recuento: configure un recuento específico como umbral.
   - Suma: configure una suma como umbral.
   - Mínimo: configure un umbral mínimo.
   - Promedio: configure un umbral promedio.
6. En Elegir periodo, elija la duración de la condición especificada en los menús anteriores que activará la alarma.

   Este sería el aspecto de un ejemplo de configuración para Configurar la agregación de métricas de flota:



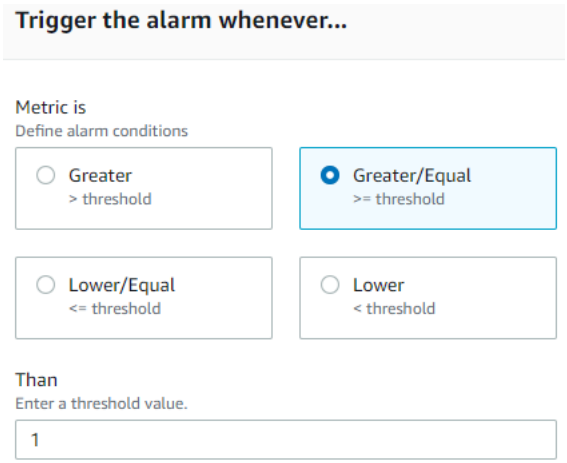
Elija Siguiente.

7. En la página Establecer umbral, en la sección Activar la alarma siempre que..., elija una de las siguientes opciones.

   - Mayor: la alarma se activa cuando la métrica y el tipo de agregación superan el valor especificado.
   - Mayor/igual: la alarma se activa cuando la métrica de agregación y el tipo son iguales o superiores al valor especificado.
   - menor: la alarma se activa cuando la métrica y el tipo de agregación caen por debajo del valor especificado.
   - Menor/igual: la alarma se activa cuando la métrica de agregación y el tipo son iguales o inferiores al valor especificado.

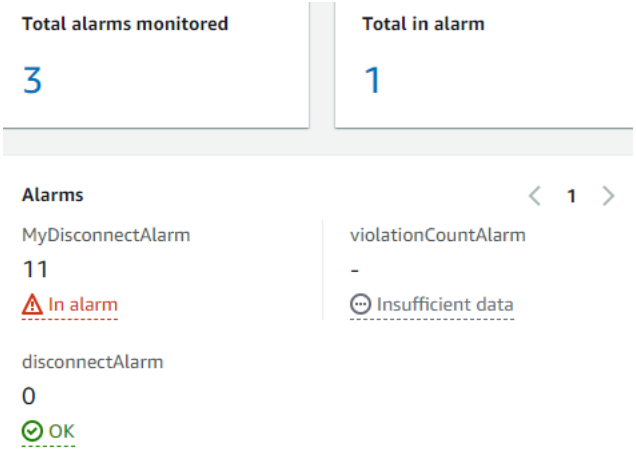
8. En el cuadro de texto Que, especifique el valor que se va a utilizar como umbral para la alarma.

   Un ejemplo de configuración para Establecer umbral, podría tener el siguiente aspecto:

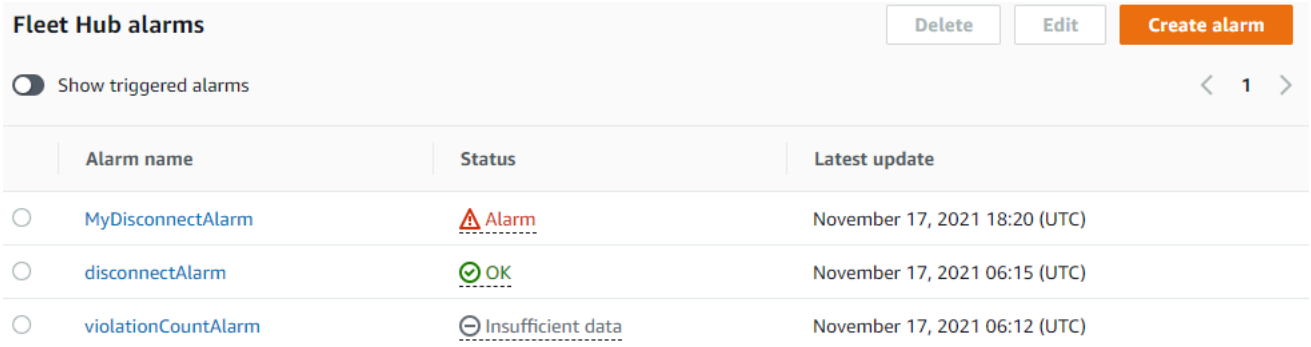


Elija Siguiente.

9. En la página Notificar al usuario, en la sección Notificar (opcional), introduzca un nombre para la lista de correo electrónico donde estarán los usuarios de la organización que recibirán notificaciones cuando la alarma se active. Introduzca una lista de direcciones de correo electrónico, separadas por comas.
10. En la sección Detalles de alarma, introduzca un nombre para la alarma y, si lo desea, una descripción. Elija Siguiente.
11. En la página Revisar, repase la información que ha introducido o seleccionado en las páginas anteriores. Elija Submit (Enviar). Con esto, volverá al panel predeterminado.
12. En el panel de control predeterminado, los widgets de alarmas muestran información de todas las alarmas que ha creado.



Para ver los detalles de las alarmas que ha creado, en el panel de navegación izquierdo, seleccione Alarmas de Fleet Hub.



Visualización de los detalles de los dispositivos

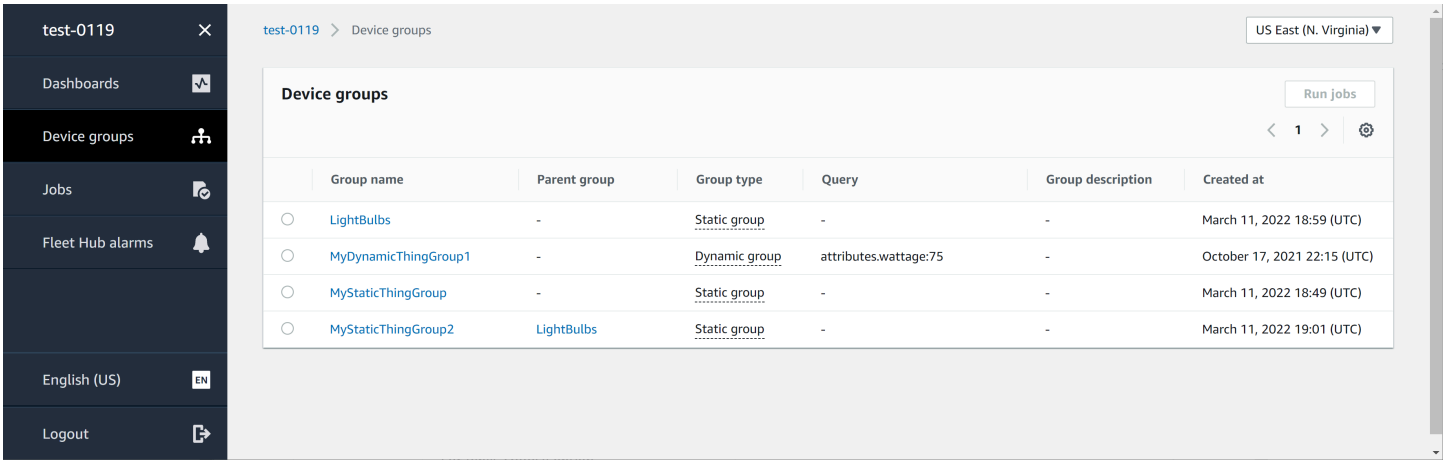
En este tema, se explican los pasos necesarios para ver información sobre los dispositivos y los grupos de dispositivos.

Requisitos previos

- Una aplicación de Fleet Hub vinculada a una cuenta de AWS IoT Core que contenga varios dispositivos (objetos).
- Una cuenta en su organización que tenga permisos para usar la aplicación Fleet Hub.

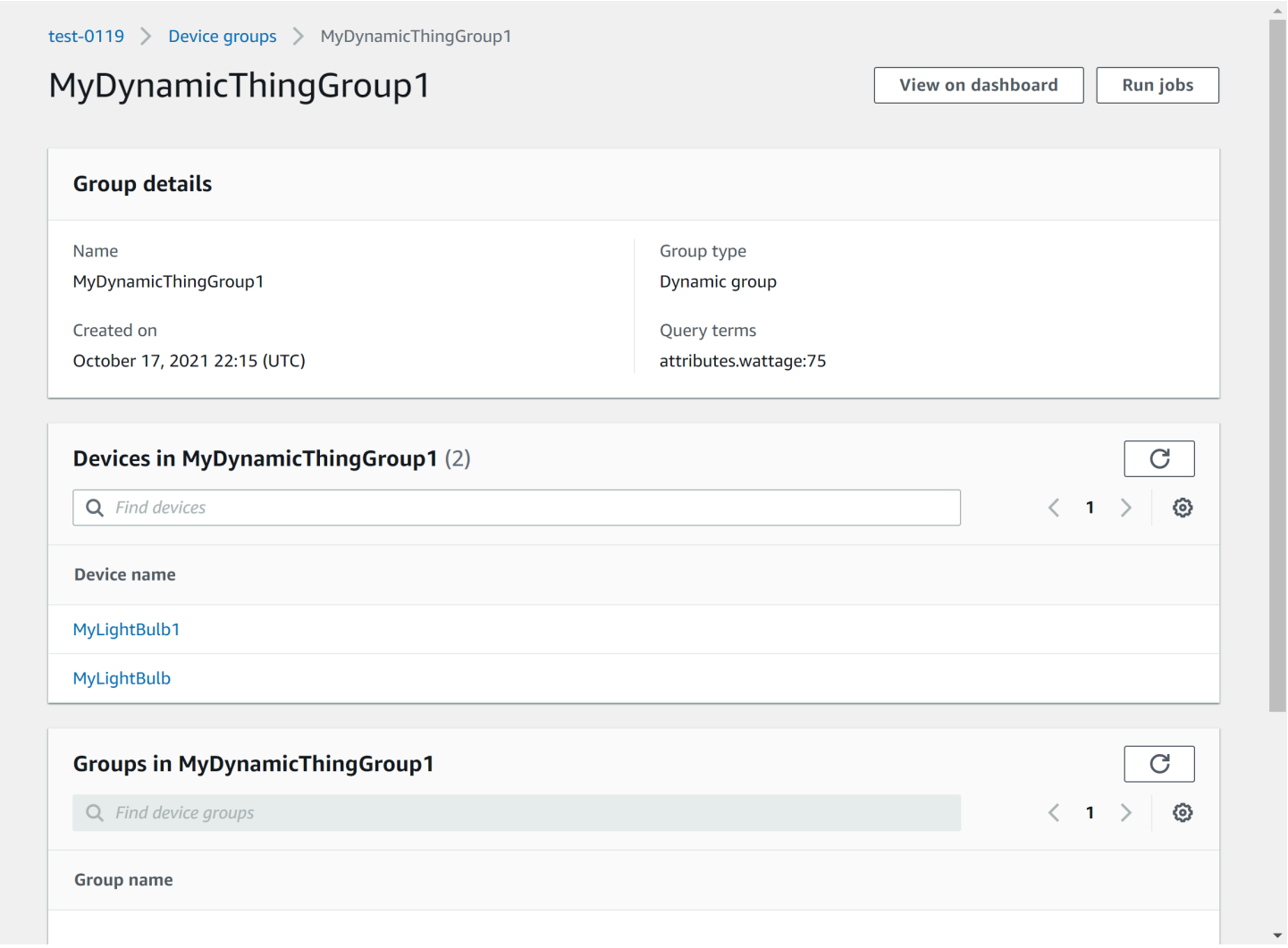
Grupos de dispositivos

Cuando inicie sesión en la aplicación web de Fleet Hub, verá la opción Grupos de dispositivos en el panel de navegación izquierdo. La página Grupos de dispositivos muestra todos los grupos de dispositivos en su aplicación web Fleet Hub. Para ver información sobre un grupo de dispositivos, seleccione un grupo específico en la columna Nombre del grupo.



Detalles de grupo de dispositivos

La página Detalles de grupo de dispositivos contiene información sobre el grupo de dispositivos seleccionado. Para ver los detalles de un dispositivo, elija un dispositivo específico en la columna Nombre del dispositivo, en la sección Dispositivos en ***XXX***.



Detalles del dispositivo

La página Detalles del dispositivo contiene información sobre el dispositivo seleccionado.

> **Note**
>
> Si su cliente utiliza un ID de cliente distinto al “Nombre del objeto” al conectarse a AWS IoT, la indexación de flotas no indexará el estado de conectividad del “objeto”.

Detalles

La sección Detalles contiene la siguiente información sobre el dispositivo:

- Nombre del dispositivo: el nombre del recurso u objeto que representa al dispositivo. Para obtener más información, consulte How to manage things with the registry.

- Tipo de objeto: el tipo de objeto asociado al dispositivo. Puede usar el tipo de objeto para almacenar información que sea común a todos los objetos del mismo tipo. Para obtener más información, consulte Thing types.

- Marca temporal de la última conexión: la marca de tiempo de la última vez que el dispositivo se haya conectado a AWS IoT.

- Enlace de dispositivo de uso compartido: un enlace que se puede compartir y que apunta a la página Detalles del dispositivo en el dispositivo seleccionado.

- Estado de última conexión: el estado de conexión del dispositivo a AWS IoT. Si el dispositivo está conectado, el valor será `true`. Si no está conectado, el valor será `false`.

- Motivo de la desconexión: el motivo por el que el dispositivo está desconectado.

Datos notificados

La sección Datos notificados contiene información sobre el registro del dispositivo, los datos de sombra de dispositivo y los grupos de objetos.

- Campos del dispositivo: los campos indexados de su dispositivo en la indexación de flotas de AWS IoT. Para obtener más información, consulte Administración de la indexación de flotas.

- Sombras de dispositivos: las sombras asociadas al dispositivo. Las sombras de dispositivos pueden incluir sombras clásicas sin nombre o sombras con nombre. Para obtener más información, consulte AWS IoT device shadow.

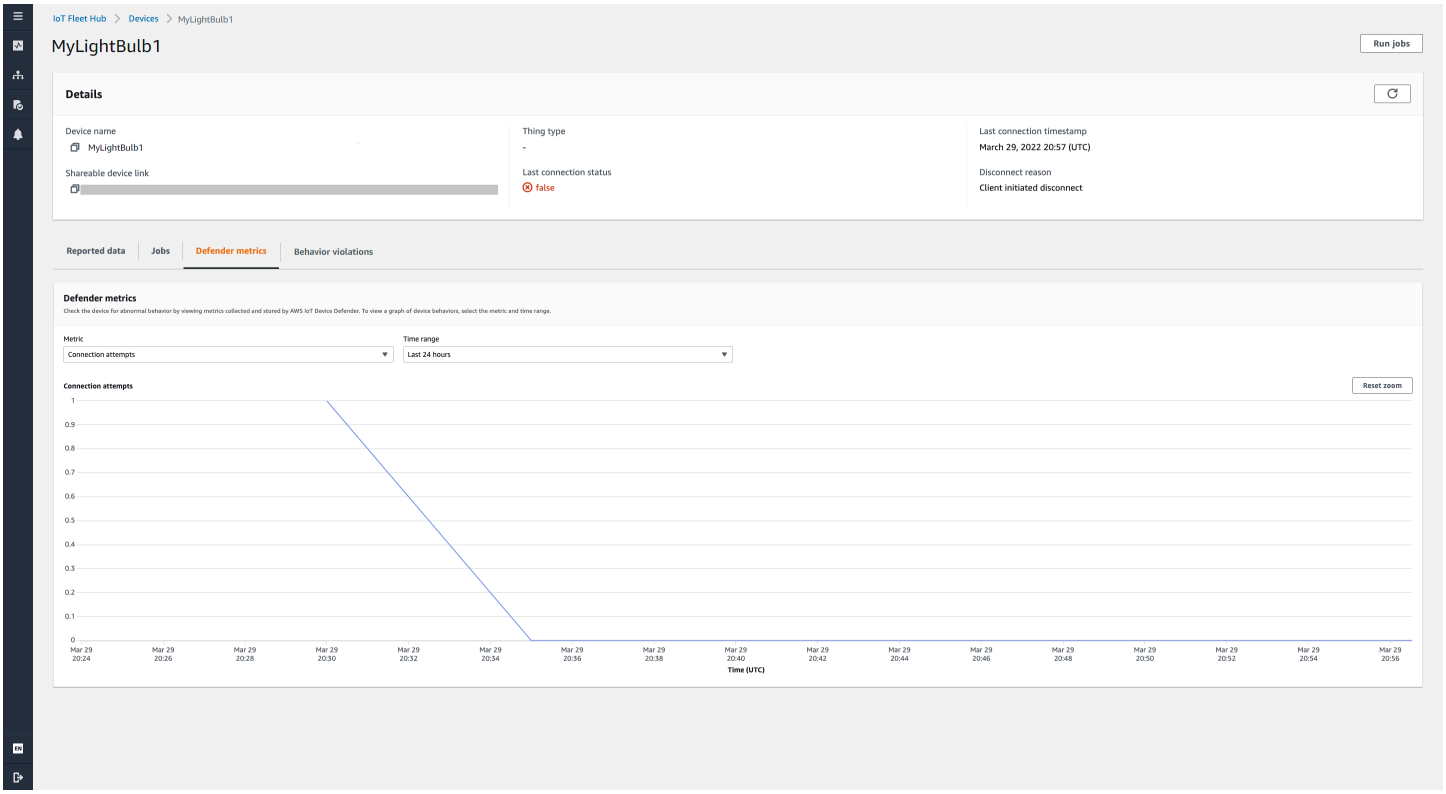
- Grupos de dispositivos: los grupos de dispositivos asociados a su dispositivo. Los grupos de dispositivos pueden incluir grupos de objetos estáticos y dinámicos. Para obtener más información, consulte Static thing groups y Dynamic thing groups.

Trabajos

La sección Trabajos muestra todos los trabajos que se están ejecutando en el dispositivo. Todos los trabajos tienen una página de detalles con información resumida sobre el trabajo, lo que incluye información sobre el destino y el tiempo de ejecución. Para obtener más información, consulte Working with jobs and job templates in Fleet Hub for AWS IoT Device Management y Jobs.

Métricas de Defender

La sección Métricas de Defender muestra las métricas de AWS IoT Device Defender asociadas al dispositivo seleccionado en ese momento. Puede usar los datos de métricas mostrados para ver el funcionamiento del dispositivo durante un periodo de tiempo que puede seleccionar. A fin de poder ver los datos de las métricas de Defender desde su aplicación Fleet Hub, el administrador de Fleet Hub deberá primero configurar las métricas de AWS IoT Device Defender asociadas al dispositivo seleccionado. Para obtener más información sobre cómo crear y configurar métricas de AWS IoT Device Defender para sus dispositivos, consulte Custom metrics, Device-side metrics y Cloud-side metrics.



Infracciones de comportamiento

La sección Infracciones de comportamiento muestra los datos indexados de infracciones de detección en AWS IoT Device Defender asociados al dispositivo seleccionado en ese momento. Los

datos de infracciones de comportamiento pueden incluir cosas como el recuento de infracciones, la hora de la última infracción o la métrica de la última infracción. Para ver los datos sobre infracciones de comportamiento de su aplicación Fleet Hub, el administrador de Fleet Hub debe configurar las infracciones de comportamiento de AWS IoT Device Defender en un perfil de seguridad y configurar las infracciones de AWS IoT Device Defender en la indexación de flotas. Para obtener más información sobre cómo configurar las infracciones de comportamiento en un perfil de seguridad de AWS IoT Device Defender, consulte AWS IoT Device Defender Detect. Para obtener más información sobre cómo configurar las infracciones de AWS IoT Device Defender, consulte Manage fleet indexing for Fleet Hub applications y Managing thing indexing.

Consultas y filtros

Puedes usar las consultas en Fleet Hub para AWS IoT Device Management a fin crear y ver listas de objetos en su flota de dispositivos. Todos los campos administrados por AWS, campos personalizados y atributos en los orígenes de datos indexados están disponibles como filtros para consultas. También puede crear campos personalizados a fin de activar la agregación para the section called “Alarmas” mediante la indexación de flotas de AWS IoT. Para obtener más información sobre la indexación de flotas, consulte Fleet indexing.

Temas

- Vista del panel
- Crear consultas con filtros

Vista del panel

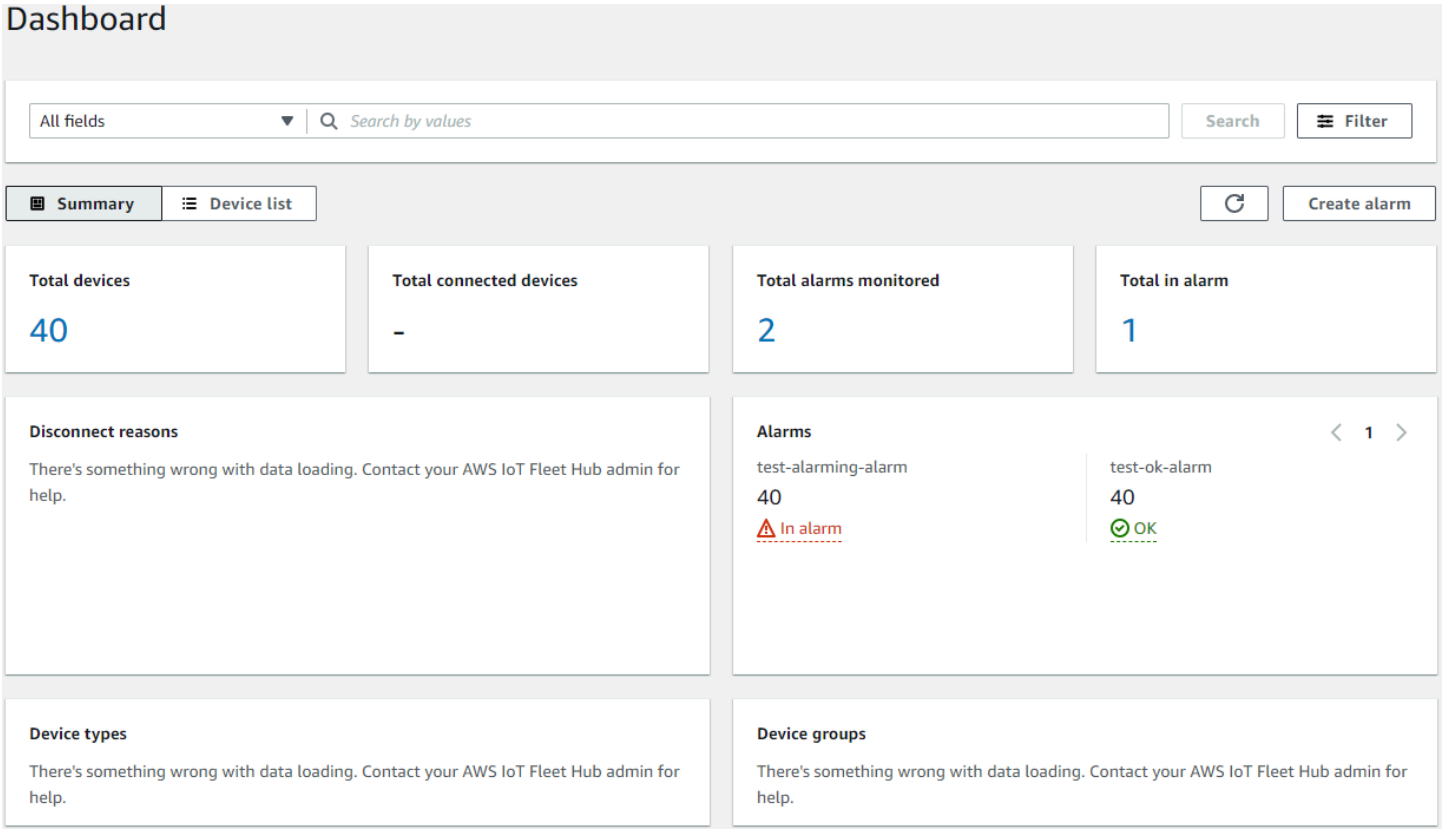
Cuando inicie sesión en la aplicación web Fleet Hub para AWS IoT Device Management, verá un panel con dos vistas de datos sobre los dispositivos de su flota.

Resumen

La vista Resumen ofrece una síntesis de los datos de todos los dispositivos de su flota. Proporciona la siguiente información.

- Número total de dispositivos.
- Número de dispositivos conectados.
- Una lista de los motivos por los que los dispositivos se han desconectado.

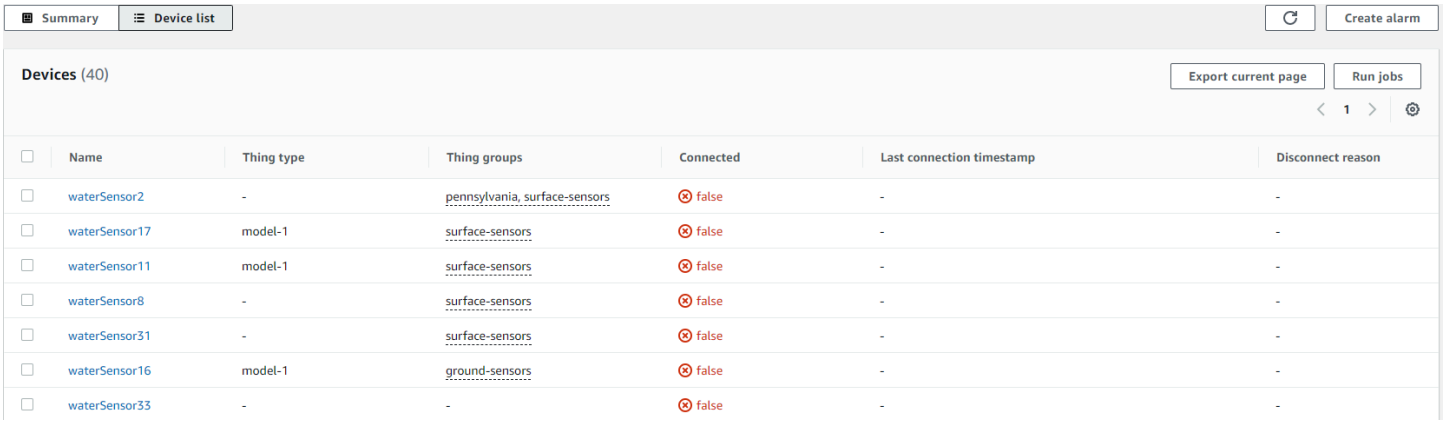
- Los tipos de objetos que ha creado para su flota y la cantidad de dispositivos para cada tipo.
- Los grupos de objetos que ha creado para su flota y la cantidad de dispositivos para cada grupo.



Lista de dispositivos

La vista Lista de dispositivos muestra una tabla con los dispositivos de su flota. La tabla proporciona la siguiente información para todos los dispositivos de la lista.

- El nombre del dispositivo
- El estado de conexión del dispositivo.
- La marca de tiempo de la última conexión del dispositivo.
- En el caso de un dispositivo que no está conectado, el motivo por el que se desconectó.
- El tipo de objeto del dispositivo.
- El grupo de objetos del dispositivo.
- Los campos personalizados que ha creado en el servicio de indexación de flotas.



Para descargar un archivo CSV que contenga los dispositivos que aparecen en la página (en la lista de dispositivos), seleccione Exportar página actual. Si se trata de una lista paginada, solo se descargarán los datos de la página actual, no los de las páginas siguientes.

Puede utilizar consultas y filtros para reducir el número de dispositivos que generan los datos resumidos en la primera vista y que aparecen en la lista de dispositivos. Para obtener más información sobre el uso de consultas y filtros a fin de obtener información más específica sobre los dispositivos de su flota, consulte the section called “Creación de consultas”.

Crear consultas con filtros

En este tema, se explica cómo funcionan las consultas en Fleet Hub para AWS IoT Device Management y se detallan los pasos necesarios para crear una consulta con filtros.

Mediante las consultas, puede controlar la cantidad y los tipos de dispositivos que aparecen en el panel, tanto en la lista de dispositivos como en el resumen. Puede filtrar las consultas mediante campos administrados por AWS, campos personalizados y cualquier atributo de los orígenes de datos indexados procedentes de la indexación de flotas de AWS IoT. Para obtener más información sobre la indexación de flotas, consulte Fleet indexing.

También puede agregar palabras clave a las consultas. Las palabras clave se aplican a todos los campos con capacidad de búsqueda. También se tienen en cuenta en el límite de tres filtros por consulta.

La siguiente sección describe los pasos necesarios para crear una consulta típica.

Creación de consultas

La siguiente sección describe cómo crear una consulta típica.

Requisitos previos

- Una aplicación de Fleet Hub vinculada a una cuenta AWS IoT Core que contenga varios dispositivos (objetos).
- Una cuenta con permisos para usar la aplicación Fleet Hub.

Creación de la primera consulta de Fleet Hub con un filtro en la consola

1. Vaya a su aplicación de Fleet Hub.
2. En el panel de control predeterminado, compruebe que puede ver la pestaña Lista de dispositivos y el número total de dispositivos (objetos) en la cuenta AWS IoT Core asociada.

   El panel de control predeterminado contiene pestañas de navegación, lo que incluye una para la lista de dispositivos. Muestra el número total de dispositivos en la cuenta AWS IoT Core asociada y el número total de dispositivos conectados.
3. En el panel de control predeterminado, seleccione la pestaña Lista de dispositivos. Compruebe que puede ver una lista con todos los dispositivos que contienen los atributos administrados y personalizados. Los atributos personalizados contienen el prefijo de atributos.

   De forma predeterminada, el panel de la lista de dispositivos muestra los atributos personalizados y administrados para todos los dispositivos de la cuenta AWS IoT Core asociada.
4. En la parte superior de la página, escriba la palabra clave que desee incluir en la consulta. Las consultas de palabras clave se aplican a todos los campos.
5. En la parte superior de la página, elija Filtro.
6. En el modal Filtro, en Campo, elija el campo que desea usar como filtro. En Operador, elija una opción. Por último, en Valor, elija el valor del campo que desee usar en el filtro.

   Puede agregar hasta tres filtros. Una consulta de palabras clave también se tiene en cuenta en este límite.
7. Para hacer la consulta, elija Aplicar filtros. El resultado mostrará todos los dispositivos que coincidan con su consulta.

Trabajos y plantillas de trabajo en Fleet Hub para AWS IoT Device Management

> **Note**
>
> La característica de plantillas de trabajo se encuentra en versión preliminar y puede experimentar cambios.

Un trabajo es una operación remota que se envía a uno o varios dispositivos conectados al AWS IoT y que se ejecuta en ellos. Por ejemplo, puede definir un trabajo que indique a un conjunto de dispositivos descargar e instalar actualizaciones de firmware y aplicaciones, reiniciar, rotar certificados o realizar operaciones remotas de solución de problemas. Puede ejecutar trabajos preconfigurados desde las aplicaciones web de Fleet Hub para AWS IoT Device Management. Los administradores de su organización crean plantillas de trabajo en la consola de AWS IoT y asocian políticas para que los usuarios de Fleet Hub tengan acceso a las plantillas. En su aplicación de Fleet Hub, debe especificar en qué dispositivo o grupo de dispositivos se ejecutará el trabajo.

Los administradores también crean grupos de dispositivos que usted puede ver en su aplicación. Para ver estos grupos, seleccione Grupos de dispositivos en el panel de navegación. Al especificar un grupo de dispositivos como destino, puede seleccionar uno de los dos siguientes tipos de opciones para la ejecución del trabajo.

- Captura: el trabajo se ejecuta una vez.
- Continuo: tras la ejecución inicial, el trabajo se ejecuta en cualquier dispositivo que se añada al grupo.

Para obtener más información sobre cómo crear y administrar plantillas de trabajo, consulte Job templates. Para obtener más información sobre cómo funcionan los trabajos, consulte Jobs.

Trabajos en ejecución

En una aplicación de Fleet Hub, se puede ejecutar un trabajo desde varias ubicaciones, pero es necesario seguir siempre los pasos enumerados a continuación.

1. Seleccione un grupo, un dispositivo o varios dispositivos como destino.
2. Elija Run job (Ejecutar trabajo).

3. En Selección de destino de trabajo, seleccione Continuo o Captura.
4. Seleccione una plantilla de trabajo. Compruebe que el texto en Resumen del trabajo describa el tipo de trabajo que desea ejecutar.
5. Introduzca un nombre para el trabajo (opcional).
6. Elija Run (Ejecutar).

Puede seleccionar destinos y seguir estos pasos desde las siguientes ubicaciones en su aplicación Fleet Hub.

- La pestaña con la lista de dispositivos en el panel de control.
- La página de detalles de un dispositivo específico.
- La página de grupos de dispositivos.
- La página de detalles de un grupo de dispositivos específico.

Ver y administrar trabajos

Puede ver los trabajos que se están ejecutando en su flota desde las siguientes ubicaciones.

- La página de la lista de trabajos: esta página muestra todos los trabajos en ejecución en su flota. Para ver esta página, seleccione Trabajos en el panel de navegación.
- La página de detalles de un dispositivo específico: esta página muestra todos los trabajos que se están ejecutando en el dispositivo.

Todos los trabajos tienen una página de detalles con información resumida sobre el trabajo, lo que incluye información sobre el destino y el tiempo de ejecución. Esta página muestra el estado de tiempo de ejecución del trabajo en cada dispositivo. También muestra los siguientes valores totales.

- Número de ejecuciones.
- Número de ejecuciones canceladas.
- Número de ejecuciones correctas.
- Número de ejecuciones con error.
- Número de ejecuciones rechazadas.
- Número de ejecuciones en cola.
- Número de ejecuciones en curso.

- Número de ejecuciones eliminadas.
- Número de ejecuciones fuera de plazo.

Para cancelar un trabajo, selecciónelo y escoja Cancelar.

Alarmas

En esta sección, se explica cómo funcionan las alarmas de Fleet Hub para AWS IoT Device Management, y se detallan los pasos necesarios para crear una alarma.

Cuando crea una alarma de Fleet Hub, esta se aplica a todos los dispositivos que aparezcan en ese momento en el panel de control. Si no hace ninguna consulta, la alarma se aplica a todos los dispositivos de la flota. Para obtener información sobre el panel y la creación de consultas, vaya a the section called “Consultas y filtros”.

Las alarmas utilizan las métricas de Amazon CloudWatch (CloudWatch) junto con campos de búsqueda del servicio de indexación de flotas AWS IoT para crear alarmas de CloudWatch. Por ejemplo, puede crear una alarma que genere un mensaje de Amazon Simple Notification Service (Amazon SNS) cada vez que el nivel medio de batería de los dispositivos de su flota caiga por debajo del 50 %.

Las alarmas de Fleet Hub utilizan las funciones GetStatistics y GetPercentiles del servicio de indexación de flotas para consultar datos agregados. Por ejemplo, cuando crea una alarma que rastrea un campo numérico personalizado, puede crear umbrales de alarma que se apliquen a los siguientes valores del atributo especificado.

- Máximo
- Recuento
- Sum
- Mínimo
- Media
- Valores de los percentiles 10, 50, 90, 95 o 99

Para obtener más información sobre la consulta de datos agregados en el servicio de indexación de flotas, consulte Querying for aggregate data.

En la siguiente tabla, se muestran algunos ejemplos de los tipos de agregación disponibles para los campos personalizados y administrados por AWS.

Campo	Tipo de agregación
Tipo de objeto (campo de cadena administrado por AWS)	Recuento
Grupo de objetos (campo de cadena administrado por AWS)	Recuento
Conectado (campo booleano administrado por AWS) El valor de `true` es 1. El valor de `false` es 0.	• Máximo • Recuento • Sum • Mínimo • Media
shadow.reported.batterylevel (campo de agregación numérica creado en el servicio de indexación de flotas)	• Máximo • Recuento • Sum • Mínimo • Media • p10 (percentil 10) • p50 (percentil 50) • p90 (percentil 90) • p95 (percentil 95) • p99 (percentil 99)

Además de especificar los campos y tipos de agregación, también debe especificar los siguientes valores.

- El tiempo (1 o 5 minutos) necesario para que el umbral de alarma especificado active la alarma.
- Uno de los siguientes operadores de comparación, para aplicarlo al campo y al tipo de agregación especificados.

  - Mayor
  - Mayor/igual
  - Menor
  - Menor/igual
- El valor que se va a utilizar con el operador de comparación especificado.
- Una lista de las direcciones de correo electrónico de las personas de su organización que reciben mensajes de Amazon SNS cada vez que se activa la alarma.
- Un nombre de alarma.

Para crear una alarma de Fleet Hub, consulte the section called “Creación de alarmas”.

Creación de alarmas

En este tema, se describen los pasos necesarios para crear una alarma en Fleet Hub para AWS IoT Device Management. En el tema, se da por sentado que el administrador ha creado un campo de agregación a partir de un campo de sombras de dispositivo denominado shadow.reported.batterylevel. Este campo personalizado indica el nivel de batería de un dispositivo. Debe pedirle a su administrador que cree campos personalizados con capacidad de búsqueda en el servicio de indexación de flotas de AWS IoT.

La alarma que cree enviará un mensaje de Amazon Simple Notification Service (Amazon SNS) a una lista de personas de su organización cuando el nivel medio de batería de los dispositivos de la flota caiga por debajo del 50 % durante un periodo de un minuto.

Creación de una consulta de Fleet Hub

1. Vaya a su aplicación de Fleet Hub.
2. Si quiere gestionar un conjunto específico de dispositivos, cree una consulta. Para obtener instrucciones sobre cómo crear una consulta sencilla, vaya a the section called “Crear consultas con filtros”. Si no crea una consulta, la alarma se aplicará a todos los dispositivos de la flota.
3. En la página del panel de control predeterminado, seleccione Crear alarma.
4. En la página Crear métrica de agregación, compruebe que la consulta se encuentre bajo Consulta de destino. En la sección Configurar la agregación de métricas de flota, en Elegir campo, seleccione shadow.reported.batterylevel. Este menú contiene los campos administrados por AWS y los campos personalizados que el administrador ha creado en el servicio de indexación de flotas AWS IoT.

5. En Elegir el tipo de agregación, seleccione Promedio. Esta opción hace que la alarma se base en el valor promedio del nivel de batería de la flota de dispositivos.
6. En Elegir periodo, seleccione 1 minuto. Con esta opción, la alarma se activará cuando la flota de dispositivos se encuentre en el estado de alarma especificado durante un minuto.

   Elija Siguiente.
7. En la página Establecer umbral, en la sección Activar la alarma siempre que..., seleccione Menor/igual. Con esta opción, la alarma se activará cuando el valor medio del nivel de batería caiga por debajo del valor que especifique.
8. En el cuadro de texto que, ponga 50.

   Elija Siguiente.
9. En la página Notificar al usuario, en la sección Notificar (opcional), introduzca un nombre para la lista de correo electrónico donde estarán los usuarios de la organización que recibirán notificaciones cuando la alarma se active. Introduzca una lista de direcciones de correo electrónico, separadas por comas.
10. En la sección Detalles de alarma, introduzca un nombre para la alarma y, si lo desea, una descripción. Elija Siguiente.
11. En la página Revisar, repase la información que ha introducido o seleccionado en las páginas anteriores. Elija Submit (Enviar). Con esto, volverá al panel predeterminado.
12. En el panel de control predeterminado, en el panel de navegación izquierdo, seleccione Alarmas de Fleet Hub. Compruebe que puede ver la alarma que ha creado.

Solución de problemas

En esta sección, encontrará información relacionada con la resolución de problemas como usuario de Fleet Hub.

Síntoma	Solución
No puedo añadir más filtros ni términos en mi consulta.	Compruebe si ha alcanzado el límite de cuatro términos y filtros de consulta.
Hay una métrica personalizada que no logro encontrar.	Pídale a su administrador que cree la métrica en el servicio de indexación de flotas.

Síntoma	Solución
Mi alarma no muestra ningún dato.	Los datos de alarma tardan unos minutos en cargarse.
Necesito cambiar los dispositivos a los que se dirige mi alarma.	Vaya al panel de control y cambie la consulta.
Aparece un error cuando cambio la región en el panel de control.	Pídale a su administrador que compruebe si se ha activado la indexación de la flotas en la región seleccionada.
El estado de conectividad de mi “objeto” no está indexado en la indexación de flotas.	El cliente debe utilizar el mismo ID de cliente que “Nombre del objeto” al conectarse a AWS IoT. Si su cliente utiliza un ID distinto al “Nombre del objeto” al conectarse a AWS IoT, la indexación de flotas no indexará el estado de conectividad del “objeto”.

Supervisión de Fleet Hub para AWS IoT Device Management

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Fleet Hub y de las demás soluciones de AWS. AWS ofrece las siguientes herramientas de monitorización para supervisar Fleet Hub, para informar cuando algo no va bien y para tomar medidas automáticamente cuando proceda.

- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Registro de las llamadas a la API de Fleet Hub para AWS IoT Device Management con AWS CloudTrail

Fleet Hub para AWS IoT Device Management está integrado en AWS CloudTrail. El servicio CloudTrail proporciona un registro de las acciones que lleva a cabo un usuario, un rol o un servicio de AWS en Fleet Hub. CloudTrail captura las llamadas a la API para Fleet Hub como eventos. Las llamadas capturadas incluyen las realizadas desde la consola Fleet Hub y las llamadas de código a las operaciones de API de Fleet Hub.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, lo que incluye los eventos para Fleet Hub. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos.

Mediante la información que CloudTrail recopila, puede determinar la solicitud que se envió a Fleet Hub, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó, etc.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Fleet Hub en CloudTrail

AWS CloudTrail se habilita en una cuenta de AWS al crearla. Cuando hay una actividad en Fleet Hub, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en su cuenta de AWS, lo que incluye los eventos de Fleet Hub, cree un registro de seguimiento. Un seguimiento habilita a CloudTrail a enviar archivos de registro a un bucket de Amazon Simple Storage Service (Amazon S3). De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado.

También puede configurar otros servicios de AWS para analizar y actuar según los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte lo siguiente:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de Fleet Hub. Estas acciones se encuentran en la documentación de referencia de las API de AWS IoT. Por ejemplo, las llamadas a las acciones `CreateApplication` y `UpdateApplication` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del nodo raíz o del usuario de AWS Identity and Access Management.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado

- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro en Fleet Hub para AWS IoT Device Management

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique.

Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc.

Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Example

La siguiente entrada de registro de CloudTrail muestra información sobre la acción `CreateApplication`.


```
{
    "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"
    }
```

Seguridad en Fleet Hub para la gestión de dispositivos AWS IoT

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a Fleet Hub, consulte AWS Servicios incluidos .AWS
- Seguridad en la nube: tu responsabilidad viene determinada por el AWS servicio que utilices. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Fleet Hub para la administración de AWS IoT dispositivos. En los siguientes temas, se le mostrará cómo configurar Fleet Hub para satisfacer sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a monitorear y proteger los recursos de Fleet Hub.

Temas

Protección de datos en Fleet Hub

El modelo de se aplica a protección de datos en Fleet Hub para la gestión de AWS IoT dispositivos. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Fleet Hub u otro dispositivo Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los

registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Fleet Hub protege los datos en reposo mediante el cifrado del servidor. Para obtener más información, consulte Cifrado de datos en AWS IoT, en la Guía para desarrolladores de AWS IoT .

Cifrado en tránsito

En las implementaciones de flujos en la nube, Fleet Hub protege los datos en tránsito mediante el protocolo de seguridad de la capa de transporte (TLS). Para obtener más información, consulte Seguridad de transporte en AWS IoT, en la Guía para desarrolladores de AWS IoT .

Identity and Access Management para Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Fleet Hub. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Fleet Hub.

Usuario de servicio: si utiliza el servicio de Fleet Hub para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Fleet Hub para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Fleet Hub, consulte Solución de problemas de Fleet Hub for AWS IoT Device Management identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Fleet Hub en su empresa, probablemente tenga acceso completo a Fleet Hub. Su trabajo consiste en determinar a qué características y recursos de Fleet Hub deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Fleet Hub, consulte ¿Cómo Fleet Hub for AWS IoT Device Management funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Fleet Hub. Para consultar ejemplos de políticas basadas en la identidad de Fleet Hub que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management.

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo Fleet Hub for AWS IoT Device Management funciona con IAM

Antes de utilizar IAM para administrar el acceso a Fleet Hub, descubra qué características de IAM se pueden utilizar con Fleet Hub.

Funciones de IAM que puede utilizar con Fleet Hub for AWS IoT Device Management

Característica de IAM	Soporte para Fleet Hub
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una visión general de cómo funcionan Fleet Hub y otros AWS servicios con la mayoría de las funciones de IAM, consulta AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades para Fleet Hub

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de Fleet Hub

Para ver ejemplos de políticas basadas en identidades de Fleet Hub, consulte Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management.

Políticas basadas en recursos dentro de Fleet Hub

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas para Fleet Hub

> **Note**
>
> Las aplicaciones de Fleet Hub utilizan la política administrada `AWSIoTFleetHubFederationAccess`. Para obtener más información, consulte ???.

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Fleet Hub, consulte Acciones definidas por Fleet Hub for AWS IoT Device Management en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Fleet Hub utilizan el siguiente prefijo antes de la acción:

```
iotfleethub
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en identidades de Fleet Hub, consulte Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management.

Recursos de políticas para Fleet Hub

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Fleet Hub y sus ARN, consulte Recursos definidos por Fleet Hub for AWS IoT Device Management en la Referencia de autorizaciones de servicio.

Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Fleet Hub for AWS IoT Device Management.

Para ver ejemplos de políticas basadas en identidades de Fleet Hub, consulte Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management.

Claves de condición de políticas para Fleet Hub

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Fleet Hub, consulte Claves de condición para Fleet Hub for AWS IoT Device Management en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Fleet Hub for AWS IoT Device Management.

Para ver ejemplos de políticas basadas en identidades de Fleet Hub, consulte Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management.

Listas de control de acceso (ACL) en Fleet Hub

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con Fleet Hub

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Fleet Hub

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios para Fleet Hub

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Fleet Hub

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Fleet Hub. Edite los roles de servicio solo cuando Fleet Hub proporcione orientación para hacerlo.

Roles vinculado a servicios para Fleet Hub

Compatible con roles vinculados al servicio	No

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para Fleet Hub for AWS IoT Device Management

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Fleet Hub. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas

de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Fleet Hub, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para Fleet Hub for AWS IoT Device Management en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola Fleet Hub
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Fleet Hub de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola Fleet Hub

Para acceder a la Fleet Hub for AWS IoT Device Management consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Fleet Hub que tiene en su poder Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Fleet Hub, adjunta también el Fleet Hub `ConsoleAccess` o la política `ReadOnly` AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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

```
}
```

Solución de problemas de Fleet Hub for AWS IoT Device Management identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Fleet Hub e IAM.

Temas

- No tengo autorización para realizar una acción en Fleet Hub
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Fleet Hub

No tengo autorización para realizar una acción en Fleet Hub

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

> **Note**
>
> Las aplicaciones de Fleet Hub utilizan la política administrada `AWSIoTFleetHubFederationAccess`. Para obtener más información, consulte ???.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `iotfleethub:`*`GetWidget`*.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `iotfleethub:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Fleet Hub.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Fleet Hub. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Fleet Hub

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Fleet Hub admite estas características, consulte ¿Cómo Fleet Hub for AWS IoT Device Management funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un usuario de IAM en otro de tu Cuenta de AWS propiedad en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación del cumplimiento de Fleet Hub para la gestión de dispositivos AWS IoT

Los auditores externos evalúan la seguridad y el cumplimiento de Fleet Hub como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para saber si un programa de cumplimiento Servicio de AWS se encuentra dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden crear aplicaciones aptas para AWS la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

La resiliencia de Fleet Hub para la gestión de AWS IoT dispositivos

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor

disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

AWS políticas gestionadas para Fleet Hub para la gestión de AWS IoT dispositivos

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política de ReadOnlyacceso AWS gestionado proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSIoTFleetHubFederationAccess

Puede adjuntar la política `AWSIoTFleetHubFederationAccess` a las identidades de IAM.

Esta política otorga a los usuarios federados de Fleet Hub for AWS IoT Device Management los permisos que necesitan para realizar acciones AWS IoT y otros AWS servicios desde las aplicaciones web de Fleet Hub.

Para obtener información sobre cómo añadir usuarios a las aplicaciones web de Fleet Hub, consulte ???.

Puede ver esta política en la Console de AWS.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `iot`- Recupera los datos AWS IoT del dispositivo y realiza acciones a nivel de flota.
- `iotfleethub`: recupera los metadatos de aplicaciones de Fleet Hub.
- `cloudwatch`- Recupere datos CloudWatch de alarmas y métricas. también permite crear y eliminar acciones relacionadas con las alarmas de Fleet Hub.
- `sns`: realiza operaciones de creación, lectura, eliminación, suscripción y cancelación de la suscripción en operaciones; estas operaciones se centran en los temas de SNS de Fleet Hub.

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

Fleet Hub actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Fleet Hub desde que este servicio comenzó a rastrear estos cambios. Para obtener más información, consulte la página de historial de documentos de Fleet Hub.

Cambio	Descripción	Fecha
AWSIoTFleetHubFederationAccess: actualización de una política actual	Fleet Hub añadió nuevos permisos para que los usuarios de la aplicación puedan recuperar datos de métricas AWS IoT Device Defender en las aplicaciones de Fleet Hub.	4 de abril de 2022
AWSIoTFleetHubFederationAccess: actualización de una política actual	Fleet Hub añadió nuevos permisos para que los usuarios de la aplicación puedan recuperar orígenes de datos adicionales para la indexación. También se añade un permiso para permitir a los usuarios de la aplicación cancelar la ejecución de un	15 de noviembre de 2021

Cambio	Descripción	Fecha
	AWS IoT trabajo dentro de la aplicación.	
AWSIoTFleetHubFederationAccess: actualización de una política actual	Fleet Hub ha añadido nuevos permisos para que los usuarios de la aplicación puedan recuperar datos de Thing Group y realizar operaciones CRUD en los AWS IoT trabajos.	24 de mayo de 2021
AWSIoTFleetHubFederationAccess: actualización de una política actual	Fleet Hub eliminó los permisos para las API del panel de control de Fleet Hub que no eran compatibles.	12 de abril de 2021
AWSIoTFleetHubFederationAccess: política nueva	Fleet Hub agregó una nueva política que otorga los permisos necesarios para que los usuarios de la aplicación Fleet Hub recuperen los datos del dispositivo y realicen AWS IoT acciones.	12 de abril de 2021
Fleet Hub comenzó a hacer el seguimiento de los cambios	Fleet Hub comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	12 de abril de 2021

Seguridad de la infraestructura en Fleet Hub para la administración de AWS IoT dispositivos

Como servicio gestionado, Fleet Hub for AWS IoT Device Management está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a Fleet Hub a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Nosotros recomendamos TLS 1.3. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Para limitar los permisos que Fleet Hub otorga a otro servicio en el recurso, recomendamos utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos. Si se utilizan ambas claves contextuales de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo del recurso. En el caso de Fleet Hub, su `aws:SourceArn` debe ajustarse al formato `arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Asegúrese de que la *`región`* coincida con su región de Fleet Hub y que el *`account-id`* coincida con el ID de su cuenta de cliente.

El siguiente ejemplo muestra cómo evitar el problema del suplente confuso utilizando las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en la política de

confianza de rol de Fleet Hub. Para encontrar el ARN de su rol de Fleet Hub, vaya a la sección Fleet Hub de la AWS IoT consola y seleccione su aplicación Fleet Hub para ver la página de detalles de la solicitud.

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

Historial de revisión

En la tabla siguiente, se describen las actualizaciones de la documentación de Fleet Hub. Para ver los cambios en las políticas administradas de AWS para Fleet Hub, consulte AWS managed policies for Fleet Hub for AWS IoT Device Management.

Cambio	Descripción	Fecha
Versión de disponibilidad general de Fleet Hub para AWS IoT Device Management	Se actualizó el contenido para reflejar las mejoras introducidas en Fleet Hub para AWS IoT Device Management durante el periodo de versión preliminar.	25 de mayo de 2021.
Versión preliminar de Fleet Hub par AWS IoT Device Management	Se publicó la versión preliminar de la Guía del usuario de Fleet Hub para AWS IoT Device Management.	16 de diciembre de 2020.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.