



Guia do Fleet Hub para gerenciamento de AWS IoT dispositivos

# Fleet Hub para gerenciamento de AWS IoT dispositivos



# Fleet Hub para gerenciamento de AWS IoT dispositivos: Guia do Fleet Hub para gerenciamento de AWS IoT dispositivos

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

---

# Table of Contents

O que é o Fleet Hub for AWS IoT Device Management? .....	1
Como o Fleet Hub for AWS IoT Device Management funciona .....	1
Como funciona a indexação de dados do Fleet Hub .....	2
Como funcionam os alarmes do Fleet Hub .....	2
Como funcionam os trabalhos do Fleet Hub .....	2
Fleet Hub para gerenciamento de AWS IoT dispositivos para administradores .....	4
Conceitos básicos .....	4
Crie seu primeiro aplicativo Fleet Hub .....	4
Gerencie a indexação de frota para aplicativos Fleet Hub .....	7
Adicionar usuários aos aplicativos Fleet Hub .....	8
Os serviços AWS e AWS IoT Core que interagem com o Fleet Hub for AWS IoT Device Management .....	8
Solução de problemas .....	10
Fleet Hub for AWS IoT Device Management para usuários .....	12
Conceitos básicos .....	12
Crie sua primeira consulta .....	12
Crie seu primeiro alarme .....	13
Visualizar detalhes do dispositivo .....	16
Consultas e filtros .....	21
Visualizar o painel .....	21
Crie consultas com filtros .....	23
Trabalhando com trabalhos e modelos de trabalho no Fleet Hub for Device Management AWS IoT .....	24
Execução de trabalhos .....	25
Visualizando e gerenciando trabalhos .....	26
Alarmes .....	26
Criar alarmes .....	29
Solução de problemas .....	30
Monitoramento do Fleet Hub para o AWS IoT Device Management .....	32
Registrando o Fleet Hub para chamadas de API de gerenciamento de AWS IoT dispositivos com AWS CloudTrail .....	32
Informações do Fleet Hub no CloudTrail .....	33
Noções básicas sobre entradas do arquivo de log do Fleet Hub for AWS IoT Device Management .....	34

---

Segurança .....	36
Proteção de dados .....	37
Criptografia em repouso .....	38
Criptografia em trânsito .....	38
Identity and Access Management .....	38
Público .....	38
Autenticando com identidades .....	39
Gerenciando acesso usando políticas .....	43
Como Fleet Hub for AWS IoT Device Management funciona com o IAM .....	45
Exemplos de políticas baseadas em identidade .....	53
Solução de problemas .....	56
Validação de conformidade .....	58
Resiliência .....	59
AWS políticas gerenciadas .....	60
AWSIoT FleetHub Federation Access .....	61
Atualizações da política .....	63
Segurança da infraestrutura .....	64
Prevenção contra o ataque do “substituto confuso” em todos os serviços .....	65
Histórico de documentação .....	67
.....	lxviii

# O que é o Fleet Hub for AWS IoT Device Management?

Com o Fleet Hub for AWS IoT Device Management (Fleet Hub), você pode criar aplicativos web autônomos para monitorar a integridade de suas frotas de dispositivos. Você pode disponibilizar esses aplicativos para os usuários da sua organização, mesmo que eles não tenham contas AWS. Use o Fleet Hub para gerenciar tarefas comuns de toda a frota, como investigar e corrigir problemas operacionais e de segurança.

O Fleet Hub oferece os seguintes recursos.

- Monitore frotas de dispositivos praticamente em tempo real.
- Defina alertas para notificar seus técnicos sobre comportamentos incomuns.
- Execução de trabalhos.

## Note

Para que o Fleet Hub indexe dados de status de conectividade, suas objetos devem se conectar a AWS IoT Core com um ID de cliente igual ao nome do objeto.

## Como o Fleet Hub for AWS IoT Device Management funciona

Os administradores podem usar o Fleet Hub for AWS IoT Device Management para criar aplicativos web seguros em alguns minutos sem provisionar nenhum recurso ou escrever nenhum código. Os aplicativos Web que você cria usando o Fleet Hub se integram aos seus sistemas de identidade existentes, como o Active Directory. Isso permite que seus administradores apliquem seus próprios modelos de autenticação e autorização.

Os aplicativos web do Fleet Hub se integram com o AWS IoT Core à indexação da frota e ao monitoramento de dispositivos. Essas integrações oferecem a capacidade de monitorar os dados de integridade do dispositivo e criar alarmes quando os dispositivos da sua frota atingem um estado especificado.

Os aplicativos do Fleet Hub usam a política gerenciada `AWSIoT FleetHub Federation Access`. Para obter mais informações, consulte [???](#).

Exemplo de casos de uso:

- Visualize problemas de conectividade do dispositivo - Você pode ver o número de dispositivos desconectados em sua frota, o status da última conexão de um dispositivo e o motivo ou motivos pelos quais os dispositivos foram desconectados.
- Definir alarmes - Você pode definir limites que acionam alarmes quando um determinado número de dispositivos se desconecta. Os alarmes também podem notificá-lo quando um dispositivo ou dispositivos se desconectam por um motivo específico. Em seguida, você pode examinar os dados detalhados do dispositivo para investigar e solucionar problemas.
- Executar trabalhos - Você pode executar operações remotas (como atualizações de firmware) em um ou mais dispositivos.

## Como funciona a indexação de dados do Fleet Hub

Você pode usar o console do Fleet Hub para ativar a indexação de frota para sua frota de dispositivos. Ao ativar a indexação da frota no Fleet Hub, você a ativa para toda a frota e a disponibiliza para todos os aplicativos do Fleet Hub.

Quando habilitada, a indexação de frota indexa automaticamente todos os campos gerenciados por AWS IoT Core. Você também pode usar a indexação de frota para adicionar dados personalizados que podem ser usados para consultar e agregar dados nos aplicativos do Fleet Hub.

## Como funcionam os alarmes do Fleet Hub

Os aplicativos da web Fleet Hub fornecem uma interface que permite aos usuários criar alarmes. As etapas a seguir mostram como os usuários criam alarmes no Fleet Hub.

1. Crie uma consulta para agregar dados: especifique uma consulta que agregue os dispositivos que seus usuários desejam atingir usando campos pesquisáveis.
2. Configurar limite - Defina um limite que acione os alarmes quando uma condição nos dados indexados (como status de conectividade em um intervalo especificado) for atingida.
3. Configurar notificação - Especifique um grupo de destinatários que o Fleet Hub notifica quando os dispositivos especificados estão em alarme.

## Como funcionam os trabalhos do Fleet Hub

Você pode usar o console do Fleet Hub para executar operações remotas em dispositivos.

Quando os modelos de trabalho estão habilitados, você pode criar trabalhos específicos a partir dos modelos em seus aplicativos do Fleet Hub.

# Fleet Hub para gerenciamento de AWS IoT dispositivos para administradores

Esta seção contém orientações para administradores sobre como criar e gerenciar o Fleet Hub para aplicativos web de gerenciamento de AWS IoT dispositivos.

## Tópicos

- [Conceitos básicos](#)
- [Os serviços AWS e AWS IoT Core que interagem com o Fleet Hub for AWS IoT Device Management](#)
- [Solução de problemas](#)

## Conceitos básicos

Esta seção explica como criar e configurar o Fleet Hub para aplicativos web de gerenciamento de AWS IoT dispositivos.

## Tópicos

- [Crie seu primeiro aplicativo Fleet Hub](#)
- [Gerencie a indexação de frota para aplicativos Fleet Hub](#)
- [Adicionar usuários aos aplicativos Fleet Hub](#)

## Crie seu primeiro aplicativo Fleet Hub

### Pré-requisitos

A lista a seguir contém os recursos necessários para criar um aplicativo web do Fleet Hub.

- Uma [conta da AWS](#).
- [AWS IAM Identity Center](#) ativado em sua conta. (Se você ainda não ativou esse serviço, o console AWS IoT Core (<https://console.aws.amazon.com/iot/>) solicitará que você faça isso.)

## Crie seu primeiro aplicativo da web Fleet Hub

As etapas a seguir descrevem como criar o Fleet Hub para aplicativos web de gerenciamento de AWS IoT dispositivos.

1. Navegue até o AWS IoT Core console (<https://console.aws.amazon.com/iot/>) e, no painel esquerdo, escolha Fleet Hub e, em seguida, Aplicativos.
2. Na página Aplicações, escolha Criar aplicação.
3. Na página Configurar o IAM Identity Center, se você não tiver ativado AWS IAM Identity Center (IAM Identity Center), siga as etapas para ativá-lo. AWS As organizações enviam um e-mail para você. Escolha o link no e-mail para concluir a ativação do IAM Identity Center.

 Note

Você pode conectar seu próprio provedor de identidade ao Centro de Identidade do IAM. Para obter mais informações, consulte [O que é AWS IAM Identity Center?](#) e [Conecte-se ao seu provedor de identidade externo](#).

Ao criar um aplicativo do Fleet Hub, você deve criar uma instância organizacional do IAM Identity Center, caso ainda não tenha uma. O aplicativo Fleet Hub que você cria também deve estar na mesma Região da AWS instância organizacional do IAM Identity Center. Para obter mais informações, consulte [Habilitar instâncias do IAM Identity Center e Organization do IAM Identity Center](#).

A página informa se você já ativou o IAM Identity Center.

Escolha Próximo.

4. Na página de AWS IoT dados do índice, revise as informações na seção Como o fluxo de dados funciona do AWS IoT Fleet Hub. Essa página o vincula às páginas do AWS IoT Core console nas quais você pode ativar e gerenciar a indexação AWS IoT Core da frota. Você pode usar esse serviço para indexar, pesquisar e agregar dados de registro, dados de sombra, dados de conectividade de dispositivos (eventos de ciclo de vida de dispositivos) e dados de violações de dispositivos. Você também pode criar campos personalizados além dos campos gerenciados que agrupam AWS IoT Core índices de indexação por padrão.
  - Se você ativou a indexação de frota, esta página exibirá as configurações de indexação de frota e os campos personalizados.

- Se você não tiver habilitado a indexação e a conectividade de objetos, deverá fazê-lo para usar o Fleet Hub.

Quando terminar de gerenciar e revisar as configurações de indexação da frota, escolha Próximo.

Para obter mais informações sobre como ativar a indexação de frota para aplicativos do Fleet Hub, consulte [Gerenciando a indexação de frota para aplicativos do Fleet Hub](#).

5. Na página Configurar aplicativo, na seção Função do aplicativo, crie um novo perfil de serviço ou selecione um perfil de serviço existente. Seu aplicativo da web Fleet Hub assume essa função quando usa recursos do Fleet Hub. Os usuários federados têm as mesmas permissões da função quando usam o aplicativo web.

- Se você criar uma nova função, o nome da função deve começar com a seguinte string: `AWSIoT FleetHub_ random_string`.
- Se você selecionar uma função existente, verifique se ela tem as permissões que estão no documento de política. Para ver as permissões que seu aplicativo web do Fleet Hub precisa, escolha Visualizar detalhes da função. É aberta uma janela que mostra o documento de política que o serviço aplica a qualquer nova função criada nessa página.

6. Na página Configure application (Configurar aplicativo), na seção Propriedades da aplicação, insira um nome para o seu aplicativo. Opcionalmente, você também pode inserir uma descrição da aplicação.

Escolha Criar aplicação.

7. Na página Aplicações, escolha o aplicativo criado e selecione Exibir detalhes. Analise os detalhes da aplicação.

#### Note

Para obter mais informações sobre possíveis soluções para resolver problemas como administrador do Fleet Hub, consulte [Solução de problemas](#).

## Gerencie a indexação de frota para aplicativos Fleet Hub

Você pode usar o AWS IoT Core console ou o AWS CLI para ativar a indexação da frota e configurar as seguintes fontes de dados para indexação: dados de [AWS IoT registro, dados do AWS IoT Device Shadow](#), dados de [AWS IoT conectividade](#) e dados de [AWS IoT Device Defender violações](#). As etapas a seguir descrevem como ativar a indexação de frotas do Fleet Hub para aplicativos de gerenciamento de AWS IoT dispositivos no AWS IoT Core console. Para ver as etapas de uso AWS CLI, consulte [Gerenciando a indexação](#) de itens.

### Important

20 de julho de 2022 é a versão de disponibilidade geral da integração da indexação de frotas de gerenciamento de AWS IoT dispositivos com sombras AWS IoT Core nomeadas e AWS IoT Device Defender detecção de violações. Com esta versão do GA, é possível indexar sombras nomeadas específicas especificando nomes das sombras. Caso tenha adicionado suas sombras nomeadas para indexação durante o período de pré-visualização pública desse atributo, de 30 de novembro de 2021 a 19 de julho de 2022, recomendamos que você reconfigure suas definições de indexação de frotas e escolha nomes de sombra específicos para reduzir o custo de indexação e otimizar o desempenho. Para obter mais informações sobre como redefinir as configurações de indexação da frota, consulte [Gerenciando a indexação da frota](#).

1. Navegue até o AWS IoT Core console (<https://console.aws.amazon.com/iot/>) e, no painel esquerdo, escolha Configurações.
2. Na página Configurações, navegue até a seção Indexação de frota e escolha Gerenciar indexação.
3. Na página Gerenciar indexação de frotas, na seção Configuração, escolha Indexação de itens e as fontes de dados que você deseja AWS IoT indexar. Você deve ativar a indexação e a conectividade de objetos para usar o Fleet Hub.
4. (Opcional) Na página Gerenciar indexação da frota, na seção Campos personalizados para agregação - opcional, crie campos personalizados além dos campos gerenciados que a indexação da frota indexa por padrão.

Quando terminar de gerenciar e revisar as configurações de indexação da frota, escolha Próximo.

Pode levar alguns minutos para que a indexação da frota atualize as configurações. Para obter mais informações sobre como gerenciar a indexação de frota, consulte [Gerenciando a indexação de frota](#).

## Adicionar usuários aos aplicativos Fleet Hub

Seu aplicativo web Fleet Hub for AWS IoT Device Management não contém nenhum usuário quando é recém-criado. Você deve adicionar usuários antes que você e os membros da sua organização possam usar o aplicativo. As etapas deste tópico descrevem como adicionar usuários ao seu aplicativo.

Você adiciona usuários do seu sistema de identidade existente configurando AWS IAM Identity Center (IAM Identity Center) para sua conta. Você pode conectar seu próprio provedor de identidade ao Centro de Identidade do IAM. Para obter mais informações, consulte [O que é o IAM Identity Center?](#).

1. Na página Aplicações, escolha sua aplicação web na lista de aplicações do Fleet Hub. Escolha Exibir detalhes.
2. Na página de detalhes da aplicação, selecione Adicionar usuário.
3. Na janela Adicionar usuários do Fleet Hub, selecione os usuários da sua organização que você deseja que tenham acesso ao aplicativo. Escolha Adicionar usuários selecionados.
4. Na página de detalhes da aplicação, verifique se você vê os usuários selecionados na lista de usuários do Fleet Hub.

## Os serviços AWS e AWS IoT Core que interagem com o Fleet Hub for AWS IoT Device Management

Este tópico explica como os recursos do Fleet Hub for AWS IoT Device Management interagem com outros serviços AWS para fornecer os recursos em seus aplicativos web do Fleet Hub.

A tabela a seguir indica quais serviços AWS o Fleet Hub for AWS IoT Device Management usa para implementar cada atributo.

Recurso	Serviço da AWS	Descrição
Integre sistemas de identidade e existentes, como o Active Directory.	AWS IAM Identity Center (Centro de Identidade do IAM)	<p>Você adiciona usuários do seu sistema de identidade e existente configurando AWS IAM Identity Center (Centro de Identidade do IAM) para sua conta. Você pode conectar seu próprio provedor de identidade ao Centro de Identidade do IAM.</p> <p>Para obter mais informações, consulte <a href="#">O que é AWS IAM Identity Center?</a> e <a href="#">Identidades da força de trabalho</a>.</p>
Crie consultas usando campos gerenciados pela AWS, campos personalizados e quaisquer atributos em suas fontes de dados indexadas.	Indexação de frotas da AWS IoT	<p>Use o serviço de indexação de frota para indexar, pesquisar e agregar dados de registro, dados de sombra e dados de conectividade de dispositivos (eventos de ciclo de vida do dispositivo). Você também pode criar campos personalizados para agregação, além dos campos gerenciados que a indexação de frota AWS IoT indexa por padrão.</p> <p>Para ver mais informações sobre indexação de frota, consulte <a href="#">Indexação de frota</a>.</p>
Crie alarmes para um conjunto de dispositivos especificados por uma consulta.	Amazon CloudWatch (CloudWatch)	Os painéis do Fleet Hub expõem métricas do CloudWatch que você pode

Recurso	Serviço da AWS	Descrição
		<p>usar em combinação com campos pesquisáveis para criar limites alarmantes. Por exemplo, é possível criar um alarme do CloudWatch que gera uma notificação do Amazon Simple Notification Service (Amazon SNS) sempre que o número de dispositivos conectados estiver abaixo de uma quantidade especificada.</p> <p>Para mais informações sobre o CloudWatch, consulte <a href="#">O que é o Amazon CloudWatch?</a> Para obter informações sobre como o AWS IoT Core funciona com o CloudWatch para criar métricas e alarmes, consulte <a href="#">Monitorar alarmes do AWS IoT e métricas usando o CloudWatch</a>.</p>

## Solução de problemas

Esta seção fornece informações sobre solução de problemas e possíveis soluções para ajudar a resolver problemas como um administrador do Fleet Hub.

Sintomas	Solução
O link do meu aplicativo da web não funciona.	Depois que o aplicativo é criado, pode levar algumas horas para o link funcionar.

Sintomas	Solução
Não consigo fazer login no meu aplicativo web.	<p>É necessário ter adicionado pelo menos um usuário ao seu aplicativo.</p> <p>Certifique-se de que sua função tenha a relação de confiança adequada, como a seguinte:</p> <pre data-bbox="831 520 1507 1037">{"Version": "2012-10-17",   "Statement": [     {       "Effect": "Allow",       "Principal": {         "Service": "iotfleethub.amazonsaws.com"       },       "Action": "sts:AssumeRole"     }   ] }</pre> <p>Para obter mais informações sobre como editar o relacionamento de confiança do IAM, consulte <a href="#">Editando o relacionamento de confiança para uma função existente</a>.</p>
Não consigo criar um aplicativo web.	<p>Certifique-se de que você não tenha atingido o limite do número total de aplicativos da web.</p>
Não estou vendo um campo personalizado que eu esperava.	<p>Verifique se você configurou a indexação de frota corretamente.</p> <p>Para obter mais informações sobre indexação de frota, consulte <a href="#">Indexação de frota</a>.</p>

# Fleet Hub for AWS IoT Device Management para usuários

Esta seção contém informações para usuários das aplicações web do Fleet Hub for AWS IoT Device Management. Para obter informações sobre como criar aplicativos do Fleet Hub e adicionar usuários a eles, consulte [Fleet Hub para gerenciamento de AWS IoT dispositivos para administradores](#).

## Tópicos

- [Conceitos básicos](#)
- [Consultas e filtros](#)
- [Trabalhando com trabalhos e modelos de trabalho no Fleet Hub for Device Management AWS IoT](#)
- [Alarmes](#)
- [Solução de problemas](#)

## Conceitos básicos

Esta seção contém informações sobre como começar a usar os recursos dos aplicativos da web Fleet Hub for AWS IoT Device Management.

## Tópicos

- [Crie sua primeira consulta](#)
- [Crie seu primeiro alarme](#)
- [Visualizar detalhes do dispositivo](#)

## Crie sua primeira consulta

Este tópico orienta você nas etapas para criar uma consulta simples do Fleet Hub for AWS IoT Device Management de dispositivos. As consultas são especificadas usando a sintaxe da consulta de pesquisa.

## Pré-requisitos

- Um aplicativo Fleet Hub associado a uma conta AWS IoT Core que contém dispositivos (objetos).
- Uma conta na sua organização que tenha permissões para usar o aplicativo Fleet Hub.

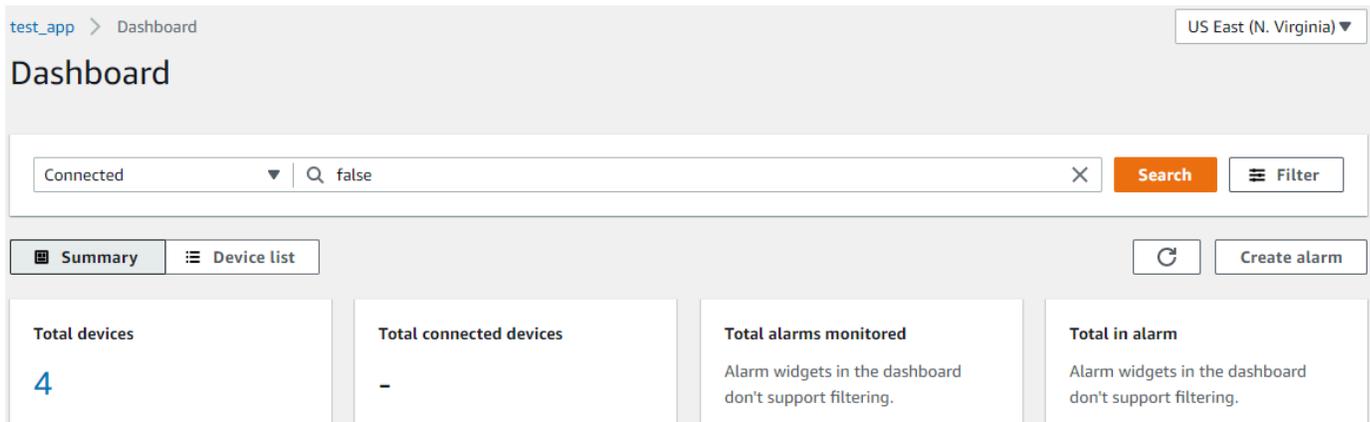
## Criar sua primeira consulta do Fleet Hub

### Criar sua primeira consulta do Fleet Hub

1. Navegue até seu aplicativo Fleet Hub.

A visualização do painel padrão exibe uma lista de todos os dispositivos que contêm os atributos gerenciados e personalizados. Os atributos que contêm o prefixo de atributos são atributos personalizados.

2. No menu na parte superior da página, escolha Conectado em Todos os campos. Digite **false** na caixa de texto ao lado do menu suspenso.



3. Para realizar a pesquisa, escolha Pesquisar. Você verá uma lista com todos os dispositivos que não estão conectados ao AWS IoT Core.

Para obter mais informações sobre a sintaxe de consulta e exemplos de consultas, consulte [Sintaxe de consulta](#), [Exemplos de consultas de objetos](#) e [Exemplos de consultas de grupos de objetos](#).

## Crie seu primeiro alarme

Este tópico orienta você nas etapas para criar um alarme simples do Fleet Hub for AWS IoT Device Management de dispositivos.

### Pré-requisitos

- Um aplicativo Fleet Hub associado a uma conta AWS IoT Core que contém dispositivos (objetos).
- Uma conta na sua organização que tenha permissões para usar o aplicativo Fleet Hub.

## Criando seu primeiro alarme

### Criar seu primeiro alarme do Fleet Hub

1. Navegue até seu aplicativo Fleet Hub.
2. Se você quiser segmentar um conjunto específico de dispositivos, crie uma consulta. Para obter instruções sobre como criar uma consulta simples, consulte [the section called “Crie sua primeira consulta”](#). Se você não criar uma consulta, seu alarme será aplicado a todos os dispositivos da sua frota.
3. Na página padrão do painel, escolha Criar alarme.
4. Na página Criar métrica de agregação, verifique se sua consulta aparece em Consulta de destino. Na seção Configurar agregação métrica da frota, no menu Escolher campo, escolha Conectado. Este campo gerenciado pela AWS indica se um dispositivo está conectado ao AWS IoT Core. O menu Escolher campo contém os campos gerenciados pela AWS e os campos personalizados que seu administrador criou na indexação da frota AWS IoT.
5. Para Escolher tipo de agregação, selecione qualquer uma das opções a seguir.
  - Máximo -- Configure um limite máximo.
  - Contagem -- Configure uma contagem específica como limite.
  - Soma -- Configure uma soma como limite.
  - Mínimo -- Configure um limite mínimo.
  - Média -- Configure um limite médio.
6. Em Escolher período, escolha a duração da condição especificada nos menus anteriores que acionará o alarme.

Um exemplo de configuração para Configurar a agregação métrica da frota pode ter a seguinte aparência:

### Configure fleet metric aggregation

#### Choose field

Choose a searchable field from your device's data.

Connected ▼

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

#### Choose aggregation type

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

Count ▼

#### Choose period

Choose the frequency on which this alarm will be based.

1 minute ▼

Escolha Próximo.

7. Na página Definir limite, no seção, Disparar o alarme sempre que..., selecione uma das opções a seguir.
  - Maior -- Alerta quando a métrica e o tipo de agregação excedem o valor especificado.
  - Maior/Igual -- Alerta quando a métrica e o tipo de agregação são iguais ou excedem o valor especificado.
  - Inferior -- Alerta quando a métrica e o tipo de agregação ficam abaixo do valor especificado.
  - Inferior/Igual -- Alerta quando a métrica e o tipo de agregação são iguais ou inferiores ao valor especificado.
8. Na caixa de texto Than, especifique o valor a ser usado como limite para o alarme.

Um exemplo de configuração para Definir limite pode ter a seguinte aparência:

**Trigger the alarm whenever...**

Metric is

Define alarm conditions

<input type="radio"/> Greater > threshold	<input checked="" type="radio"/> Greater/Equal >= threshold
<input type="radio"/> Lower/Equal <= threshold	<input type="radio"/> Lower < threshold

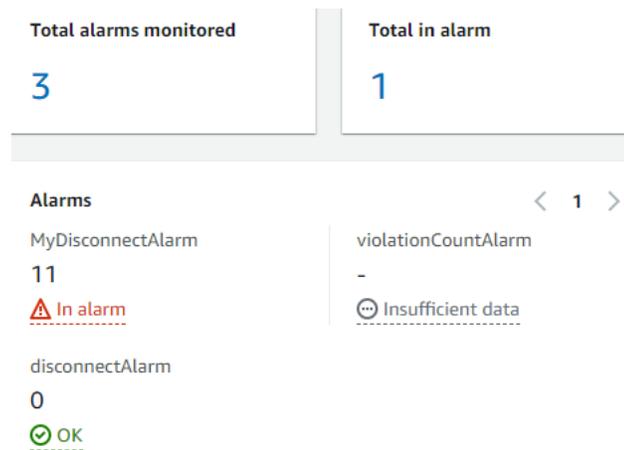
Than

Enter a threshold value.

1

Escolha Próximo.

9. Na página Notificar usuário, na seção Notificar -- opcional, insira um nome para a lista de e-mail que contém os usuários da sua organização que recebem notificações quando o alarme está ativo. Insira uma lista de endereços de e-mail separados por vírgula para preencher esta lista.
10. Na seção Detalhes do alarme, insira um nome para o alarme e, opcionalmente, insira uma descrição para o alarme. Escolha Próximo.
11. Na página Revisar, verifique as informações inseridas nas páginas anteriores. Selecione Enviar. Você retorna ao painel padrão.
12. No painel padrão, os widgets de alarmes exibem informações de todos os alarmes que você criou.



Para ver detalhes dos alarmes que você criou, no painel de navegação esquerdo, escolha Alarmes do Fleet Hub.

Fleet Hub alarms			Delete	Edit	Create alarm
<input checked="" type="checkbox"/> Show triggered alarms			< 1 >		
Alarm name	Status	Latest update			
<input type="radio"/> MyDisconnectAlarm	<span style="color: red;">⚠ Alarm</span>	November 17, 2021 18:20 (UTC)			
<input type="radio"/> disconnectAlarm	<span style="color: green;">✔ OK</span>	November 17, 2021 06:15 (UTC)			
<input type="radio"/> violationCountAlarm	<span style="color: grey;">⊖ Insufficient data</span>	November 17, 2021 06:12 (UTC)			

## Visualizar detalhes do dispositivo

Este tópico orienta você nas etapas para visualizar detalhes sobre seus grupos de dispositivos e seus dispositivos.

## Pré-requisitos

- Um aplicativo Fleet Hub associado a uma conta AWS IoT Core que contém dispositivos (objetos).
- Uma conta na sua organização que tenha permissões para usar o aplicativo Fleet Hub.

## Grupos de dispositivos

Ao fazer login no aplicativo web do Fleet Hub, você vê grupos de dispositivos no painel de navegação esquerdo. A página Grupos de dispositivos lista todos os grupos de dispositivos em seu aplicativo web do Fleet Hub. Para ver os detalhes de um grupo de dispositivos, escolha um grupo de dispositivos específico na coluna Nome do grupo.

	Group name	Parent group	Group type	Query	Group description	Created at
<input type="radio"/>	<a href="#">LightBulbs</a>	-	Static group	-	-	March 11, 2022 18:59 (UTC)
<input type="radio"/>	<a href="#">MyDynamicThingGroup1</a>	-	Dynamic group	attributes.wattage:75	-	October 17, 2021 22:15 (UTC)
<input type="radio"/>	<a href="#">MyStaticThingGroup</a>	-	Static group	-	-	March 11, 2022 18:49 (UTC)
<input type="radio"/>	<a href="#">MyStaticThingGroup2</a>	<a href="#">LightBulbs</a>	Static group	-	-	March 11, 2022 19:01 (UTC)

## Detalhes do grupo de dispositivos

A página de Detalhes do grupo de dispositivos contém informações sobre o grupo de dispositivos selecionado. Para ver os detalhes de um dispositivo, escolha um dispositivo específico na coluna Nome do dispositivo da seção Dispositivos em **XXX**.

test-0119 > Device groups > MyDynamicThingGroup1

## MyDynamicThingGroup1

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

### Group details

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

### Devices in MyDynamicThingGroup1 (2)

< 1 >  

Device name
<a href="#">MyLightBulb1</a>
<a href="#">MyLightBulb</a>

### Groups in MyDynamicThingGroup1

< 1 >  

Group name
------------

## Detalhes do dispositivo

A página de Detalhes de dispositivos contém informações sobre o dispositivo selecionado.

### Note

Se o seu cliente estiver usando um ID diferente do Nome do Objeto ao se conectar a AWS IoT, o status de conectividade do "objeto" não será indexado pela Indexação de Frota.

## Detalhes

A seção Detalhes contém as seguintes informações sobre seu dispositivo:

- Nome do dispositivo — O nome do recurso que representa seu dispositivo. Para acessar mais informações, consulte [Como gerenciar objetos com o registro](#).
- Tipo de objeto — O tipo de objeto que está associado ao seu dispositivo. Você pode usar o tipo de objeto para armazenar informações comuns a todas as objetos com o mesmo tipo de objeto. Para saber mais, consulte [Tipos de objetos](#).
- Carimbo de data e hora da última conexão — O registro de data e hora de quando seu dispositivo se conectou pela última vez a AWS IoT.
- Link de dispositivo compartilhável — Um link compartilhável que aponta para a página de Detalhes do dispositivo selecionado.
- Status da última conexão — O status da conexão do seu dispositivo com AWS IoT. Se seu dispositivo estiver conectado, o valor será *true*. Se não estiver conectado, o valor será *false*.
- Motivo da desconexão — O motivo pelo qual seu dispositivo está desconectado.

## Dados reportados

A seção Dados relatados contém informações sobre os dados de registro do seu dispositivo, dados de sombras do dispositivo e grupos de objetos.

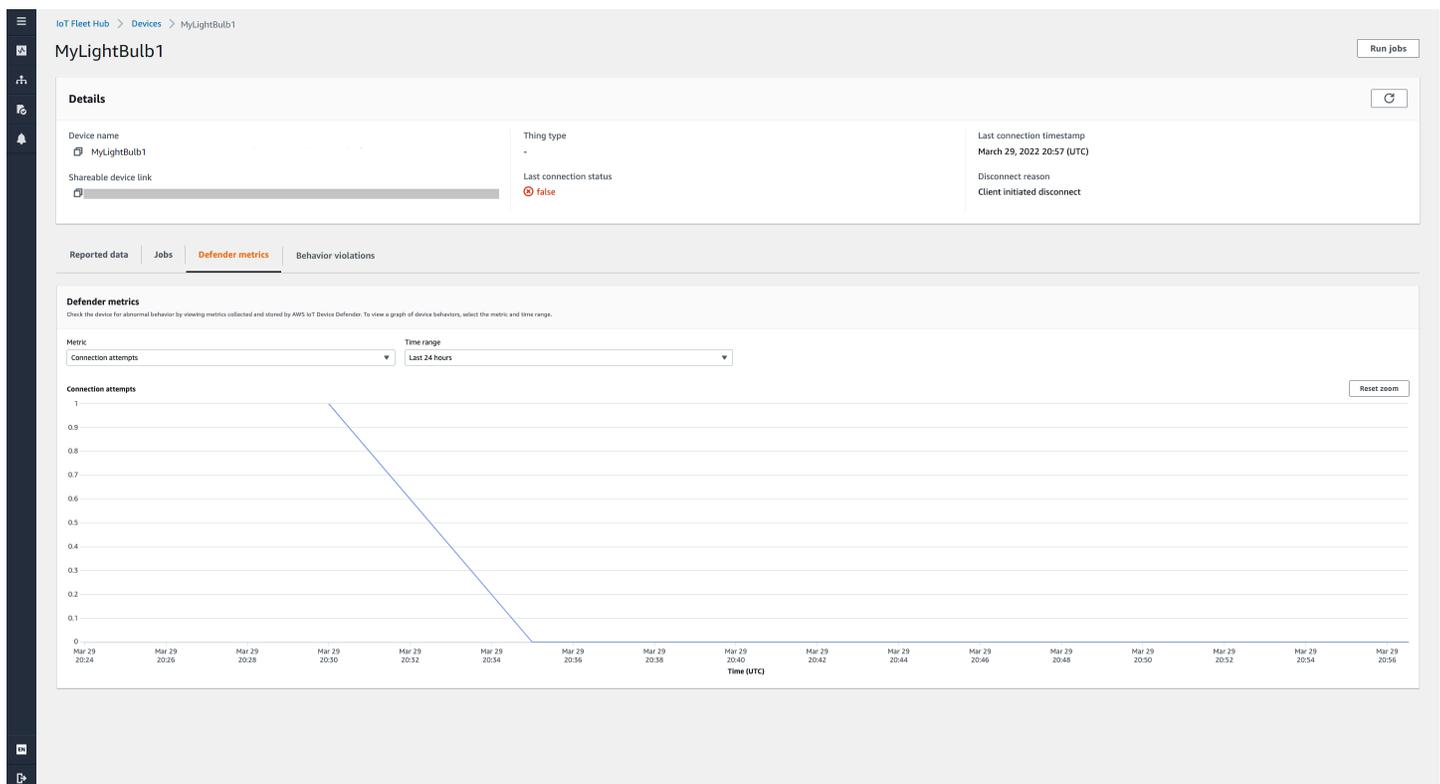
- Campos do dispositivo — Os campos indexados do seu dispositivo na indexação da frota de AWS IoT. Para acessar mais informações, consulte [Gerenciar a indexação de frota](#).
- Sombras do dispositivo — As sombras associadas ao seu dispositivo. As sombras do dispositivo podem incluir sombras clássicas sem nome e sombras nomeadas. Para obter mais informações, visite [sombra do dispositivo AWS IoT](#).
- Grupos de dispositivos — Os grupos de dispositivos associados ao seu dispositivo. Os grupos de dispositivos podem incluir grupos de objetos estáticas e grupos de objetos dinâmicas. Para obter mais informações, consulte [Grupos de objetos estáticos](#) e [Grupos de objetos dinâmicos](#).

## Trabalhos

A seção Trabalhos exibe todos os trabalhos em execução no dispositivo. Cada tarefa possui uma página de detalhes que exibe informações resumidas sobre a tarefa, incluindo informações de destino e de runtime (tempo de execução). Para obter mais informações, consulte [Trabalhando com trabalhos e modelos de trabalho no Fleet Hub for AWS IoT Device Management](#) e [Jobs](#).

## Métricas do Defender

A seção Métricas do Defender exibe AWS IoT Device Defender métricas associadas ao dispositivo atualmente selecionado. Você pode usar os dados de métricas exibidos para visualizar a operação do seu dispositivo em um período de tempo escolhido. Para visualizar os dados de métricas do defensor do seu aplicativo Fleet Hub, o administrador do Fleet Hub deve primeiro configurar métricas AWS IoT Device Defender associadas ao dispositivo selecionado. Para obter mais informações sobre como criar e configurar métricas do AWS IoT Device Defender para seus dispositivos, consulte [Métricas personalizadas](#), [Métricas do lado do dispositivo](#) e [Métricas do lado da nuvem](#).



## Violações de comportamento

A seção Violações de comportamento exibe os dados indexados de detecção de violações do AWS IoT Device Defender associados ao dispositivo atualmente selecionado. Os dados de violações de comportamento podem incluir a contagem de violações, a hora da última violação e o valor

da métrica da última violação. Para visualizar os dados de violações de comportamento do seu aplicativo Fleet Hub, o administrador do Fleet Hub deve configurar violações de comportamento AWS IoT Device Defender em um perfil de segurança e configurar violações AWS IoT Device Defender na [indexação da frota](#). Para obter mais informações sobre como configurar violações de comportamento em um perfil de segurança AWS IoT Device Defender, consulte [Detectar AWS IoT Device Defender](#). Para obter mais informações sobre como configurar violações AWS IoT Device Defender, consulte [Gerenciar a indexação de frota para aplicativos do Fleet Hub](#) e [Gerenciar a indexação de itens](#).

## Consultas e filtros

Você pode usar consultas do Fleet Hub for AWS IoT Device Management para criar e visualizar listas de itens em sua frota de dispositivos. Todos os campos gerenciados por AWS, campos personalizados e quaisquer atributos em suas fontes de dados indexadas estão disponíveis como filtros de consulta. Você também pode criar campos personalizados para ativar a agregação para [the section called “Alarmes”](#) usando a indexação da frota AWS IoT. Para ver mais informações sobre indexação de frota, consulte [Indexação de frota](#).

### Tópicos

- [Visualizar o painel](#)
- [Crie consultas com filtros](#)

## Visualizar o painel

Ao fazer login no aplicativo web Fleet Hub for AWS IoT Device Management, você vê um painel que apresenta duas visualizações de dados sobre os dispositivos da sua frota.

### Resumo

A visualização resumida exibe uma visão resumida dos dados sobre todos os dispositivos da sua frota. Ele fornece as informações a seguir.

- Número total de dispositivos
- Número de dispositivos conectados
- Uma lista dos motivos pelos quais os dispositivos foram desconectados
- Os tipos de objetos que você criou para sua frota e o número de dispositivos para cada tipo
- Os grupos de objetos que você criou para sua frota e o número de dispositivos em cada grupo

## Dashboard

All fields ▼ | 🔍 Search by values | Search | Filter

Summary | Device list | Refresh | Create alarm

<b>Total devices</b> 40	<b>Total connected devices</b> -	<b>Total alarms monitored</b> 2	<b>Total in alarm</b> 1
----------------------------	-------------------------------------	------------------------------------	----------------------------

**Disconnect reasons**

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

**Alarms** < 1 >

test-alarming-alarm 40 <span style="color: red;">⚠ In alarm</span>	test-ok-alarm 40 <span style="color: green;">✅ OK</span>
--	--

**Device types**

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

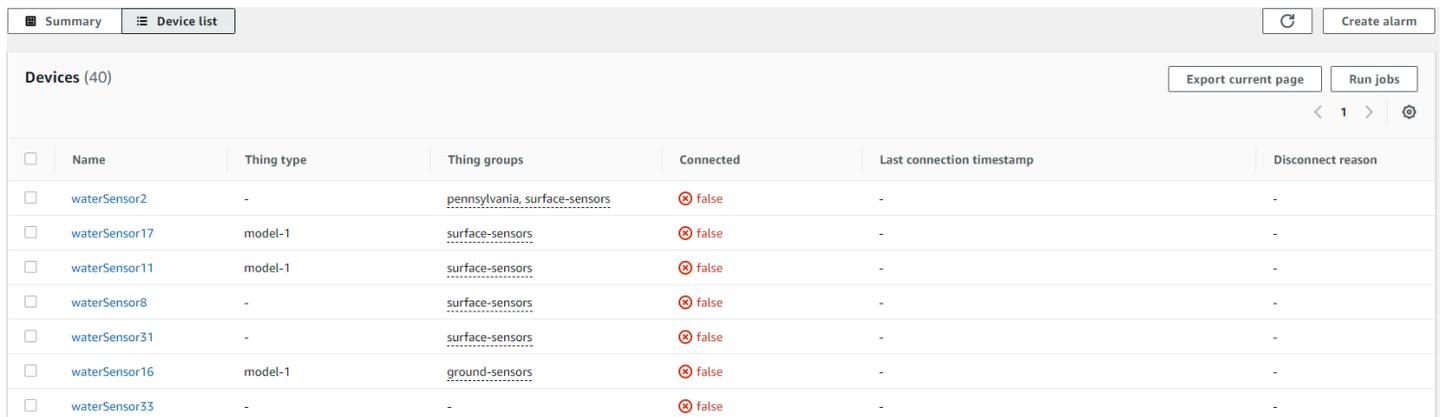
**Device groups**

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

## Lista de dispositivos

A visualização da lista de dispositivos exibe uma tabela que lista os dispositivos da sua frota. A tabela fornece as seguintes informações para cada dispositivo da lista.

- O nome do dispositivo
- O status da conexão do dispositivo
- A data e hora da última conexão do dispositivo
- Para um dispositivo que não está conectado, o motivo pelo qual ele foi desconectado
- O tipo de objeto do dispositivo
- O grupo de objetos do dispositivo
- Os campos personalizados que você criou no serviço de indexação de frota



<input type="checkbox"/>	Name	Thing type	Thing groups	Connected	Last connection timestamp	Disconnect reason
<input type="checkbox"/>	waterSensor2	-	pennsylvania, surface-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor17	model-1	surface-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor11	model-1	surface-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor8	-	surface-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor31	-	surface-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor16	model-1	ground-sensors	<span style="color: red;">⊗ false</span>	-	-
<input type="checkbox"/>	waterSensor33	-	-	<span style="color: red;">⊗ false</span>	-	-

Para baixar um arquivo CSV que contém os dispositivos exibidos na página, na lista de dispositivos, escolha Exportar página atual. Observe que, se a lista for paginada, isso só baixará os dados exibidos na página atual, não nas páginas subsequentes.

Você pode usar consultas e filtros para restringir o número de dispositivos que geram os dados resumidos na primeira visualização e que aparecem na lista de dispositivos. Para obter mais informações sobre o uso de consultas e filtros para obter informações mais específicas sobre dispositivos em sua frota, consulte [the section called “Criação de consultas”](#).

## Crie consultas com filtros

Este tópico explica como funcionam as consultas do Fleet Hub for AWS IoT Device Management e orienta você nas etapas necessárias para criar uma consulta com filtros.

Você pode controlar o número e os tipos de dispositivos que são exibidos no resumo do painel e nas exibições de lista usando consultas. Você filtra consultas usando campos gerenciados por AWS, campos personalizados e quaisquer atributos de suas fontes de dados indexadas da indexação da frota AWS IoT. Para obter mais informações sobre a indexação da frota, consulte a [indexação da frota](#).

Você também pode adicionar palavras-chave às suas consultas. As palavras-chave se aplicam a todos os campos pesquisáveis. Eles também são contabilizados no limite de três filtros que você pode aplicar em uma única consulta.

A seção a seguir descreve as etapas necessárias para criar uma consulta típica.

## Criação de consultas

As etapas a seguir descrevem como criar uma consulta típica.

## Pré-requisitos

- Um aplicativo Fleet Hub vinculado a uma conta AWS IoT Core que contém vários dispositivos (objetos)
- Uma conta que tenha permissões para usar o aplicativo Fleet Hub

Crie sua primeira consulta do Fleet Hub com um filtro no console

1. Navegue até seu aplicativo Fleet Hub.
2. No painel padrão, verifique se você pode ver a guia Lista de dispositivos e o número total de dispositivos (itens) na conta AWS IoT Core associada.
3. No painel padrão, escolha a guia Lista de dispositivos. Verifique se você vê uma lista de todos os dispositivos que contêm os atributos gerenciados e personalizados. Os atributos personalizados contêm o prefixo dos atributos.
4. Na parte superior da página, insira qualquer palavra-chave que você deseja incluir na sua consulta. As consultas por palavra-chave se aplicam a todos os campos.
5. Na parte superior da página, escolha Filtro.
6. No modal Filtro, em Campo, escolha o campo que você deseja usar como filtro. Em Operador, escolha uma opção. Por fim, em Valor, escolha o valor do campo a ser usado em seu filtro.

É possível adicionar até três filtros. Uma consulta de palavra-chave é contabilizada nesse número.

7. Para realizar sua consulta, escolha Aplicar filtros. Os resultados mostram todos os dispositivos que correspondem à sua consulta.

## Trabalhando com trabalhos e modelos de trabalho no Fleet Hub for Device Management AWS IoT

### Note

O atributo de modelos de trabalho está em versão prévia e sujeito a alterações.

Um trabalho é uma operação remota que é enviada e executada em um ou mais dispositivos conectados à AWS IoT. Por exemplo, você pode definir um trabalho que instrui um conjunto de

dispositivos a baixar e instalar um aplicativo ou atualizações de firmware, reinicializar, alternar certificados ou executar operações de solução de problemas remotamente. Você pode executar trabalhos pré-configurados a partir de aplicativos da web Fleet Hub for Device Management AWS IoT. Os administradores da sua organização criam modelos de trabalho no console AWS IoT e anexam políticas que disponibilizam os modelos aos usuários do Fleet Hub. No aplicativo Fleet Hub, você especifica os dispositivos ou um grupo de dispositivos nos quais o trabalho é executado.

Os administradores também criam grupos de dispositivos que você pode visualizar no seu aplicativo. Para ver esses grupos, escolha Device groups (Grupos de dispositivos) no painel de navegação. Ao especificar um grupo de dispositivos como destino, você pode especificar um dos dois tipos de opções a seguir para a execução do trabalho.

- instantâneo: o trabalho é executado uma vez.
- contínuo: após a execução inicial, o trabalho é executado em qualquer dispositivo adicionado ao grupo.

Para obter mais informações sobre como criar e gerenciar modelos de trabalho, consulte [Modelos de trabalho](#). Para obter mais informações sobre como os trabalhos funcionam, consulte [Trabalhos](#).

## Execução de trabalhos

Você pode executar um trabalho em vários locais em um aplicativo Fleet Hub, mas as etapas a seguir são sempre as mesmas.

1. Selecione um grupo ou um ou mais dispositivos como destino.
2. Escolha Run job (Executar trabalho).
3. Em Seleção de destino de trabalho, escolha contínuo ou instantâneo.
4. Selecione um modelo de trabalho. Verifique se o texto em Resumo do trabalho descreve o tipo de trabalho que você deseja executar.
5. Opcionalmente, insira um nome para o trabalho.
6. Escolha Executar.

Você pode selecionar alvos e seguir estas etapas nos seguintes locais em seu aplicativo Fleet Hub.

- A guia da lista de dispositivos no painel.
- A página de detalhes de um dispositivo específico.

- Página de grupos de dispositivos.
- A página de detalhes de um grupo de dispositivos específico.

## Visualizando e gerenciando trabalhos

Você pode ver os trabalhos em execução na sua frota nos seguintes locais.

- A página da lista de trabalhos: esta página exibe todos os trabalhos em execução na sua frota. Para ver esta página, escolha Trabalhos no painel de navegação.
- A página de detalhes de um dispositivo específico – esta página exibe todos os trabalhos em execução no dispositivo.

Cada tarefa possui uma página de detalhes que exibe informações resumidas sobre a tarefa, incluindo informações de destino e de runtime (tempo de execução). Esta página mostra o status do runtime (tempo de execução) do trabalho em cada dispositivo. Ele também exibe os seguintes totais.

- Número de execuções.
- Número de execuções canceladas.
- Número de execuções bem-sucedidas.
- Número de execuções com falha.
- Número de execuções rejeitadas.
- Número de execuções em fila.
- Número de execuções em andamento.
- Número de execuções removidas.
- Número de execuções com tempo limite.

Para cancelar um trabalho, selecione o trabalho e escolha Cancelar.

## Alarmes

Esta seção explica como os alarmes do Fleet Hub for Device Management AWS IoT funcionam e orienta você nas etapas necessárias para criar um alarme.

Quando você cria um alarme do Fleet Hub, ele se aplica a todos os dispositivos atualmente exibidos no seu painel. Se você não aplicar nenhuma consulta, o alarme será aplicado a todos os dispositivos

da sua frota. Para obter informações sobre como usar seu painel e criar consultas, consulte [the section called “Consultas e filtros”](#).

Os alarmes usam métricas do Amazon CloudWatch (CloudWatch) em combinação com campos pesquisáveis do serviço de indexação de frota AWS IoT para criar alarmes do CloudWatch. Por exemplo, você pode criar um alarme que gere uma mensagem do Amazon Simple Notification Service (Amazon SNS) sempre que o nível médio da bateria dos dispositivos da sua frota cair abaixo de 50%.

Os alarmes do Fleet Hub usam os recursos [getStatistics](#) e [getPercentiles](#) do serviço de indexação de frota para consultar dados agregados. Por exemplo, ao criar um alarme que rastreia um campo numérico personalizado, você pode criar limites de alarme que se aplicam aos seguintes valores do atributo especificado.

- Máximo
- Contagem
- Soma
- Mínimo
- Média
- Valores no percentil 10º, 50º, 90º, 95º ou 99º

Para obter mais informações sobre como consultar dados agregados no serviço de indexação de frota, consulte [Consultar dados agregados](#).

A tabela a seguir lista alguns exemplos de tipos de agregação disponíveis para campos AWS gerenciados e personalizados.

Campo	Tipo de agregação
Tipo de objeto (campo de string AWS gerenciado)	Contagem
Grupo de objetos (campo de string AWS gerenciado)	Contagem
Conectado (campo booleano AWS gerenciado)	<ul style="list-style-type: none"> <li>• Máximo</li> <li>• Contagem</li> </ul>

Campo	Tipo de agregação
O valor de <code>true</code> é 1. O valor de <code>false</code> é 0.	<ul style="list-style-type: none"> <li>• Soma</li> <li>• Mínimo</li> <li>• Média</li> </ul>
<code>shadow.reported.batterylevel</code> (campo de agregação numérica criado no serviço de indexação de frota)	<ul style="list-style-type: none"> <li>• Máximo</li> <li>• Contagem</li> <li>• Soma</li> <li>• Mínimo</li> <li>• Média</li> <li>• p10 (percentil 10)</li> <li>• p50 (percentil 50)</li> <li>• p90 (percentil 90)</li> <li>• p95 (percentil 95)</li> <li>• p99 (percentil 99)</li> </ul>

Além de especificar campos e tipos de agregação, você também especifica os valores a seguir.

- A duração (1 minuto ou 5 minutos) necessária para que o limite de alarme especificado acione o alarme.
- Um dos seguintes operadores de comparação para aplicar ao campo e tipo de agregação especificados.
  - Maior
  - Maior/Igual
  - Menor
  - Menor/Igual
- O valor a ser usado com o operador de comparação especificado.
- Uma lista de endereços de e-mail de pessoas da sua organização que recebem mensagens do Amazon SNS sempre que o alarme é acionado.
- Um nome de alarme.

Para criar um alarme do Fleet Hub, consulte [the section called “Criar alarmes”](#).

## Criar alarmes

Este tópico orienta você nas etapas necessárias para criar um alarme do Fleet Hub for Device Management AWS IoT. Ele pressupõe que seu administrador tenha criado um campo de agregação a partir de um campo sombra do dispositivo chamado `shadow.reported.batterylevel`. Esse campo personalizado indica o nível da bateria de um dispositivo. Você precisa pedir ao seu administrador para criar campos personalizados pesquisáveis no AWS IoT serviço de indexação de frota.

O alarme que você cria envia uma mensagem do Amazon Simple Notification Service (Amazon SNS) para uma lista de pessoas da sua organização sempre que o nível médio da bateria dos dispositivos da sua frota cai abaixo de 50% durante um período de 1 minuto.

### Criar uma consulta do Fleet Hub

1. Navegue até seu aplicativo Fleet Hub.
2. Se você quiser segmentar um conjunto específico de dispositivos, crie uma consulta. Para obter instruções sobre como criar uma consulta simples, consulte [the section called “Crie consultas com filtros”](#). Se você não criar uma consulta, seu alarme será aplicado a todos os dispositivos da sua frota.
3. Na página padrão do painel, escolha Criar alarme.
4. Na página Criar métrica de agregação, verifique se sua consulta aparece em Consulta de destino. Na seção Configurar agregação métrica da frota, em Escolher campo, escolha `shadow.reported.batterylevel`. Esse menu contém os campos AWS gerenciados e os campos personalizados que seu administrador criou no AWS IoT serviço de indexação de frota.
5. Em Escolher tipo de agregação, escolha Média. Esta escolha baseia o alarme no valor médio do nível da bateria na sua frota de dispositivos.
6. Para Escolher período, escolha 1 minuto. Isso aciona o alarme quando sua frota de dispositivos permanece no estado de alarme especificado por um minuto.

Escolha Próximo.

7. Na página Definir limite, na seção Acionar o alarme sempre que..., escolha Menor/Igual. Isso aciona o alarme quando o valor médio do nível da bateria cai abaixo de um valor especificado por você.
8. Na caixa de texto Do que, insira 50.

Escolha Próximo.

9. Na página Notificar usuário, na seção Notificar -- opcional, insira um nome para a lista de e-mail que contém os usuários da sua organização que recebem notificações quando o alarme está ativo. Insira uma lista de endereços de e-mail separados por vírgula para preencher esta lista.
10. Na seção Detalhes do alarme, insira um nome para o alarme e, opcionalmente, insira uma descrição para o alarme. Escolha Próximo.
11. Na página Revisar, verifique as informações inseridas nas páginas anteriores. Selecione Enviar. Você retorna ao painel padrão.
12. No painel padrão, no painel de navegação esquerdo, escolha Alarmes do Fleet Hub. Verifique se você vê o alarme que criou.

## Solução de problemas

Esta seção fornece informações sobre solução de problemas e possíveis soluções para ajudar a resolver problemas como usuário do Fleet Hub.

Sintomas	Solução
Não consigo adicionar mais filtros ou termos à minha consulta.	Verifique se você não atingiu o limite de quatro termos e filtros de consulta.
Não consigo encontrar uma métrica personalizada.	Peça ao administrador que crie a métrica no serviço de indexação de frota.
Meu alarme não está mostrando nenhum dado.	Demora alguns minutos até que os dados do alarme sejam carregados.
Preciso alterar os dispositivos direcionados ao meu alarme.	Acesse seu painel e altere a consulta.
Eu vejo um erro quando eu altero a região no meu painel.	Peça ao seu administrador para certificar-se de que a indexação de frota esteja ativada na região selecionada.
O status de conectividade do meu objeto não é indexado pelo Fleet Indexing.	Certifique-se de que seu cliente esteja usando o mesmo ID de cliente do Nome do objeto ao se conectar a AWS IoT. Se o seu cliente estiver usando um ID diferente do Nome do

Sintomas	Solução
	Objeto ao se conectar a AWS IoT, o status de conectividade do "objeto" não será indexado pela Indexação de Frota.

# Monitoramento do Fleet Hub para o AWS IoT Device Management

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do Fleet Hub e das outras soluções da AWS. A AWS fornece as seguintes ferramentas de monitoramento para observar o Fleet Hub, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

## Tópicos

- [Registrando o Fleet Hub para chamadas de API de gerenciamento de AWS IoT dispositivos com AWS CloudTrail](#)

## Registrando o Fleet Hub para chamadas de API de gerenciamento de AWS IoT dispositivos com AWS CloudTrail

O Fleet Hub for AWS IoT Device Management está integrado ao AWS CloudTrail. O serviço CloudTrail fornece um registro de ações que um usuário, função ou serviço AWS realiza no Fleet Hub. O CloudTrail captura as chamadas de API do Fleet Hub como eventos. As chamadas capturadas incluem as do console do Fleet Hub e as chamadas de código para as operações da API do Fleet Hub.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Fleet Hub. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos.

Usando as informações coletadas pelo CloudTrail, você pode determinar a solicitação feita ao Fleet Hub, o endereço IP do qual a solicitação foi feita, quem fez a solicitação e quando, além de mais detalhes.

Para saber mais sobre o CloudTrail, consulte o [Guia do usuário do AWS CloudTrail](#).

## Informações do Fleet Hub no CloudTrail

O AWS CloudTrail está habilitado na sua conta da AWS ao criá-la. Quando ocorre uma atividade no Fleet Hub, ela é registrada em um evento do CloudTrail junto com outros AWS Eventos de serviço em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro contínuo de eventos da conta da AWS, incluindo eventos do Fleet Hub, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon Simple Storage Service (Amazon S3). Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você.

Também é possível configurar outros produtos da AWS para analisar e atuar mais profundamente sobre os dados de eventos coletados nos logs do CloudTrail. Para ver mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configurar notificações do Amazon SNS para o CloudTrail](#)
- [Recebimento de arquivos de log do CloudTrail de várias regiões](#)
- [Recebimento de arquivos de log do CloudTrail de várias contas](#)

O CloudTrail registra todas as ações do Fleet Hub. Eles estão documentados na [Referência da API AWS IoT](#). Por exemplo, as chamadas para as ações `CreateApplication` e `UpdateApplication` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte [Elemento `userIdentity` do CloudTrail](#).

## Noções básicas sobre entradas do arquivo de log do Fleet Hub for AWS IoT Device Management

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado.

Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante.

Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

### Example

A seguinte entrada de log do CloudTrail mostra informações sobre a ação `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"
}
```

# Segurança no Fleet Hub para gerenciamento de AWS IoT dispositivos

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Fleet Hub, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Fleet Hub para gerenciamento de AWS IoT dispositivos. Os tópicos a seguir mostram como configurar o Fleet Hub para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Fleet Hub.

## Tópicos

- [Proteção de dados no Fleet Hub](#)
- [Identity and Access Management para Fleet Hub for AWS IoT Device Management](#)
- [Validação de conformidade do Fleet Hub para gerenciamento de AWS IoT dispositivos](#)
- [Resiliência no Fleet Hub para gerenciamento de AWS IoT dispositivos](#)
- [AWS políticas gerenciadas do Fleet Hub para gerenciamento de AWS IoT dispositivos](#)
- [Segurança da infraestrutura no Fleet Hub para gerenciamento de AWS IoT dispositivos](#)
- [Prevenção contra o ataque do “substituto confuso” em todos os serviços](#)

## Proteção de dados no Fleet Hub

O modelo de [responsabilidade AWS compartilhada O modelo](#) se aplica à proteção de dados no Fleet Hub for AWS IoT Device Management. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos AWS services que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas Frequentes sobre Privacidade de Dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão AWS services.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Fleet Hub ou outro AWS services usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Criptografia em repouso

O Fleet Hub protege os dados em repouso por meio de criptografia no servidor. Para obter mais informações, consulte [Criptografia de dados na AWS IoT](#), no Guia do Desenvolvedor do AWS IoT .

## Criptografia em trânsito

Em implantações na nuvem, o Fleet Hub protege dados em trânsito usando o protocolo Transport Layer Security (TLS). Para obter mais informações, consulte [Segurança de transporte na AWS IoT](#) no Guia do desenvolvedor do AWS IoT .

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

AWS Identity and Access Management (IAM) é uma ferramenta AWS service que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos Fleet Hub. O IAM é um AWS service que você pode usar sem custo adicional.

### Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como Fleet Hub for AWS IoT Device Management funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#)
- [Solução de problemas Fleet Hub for AWS IoT Device Management de identidade e acesso](#)

## Público

A forma como você usa o AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Fleet Hub.

Usuário do serviço - se você usa o serviço Fleet Hub para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Fleet Hub para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Fleet Hub, consulte [Solução de problemas Fleet Hub for AWS IoT Device Management de identidade e acesso](#).

Administrador do serviço – Se você é responsável pelos recursos do Fleet Hub em sua empresa, provavelmente terá acesso total ao Fleet Hub. Cabe a você determinar quais funcionalidades e recursos do Fleet Hub os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Fleet Hub, consulte [Como Fleet Hub for AWS IoT Device Management funciona com o IAM](#).

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Fleet Hub. Para visualizar exemplos de políticas baseadas em identidade do Fleet Hub que podem ser usadas no IAM, consulte [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#).

## Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte [Como fazer login Conta da AWS](#) no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações

usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte [Assinatura de solicitações de AWS API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação Multifator](#) no Guia do Usuário do AWS IAM Identity Center . [Usar a autenticação multifator \(MFA\) na AWS](#) no Guia do Usuário do IAM.

## Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos AWS services os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do Usuário do IAM.

## Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar AWS services usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas AWS services por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no Manual do Usuário do AWS IAM Identity Center .

## Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um usuário do IAM \(em vez de um perfil\)](#) no Guia do usuário do IAM.

## Perfis do IAM

Uma [função do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte [Utilizar perfis do IAM](#) no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidades de terceiros](#) no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a

autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM — um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns AWS services, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.
- Acesso entre serviços — Alguns AWS services usam recursos em outros AWS services. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a um serviço.
- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service, combinadas com a solicitação AWS service para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros AWS services ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).
- Função de serviço: um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service](#) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service. O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e

fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

## Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições.

Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do Usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. AWS services

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte [Visão geral da lista de controle de acesso \(ACL\)](#) no Guia do Desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões:** um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do Usuário do IAM.
- **Políticas de controle de serviço (SCPs)** — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizações e SCPs, consulte [Como os SCPs Funcionam](#) no Manual do Usuário do AWS Organizations .
- **Políticas de sessão:** são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do Usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

## Como Fleet Hub for AWS IoT Device Management funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Fleet Hub, saiba quais recursos do IAM estão disponíveis para uso com o Fleet Hub.

## Recursos do IAM que você pode usar com Fleet Hub for AWS IoT Device Management

Atributo do IAM	Suporte ao Fleet Hub
<a href="#">Políticas baseadas em identidade</a>	Sim
<a href="#">Políticas baseadas em recursos</a>	Não
<a href="#">Ações das políticas</a>	Sim
<a href="#">Atributos de políticas</a>	Sim
<a href="#">Chaves de condição de políticas</a>	Sim
<a href="#">ACLs</a>	Não
<a href="#">ABAC (tags em políticas)</a>	Sim
<a href="#">Credenciais temporárias</a>	Sim
<a href="#">Permissões de entidade principal</a>	Sim
<a href="#">Perfis de serviço</a>	Sim
<a href="#">Perfis vinculados ao serviço</a>	Não

Para ter uma visão de alto nível de como o Fleet Hub e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

### Políticas baseadas em identidade para o Fleet Hub

Compatível com políticas baseadas em identidade: Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elementos da política JSON do IAM](#) no Guia do Usuário do IAM.

## Exemplos de políticas baseadas em identidade para o Fleet Hub

Para visualizar exemplos de políticas baseadas em identidade do Fleet Hub, consulte [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#).

## Políticas baseadas em recursos no Fleet Hub

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. AWS services

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Ações políticas para o Fleet Hub

### Note

Os aplicativos do Fleet Hub usam a política gerenciada `AWSIoT FleetHubFederationAccess`. Para ter mais informações, consulte [???](#).

Suporte a ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Fleet Hub, consulte [Ações definidas pelo Fleet Hub for AWS IoT Device Management](#) na Referência de autorização do serviço.

As ações de políticas no Fleet Hub usam o seguinte prefixo antes da ação:

```
iotfleethub
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Para visualizar exemplos de políticas baseadas em identidade do Fleet Hub, consulte [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#).

## Recursos de política para o Fleet Hub

Compatível com recursos de políticas: Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (\*) para indicar que a instrução se aplica a todos os recursos.

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

Para obter uma lista dos tipos de recursos do Fleet Hub e seus ARNs, consulte [Recursos definidos pelo Fleet Hub for AWS IoT Device Management](#) na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte [Ações definidas pelo Fleet Hub for AWS IoT Device Management](#).

Para visualizar exemplos de políticas baseadas em identidade do Fleet Hub, consulte [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#).

## Chaves de condição de políticas para o Fleet Hub

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Fleet Hub, consulte [Chaves de condição do Fleet Hub for AWS IoT Device Management](#) na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas por Fleet Hub for AWS IoT Device Management](#).

Para visualizar exemplos de políticas baseadas em identidade do Fleet Hub, consulte [Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management](#).

## Listas de controle de acesso (ACLs) no Fleet Hub

Compatível com ACLs: Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## Controle de acesso por atributo (ABAC) com o Fleet Hub

Suporte a ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir

operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [O que é ABAC?](#) no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Utilizar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

## Usando credenciais temporárias com Fleet Hub

Compatível com credenciais temporárias: Sim

Alguns AWS services não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais AWS services funcionam com credenciais temporárias, consulte AWS services [“Trabalhe com o IAM”](#) no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para um perfil \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

## Permissões de entidade principal entre serviços para o Fleet Hub

Suporte ao recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações em AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service, combinadas com a solicitação AWS service para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros AWS services ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).

## Perfil de serviço do Fleet Hub

Compatível com perfis de serviço: Sim

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service](#) no Guia do Usuário do IAM.

### Warning

Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do Fleet Hub. Só edite os perfis de serviço quando o Fleet Hub orientá-lo a fazê-lo.

## Funções vinculadas ao serviço para Fleet Hub

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte [Serviços da AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

## Exemplos de políticas baseadas em identidade para Fleet Hub for AWS IoT Device Management

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Fleet Hub. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte [Criação de políticas do IAM](#) no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Fleet Hub, incluindo o formato dos ARNs para cada tipo de recurso, consulte [Ações, recursos e chaves de condição do Fleet Hub for AWS IoT Device Management](#) na Referência de autorização do serviço.

### Tópicos

- [Melhores práticas de política](#)
- [Usando o console do Fleet Hub](#)
- [Permitir que usuários visualizem suas próprias permissões](#)

### Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Fleet Hub em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo — ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também

conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do Usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso — você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service, como AWS CloudFormation. Para obter mais informações, consulte [Elementos da política JSON do IAM: Condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais — o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas Recomendadas de Segurança no IAM](#) no Guia do Usuário do IAM.

## Usando o console do Fleet Hub

Para acessar o Fleet Hub for AWS IoT Device Management console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Fleet Hub em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do Fleet Hub, anexe também o Fleet Hub ConsoleAccess ou a política ReadOnly AWS gerenciada às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

## Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

## Solução de problemas Fleet Hub for AWS IoT Device Management de identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Fleet Hub e o IAM.

### Tópicos

- [Não tenho autorização para executar uma ação no Fleet Hub](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Fleet Hub](#)

### Não tenho autorização para executar uma ação no Fleet Hub

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

#### Note

Os aplicativos do Fleet Hub usam a política gerenciada `AWSIoT FleetHubFederationAccess`. Para ter mais informações, consulte [???](#).

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso do `my-example-widget` fictício, mas não tem as permissões fictícias do `iotfleethub: GetWidget`.

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-example-widget` usando a ação `iotfleethub: GetWidget`.

## Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Fleet Hub.

Alguns AWS services permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando um usuário do IAM chamada `marymajor` tenta usar o console para executar uma ação no Fleet Hub. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Fleet Hub

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Fleet Hub oferece suporte a esses recursos, consulte [Como Fleet Hub for AWS IoT Device Management funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte [Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Como fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Validação de conformidade do Fleet Hub para gerenciamento de AWS IoT dispositivos

Audidores terceirizados avaliam a segurança e a conformidade do Fleet Hub como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para saber se um AWS service está dentro do escopo de programas de conformidade específicos, consulte [AWS services Escopo por Programa de Conformidade AWS services](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar AWS services é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

**Note**

Nem todos AWS services são elegíveis para a HIPAA. Para mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção AWS services e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#) — Isso AWS service fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [AWS Audit Manager](#) — Isso AWS service ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência no Fleet Hub para gerenciamento de AWS IoT dispositivos

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas,

conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

## AWS políticas gerenciadas do Fleet Hub para gerenciamento de AWS IoT dispositivos

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais informações sobre políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

## AWS política gerenciada: AWSIoT FleetHubFederationAccess

É possível anexar a política `AWSIoT FleetHubFederationAccess` a suas identidades do IAM.

Essa política concede aos usuários federados do Fleet Hub for AWS IoT Device Management as permissões necessárias para realizar ações AWS IoT e outros AWS serviços dos aplicativos web do Fleet Hub.

Para obter mais informações sobre como adicionar usuários aos aplicativos Web Fleet Hub, consulte [???](#).

Veja esta política em [Console AWS](#).

### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `iot`- Recupere dados AWS IoT do dispositivo e execute ações em nível de frota.
- `iotfleethub` - Recupere os metadados do aplicativo Fleet Hub.
- `cloudwatch`- Recupere dados métricos e de CloudWatch alarme. Também permite criar e excluir ações com escopo para alarmes do Fleet Hub.
- `sns` - Execute operações de criação, leitura, exclusão, assinatura e cancelamento de assinatura. Essas operações têm como escopo os tópicos do Fleet Hub SNS.

```
{
  "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*"
  }
]
}

```

## Atualizações do Fleet Hub nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Fleet Hub desde que esse serviço começou a rastrear essas alterações. Para obter mais informações, consulte a página de [histórico de documentação](#) do Fleet Hub.

Alteração	Descrição	Data
<a href="#">AWSIoTfleethubFederationAccess</a> : atualizar para uma política existente	Fleet Hub adicionou novas permissões para permitir que os usuários do aplicativo recuperem dados de métricas AWS IoT Device Defender em aplicativos Fleet Hub.	4 de abril de 2022
<a href="#">AWSIoTfleethubFederationAccess</a> : atualizar para uma política existente	Fleet Hub adicionou novas permissões para permitir que os usuários do aplicativo recuperem fontes de dados adicionais para indexação. Uma permissão também é adicionada para permitir que os usuários do aplicativo	15 de novembro de 2021

Alteração	Descrição	Data
	cancelam a execução de um AWS IoT trabalho dentro do aplicativo.	
<a href="#">AWSIoT FleetHub FederationAccess</a> : atualizar para uma política existente	O Fleet Hub adicionou novas permissões para que os usuários do aplicativo recuperem dados do Thing Group e realizem operações CRUD em AWS IoT trabalhos.	24 de maio de 2021
<a href="#">AWSIoT FleetHub FederationAccess</a> : atualizar para uma política existente	O Fleet Hub removeu permissões para APIs de painel do Fleet Hub não suportadas.	12 de abril de 2021
<a href="#">AWSIoT FleetHub FederationAccess</a> – Nova política	O Fleet Hub adicionou uma nova política que concede as permissões necessárias para que os usuários do aplicativo Fleet Hub recuperem dados do dispositivo e realizem AWS IoT ações.	12 de abril de 2021
O Fleet Hub começou a monitorar alterações	O Fleet Hub começou a monitorar as mudanças em suas políticas AWS gerenciadas.	12 de abril de 2021

## Segurança da infraestrutura no Fleet Hub para gerenciamento de AWS IoT dispositivos

Como um serviço gerenciado, o Fleet Hub for AWS IoT Device Management é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper [Amazon Web Services: Visão geral dos processos de segurança](#).

Você usa chamadas de API AWS publicadas para acessar o Fleet Hub pela rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.2 ou posterior. Recomendamos utilizar o TLS 1.3. Os clientes também devem ter compatibilidade com conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece compatibilidade com esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

## Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Para limitar as permissões que o Fleet Hub concede a outro serviço para o recurso, recomendamos o uso das chaves de contexto de condição global [aws:SourceArn](#) and [aws:SourceAccount](#) nas políticas de recursos. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

A maneira mais eficaz de se proteger contra o problema substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o nome do recurso da Amazon (ARN) completo do recurso. Para Fleet Hub, o seu `aws:SourceArn` deve estar em conformidade com o formato: `arn:aws:iot:region:account-id:*`. Certifique-se de que a **região** corresponda à sua região do Fleet Hub e que o **ID da conta** corresponda ao ID da sua conta de cliente.

O exemplo a seguir mostra como evitar o problema de substituto confuso usando as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` em uma política de confiança do perfil do Fleet Hub. Para encontrar o ARN da função do Fleet Hub, acesse a seção Fleet Hub no AWS IoT console e selecione seu aplicativo do Fleet Hub para ver a página de detalhes do aplicativo.

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

## Histórico de documentação

A tabela a seguir descreve as atualizações da documentação para o Fleet Hub. Para alterações nas políticas gerenciadas AWS para Fleet Hub, consulte [AWS políticas gerenciadas para Fleet Hub for AWS IoT Device Management](#).

Alteração	Descrição	Data
Versão de disponibilidade geral do Fleet Hub for AWS IoT Device Management	Conteúdo atualizado para refletir as melhorias feitas no Fleet Hub for AWS IoT Device Management durante o período de pré-visualização.	25 de maio de 2021.
Versão prévia do Fleet Hub for AWS IoT Device Management	Publicada a versão prévia do Guia do usuário do Fleet Hub for AWS IoT Device Management.	16 de dezembro de 2020.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.